

CRYPTO-GRAM
15 settembre 2003

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:

[Incidenti fortuiti e incidenti di sicurezza](#)
[Le reazioni a "Beyond Fear"](#)
[Le ristampe di Crypto-Gram](#)
[Concedere licenze agli utenti](#)
[News](#)
[Le news di Counterpane](#)
[Note di sicurezza da ogni dove: i copricapi nelle banche](#)
[Worm benigni](#)
[La Security-Breach Disclosure Law della California](#)
[Rettifica](#)
[Commenti dei lettori](#)

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

Incidenti fortuiti e incidenti di sicurezza

Il 14 agosto, alle ore 16:00, l'energia elettrica è venuta a mancare a New York e in buona parte del nord-est degli Stati Uniti. Circa cinquanta milioni di persone sono rimasti senza corrente, alcune per giorni. Anche se ci sono state iniziali voci di corridoio che hanno parlato di terrorismo (poche, fortunatamente), si è trattato di un imprevisto, un incidente fortuito.

In un periodo come questo, in cui ci si preoccupa di vari tipi di attacco -- da parte di terroristi, hacker e comuni malviventi -- è bene spendere un po' di tempo prendendo in considerazione i normali incidenti dovuti al caso.

Alcuni anni fa Ross Anderson, ricercatore di sicurezza informatica, ha parlato di differenza basata sulla dicotomia Murphy - Satana. Difendersi contro gli incidenti fortuiti, ha dichiarato, significa progettare e costruire in un mondo dominato dalla Legge di Murphy. Le cose vanno male perché... beh, perché vanno male. Quando si progetta mirando all'incolumità, si sta progettando per un mondo dove possono manifestarsi anomalie casuali. Si progetta un ponte che non crollerà in caso di terremoto, si producono lenzuola che non si infiammano in caso di incendio, e sistemi informatici che continueranno a funzionare -- o che almeno verranno elegantemente a mancare -- in caso di black-out. A volte si stanno studiando soluzioni per eventi di larga scala (trombe d'aria, terremoti, e altri disastri naturali), altre volte si progetta appositamente per eventi singoli: qualcuno che scivola sul pavimento del bagno, un bambino che infila una forchetta da qualche parte (un evento accidentale dal punto di vista dei genitori, anche se il bambino può averlo fatto deliberatamente), un albero che cade sul tetto di un edificio.

Con la sicurezza, le cose sono differenti. Oltre a doversi preoccupare degli incidenti fortuiti, occorre anche pensare a quegli eventi tutt'altro che casuali. Difendersi contro gli attacchi significa progettare e costruire in un mondo dominato dalla Legge di Satana. Le cose vanno male perché esiste un avversario intelligente e maligno che cerca di fare in modo che le cose vadano male, nel momento peggiore e con i peggiori risultati. Le differenze fra gli attacchi e gli incidenti fortuiti risiedono nell'intento, nell'intelligenza e nel controllo.

Ecco alcuni esempi:

Prevenzione: è possibile prevedere quante caserme dei pompieri servono ad una città per gestire i vari incendi che possono propagarsi casualmente.

Sicurezza: un piromane può deliberatamente far scattare più allarmi antincendio di quanti le varie caserme dei pompieri della città possano gestire, in modo da rendere i suoi attacchi maggiormente efficaci.

Prevenzione: capita che vengano lasciati accidentalmente dei coltelli nel bagaglio a mano che viene portato a bordo di un aereo; in genere vengono rilevati dai dispositivi a raggi X dell'aeroporto.

Sicurezza: un aggressore cerca di far passare un coltello realizzato in un materiale difficile da rilevare ai raggi X, e poi lo sistema deliberatamente nel proprio bagaglio per renderlo ancora più difficile da scoprire con un dispositivo a raggi X.

Prevenzione: gli ingegneri edili calcolano quante uscite d'emergenza sono necessarie per avere un'evacuazione sicura in caso di emergenza.

Sicurezza: quelle uscite vengono deliberatamente sbarrate prima che gli uccisori diano fuoco all'edificio (è accaduto in un convento del Rwanda nel 1994).

Alcuni anni fa, un mio collega stava sfoggiando il centro operativo di sicurezza di rete della sua azienda. Era certo che il suo team avrebbe potuto rispondere a qualsiasi intrusione informatica. "Che cosa succederebbe se l'hacker, prima di attaccare la vostra rete, facesse una telefonata annunciando la presenza di una bomba all'interno dell'edificio?", gli ho chiesto. Non aveva pensato a una simile opportunità. Il problema è che gli aggressori pensano a queste cose. Nel 1998 gli assassini adolescenti alla Westside Middle School nella città di Jonesboro, Arkansas, avevano azionato l'allarme antincendio prima di uccidere cinque persone e ferirne altre dieci mentre tutti stavano evacuando.

In un incidente fortuito, l'aggressore è il fato, la fortuna o madre natura. In un attacco, l'aggressore è intelligente e deliberato. Degli aggressori possono volontariamente causare danni precisamente nell'istante più opportuno e nella modalità più opportuna. Essi possono sfruttare incidenti capitati ad altre persone. E quando un aggressore scopre una vulnerabilità, può sfruttarla ripetutamente. Le probabilità di un incendio provocato da cause naturali sono molto basse nella maggior parte dei paesi industrializzati, ma un piromane può generare un incendio a richiesta. I buffer overflow possono capitare per caso in un computer, ma accade molto raramente; un aggressore può forzare un buffer overflow che provoca i danni peggiori in un sistema informatico. È la nozione di aggressore che separa gli ambiti della precauzione e della sicurezza. Nell'ambito della sicurezza, un'opposizione intelligente cerca di far vacillare la sicurezza. E un'insufficienza di protezione causata da un aggressore diventa un'insufficienza di sicurezza.

Le due cose sono anche molto simili. Che si venga accoltellati da un rapinatore, o il coltello è sfuggito in un incidente domestico, il pronto soccorso risponderà allo stesso modo. La risposta da parte di vigili del fuoco, agenti di polizia e altro personale di soccorso dopo l'11 settembre non sarebbe stata diversa se gli aerei avessero perso l'orientamento nella nebbia e si fossero accidentalmente schiantati contro le Torri Gemelle (proprio come un aereo si schiantò contro l'Empire State Building nel 1945). Le procedure di backup sono le stesse sia nel caso che qualcuno abbia cancellato un file per errore, sia nel caso il file sia stato eliminato dal codice di un worm.

Le difese sono pressoché la stessa cosa: contromisure per proteggere i sistemi e misure di reazione dopo gli eventi. Un migliore isolamento di singole centrali elettriche evita la propagazione dei black-out, a prescindere dalle cause. La rarità dei black-out, che ha portato alla scarsa esperienza nel saperli affrontare, ha aggravato il problema. Il ripristino a seguito di una calamità funziona sia contro le inondazioni che contro le bombe. Assicurare l'anello più debole, implementare difese in profondità, dividere in compartimenti -- tutte le tecniche cui accenno per migliorare la sicurezza -- contribuiscono a prevenire incidenti.

In entrambi i casi -- mancanza di sicurezza e incidenti fortuiti -- è una serie di mancanze che finiscono col produrre risultati spettacolari. Quel black-out è iniziato come un lieve guasto, e poi con una reazione a catena si è trasformato in un black-out di vaste proporzioni. L'attacco terroristico dell'11 settembre è iniziato come un difetto di sicurezza piuttosto lieve (il dirottamento degli aerei), è diventato una grande sciagura (lo schiantarsi degli aerei contro il World Trade Center), fino a trasformarsi in una enorme tragedia (migliaia di vittime, edifici distrutti, interruzione delle comunicazioni, ecc.). In nessuno dei due casi i risultati finali avrebbero potuto essere previsti basandosi soltanto sui difetti iniziali; i sistemi erano semplicemente troppo complicati.

È a causa dell'interconnessione dei nostri sistemi che questi eventi si sono tramutati in disastri su larga scala. Succede di rado -- né il black-out, né gli attacchi terroristici erano eventi comuni -- ma a volte le cose si allineano con precisione in modo che gli esiti siano tragicamente negativi. Tuttavia, se un aggressore intelligente e maligno cerca di forzare gli eventi, un disastro sarà ancora più probabile.

** ** *

Le reazioni a "Beyond Fear"

Voglio ringraziare tutti coloro che hanno acquistato "Beyond Fear" da Amazon il 15 agosto. Il libro ha raggiunto il primo posto nell'elenco dei best-seller di saggistica (superando il libro di Al Franken), e il terzo posto nell'elenco dei best-seller in generale (dietro "The Da Vinci Code" e un libro di diete).

Tecnicamente, il libro non è stato pubblicato prima del 4 settembre, e già stanno aparendo alcune recensioni.

"L'ultimo libro di Schneier, Beyond Fear (Copernicus Books, 2003), è un compendio assai leggibile delle sue osservazioni sui vari aspetti della sicurezza nel mondo reale. Pensato per un pubblico di non addetti ai lavori, è un'ottima introduzione ad un argomento complesso e che può generare confusione". -- Business Week

<http://www.businessweek.com/technology/content/sep2003/tc2003092_0578.htm>

"In 'Beyond Fear', Schneier ha completamente demistificato l'idea della sicurezza grazie a un testo mirato direttamente ad un pubblico di non tecnici. Si serve della sua proverbiale bravura nell'applicare lucidità e buonsenso a problematiche di information security, la applica a tutti gli spauracchi del dopo-11 settembre, e pone la domanda cruciale: che cosa stiamo avendo in cambio di quelle libertà che le autorità di Ashcroft ci hanno tolto in nome della sicurezza?"

Si tratta forse della questione più importante di tutto questo decennio, e ciò rende il libro di Schneier uno dei testi più importanti di questo decennio. Dovrebbe essere una lettura obbligatoria per ogni cittadino americano, e il mondo sarebbe un posto migliore se chiunque osasse manifestare un'opinione in merito al voto elettronico, alla sicurezza delle linee aeree, alle intercettazioni, o a qualsiasi altro orrore moderno, facesse prima tesoro delle lezioni di questo libro". -- Cory Doctorow, BoingBoing

<http://boingboing.net/2003_08_01_archive.html#200444060>

Un affascinante articolo riguardante un hacker delle slot machine:

<http://www.usatoday.com/tech/news/2003-08-11-slot-cheats_x.htm>

Modi di sfruttare la tessera fedeltà dei supermercati Safeway nel tentativo di difendere la privacy:

<<http://www.wired.com/news/business/0,1367,59589,00.html>>

Una dimostrazione della nuova tecnologia di rilevamento a raggi X degli aeroporti:

<<http://www.wired.com/news/images/0,2334,59401-7859,00.html>>

Quando Windows XP va in crash, chiede se si desidera inviare un report a Microsoft. Vi siete mai chiesti che fine facciano quei report?

<<http://www.pcmag.com/article2/0,4149,1210067,00.asp>>

Applicare patch non funziona. (Io lo avevo già detto nel 2000).

<<http://www.computerworld.com/securitytopics/security/holes/story/0,10801,84083,00.html>> oppure <<http://tinyurl.com/n55b>>
<<http://www.computerworld.com/softwaretopics/os/windows/story/0,10801,84084,00.html>> oppure <<http://tinyurl.com/n55e>>

Il Dipartimento di Giustizia degli Stati Uniti ha rilasciato "una relazione dell'Operato dell'FBI nel contrastare, rilevare ed investigare le attività di spionaggio di Robert Philip Hanssen". Quantomeno il riassunto esecutivo non coperto da segretezza.

<<http://www.usdoj.gov/oig/special/03-08/index.htm>>

Relazione del NIST sugli IDS:

<<http://csrc.nist.gov/publications/nistir/nistir-7007.pdf>>

Decrittazione di un documento storico del XVII secolo:

<<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/08/29/ndiary29.xml>> oppure <<http://tinyurl.com/n55o>>

La triste, tristissima storia della policy della licenza software di Dell. Una licenza impossibile da leggere non aiuta nessuno, né l'acquirente né il venditore. Si tratta di pessima sicurezza davvero.

<<http://www.cypherpunks.ca/dell.html>>

In un mondo dove la tecnologia è sempre più onnipresente, è importante ricordare che funzionano anche stratagemmi low-tech. Due persone travestite da tecnici si sono introdotte nel "customs cargo processing and intelligence center" [lett. trattamento di merci doganali e centro di intelligence] dell'aeroporto di Sydney, hanno armeggiato per un paio d'ore e se ne sono andate con un paio di server (nota: "ASIO" significa Australian Security Intelligence Organization, un'entità simile alla CIA).

<http://news.ninemsn.com.au/National/story_51495.asp>
<<http://www.smh.com.au/articles/2003/09/04/1062548967124.html>>
<<http://www.theregister.co.uk/content/55/32677.html>>

Gravi difetti nella crittografia del protocollo GSM di telefonia cellulare:

<<http://www.newscientist.com/news/news.jsp?id=ns99994130>>

Un rapporto interessante sulla sicurezza delle macchine Diebold per il voto elettronico. Cose allarmanti, se si considera che queste macchine vengono già acquistate per essere utilizzate nelle elezioni negli Stati Uniti.

<<http://avirubin.com/vote.pdf>>

virale sono intrinsecamente cattivi e sbagliati, e utilizzarli con payload benefici non migliora le cose. Un worm non è un tool per nessun ragionevole amministratore di rete, a prescindere dagli intenti.

Un buon meccanismo di distribuzione di un software presenta le seguenti caratteristiche:

- 1) È possibile scegliere le opzioni desiderate.
- 2) L'installazione è adattata alla macchina su cui sta girando.
- 3) È semplice fermare una installazione in corso, o disinstallare il software.
- 4) È semplice venire a sapere che cosa è stato installato e dove.

Un buon worm, al contrario, si attiva senza il consenso dell'utente. Ha una piccola porzione di codice, e una volta che inizia a diffondersi, si auto-propaga, e continuerà a farlo finché non lo si arresta.

Queste caratteristiche sono semplicemente incompatibili. Offrendo all'utente un margine di scelta maggiore, rendere l'installazione flessibile e universale, permettere la disinstallazione -- tutte queste cose impediscono agli worm di propagarsi. Progettare un meccanismo di distribuzione migliore di un software, lo rende un worm peggiore, e viceversa. Dall'altra parte, rendere il worm più invisibile e meno evidente per l'utente, più piccolo e più facilmente propagabile e quindi impossibile da contenere, tutte queste cose significano una pessima distribuzione di un software.

Tutto ciò rende gli worm più pericolosi e diventa più arduo "guarire" da essi. I vari esperimenti, il più delle volte involontari, dimostrano che è molto difficile effettuare con successo il debugging di un worm: in altre parole, una volta che gli worm iniziano a diffondersi, è complicato predire esattamente che cosa faranno. Alcuni virus sono stati scritti per propagarsi senza causare danni, ma ne hanno fatti (da macchine che andavano in crash a reti intasate) a causa di bug nel loro codice. Molti worm sono stati scritti per causare dei danni e si sono rivelati innocui (il che è ancora più emblematico).

Degli esperimenti condotti intenzionalmente da amministratori di sistema ben intenzionati provano che in un normale ambiente d'ufficio, il codice che ripara con successo una macchina non funziona su di un'altra. Addirittura a volte i risultati sono peggiori di qualsiasi minaccia di attacco esterno. La combinazione di un problema complicato con un meccanismo di distribuzione impossibile da controllare e da effettuare il debugging è ricca di pericoli. Ogni amministratore di sistema che abbia mai distribuito software automaticamente sulla propria rete ha sperimentato la classica situazione "premendo un solo bottone ho appena distrutto il software su centinaia di macchine in un solo colpo!". E questo con sistemi controllabili e di cui è possibile fare il debugging; quei sistemi auto-propaganti non permettono nemmeno di essere disattivati una volta scoperto il problema. Applicare patch ai sistemi è fondamentalmente un problema umano, e worm benefici sono una soluzione tecnica che non funziona.

D'altro canto, certe funzioni di aggiornamento automatico sono a volte una buona idea. Spesso gli amministratori delle reti aziendali le odiano, per tutta una serie di buoni motivi, ma non c'è altro sistema per applicare patch a moltissimi sistemi domestici. Vi sono intere schiere di utenti che non possono amministrare le loro macchine. Per queste persone, consiglio caldamente gli aggiornamenti automatici. Non saranno una cosa perfetta. Occasionalmente manderanno in tilt il computer. E presto o tardi qualcuno scoprirà come installare software maligno grazie al sistema di aggiornamento automatico. Ma si tratta sempre di una soluzione migliore di quella alternativa, che è quella di non applicare mai patch a questi sistemi.

(Una precedente versione di questo studio è stata scritta insieme a Elizabeth Zwicky nel 2000 e apparve in "The Industry Standard").

Articoli riguardanti Blast.D:

<<http://www.washingtonpost.com/ac2/wp-dyn/A9531-2003Aug18>>

<<http://www.computerworld.com/printthis/2003/0,4814,84126,00.html>>
<http://news.com.com/2102-1002_3-5065117.html?tag=ni_print>

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

La Security-Breach Disclosure Law della California
[lett. Legge sulla Divulgazione delle Falle di Sicurezza]

Il Security Breach Information Act della California è entrato in vigore dal primo luglio. Secondo quanto riportato dalla stampa, lo scopo della legge è quello di obbligare le aziende a rendere note le falle di sicurezza a tutti coloro che possono subirne le conseguenze. Per esempio, se il vostro numero di carta di credito venisse rubato dal database di una certa azienda, quell'azienda deve informarvi dell'accaduto -- se ovviamente siete residenti in California. L'idea è duplice. Primo: i consumatori saranno in grado di prendere migliori decisioni di sicurezza perché più informazioni vengono rese pubbliche. Secondo: le aziende che intendono evitare imbarazzi investiranno più denaro per migliorare la propria sicurezza informatica.

L'idea è veramente buona, ma la legge è scritta talmente male da risultare una farsa. Vi sono scappatoie così grandi da nascondere qualsiasi falla di sicurezza.

1) Viene applicata solo al furto di dati comprendenti il nome della persona e uno dei seguenti: il numero di previdenza sociale (SSN), il numero della patente di guida, il numero di conto corrente più i relativi PIN o password. Un database di nomi e di numeri SSN rientrerebbe nella legge. Un database di nomi, numeri di carte di debito e PIN, anche. Un database di numeri SSN, di numeri di carte di debito e di PIN non rientrerebbe nella legge. Così come non rientrerebbe un database di nomi e di numeri di carte di credito (senza PIN). E nemmeno un estratto conto bancario o di carta di credito, nel caso non vi sia riportato il numero SSN.

2) Non viene applicata al furto di nessun altro tipo di dati. Non è necessaria alcuna divulgazione se qualcuno ruba un database di dati sanitari sensibili. Non è necessaria alcuna divulgazione se qualcuno ruba un database relativo a uno storico acquisti. Non è necessaria alcuna divulgazione se qualcuno ruba i registri di un videonoleggio, o uno storico acquisti librario, o email personali, procedimenti legali, registri penali, o qualsiasi altro tipo di informazione personale.

3) Viene applicata soltanto se il nome o gli altri dati non sono protetti da crittografia. Questo avrebbe anche un senso, finché non si tiene presente che non viene specificato il metodo crittografico. Anche se la crittografia è decodificabile, anche se la chiave crittografica viene rubata insieme ai dati, anche se il database è protetto da ROT 13, non è necessaria alcuna divulgazione.

4) La divulgazione può essere ritardata "se un'agenzia delle forze dell'ordine stabilisce che la notifica verrebbe ad ostacolare un'indagine su un reato". Almeno la deliberazione deve essere prodotta dalla polizia e non dall'azienda attaccata, ma non credo sarà così difficile trovare un'agenzia di forze dell'ordine locale intenzionata a produrre quella deliberazione.

Obbligare le aziende all'apertura quando le informazioni private dei loro clienti sono state compromesse è una buona idea; sfortunatamente però questa legge è scritta così male che può essere tranquillamente ignorata. Secondo un articolo di Computerworld, un procuratore ha detto: "quel che alcune aziende stanno pensando di fare è assegnare un numero casuale al nome del cliente in un database e collegare quel numero casuale alle informazioni personali identificabili registrate in un altro database, completamente distinto". Sarà anche seguire la legge alla lettera, ma è di certo contro lo spirito.

Ecco un esempio soltanto. Lo scorso mese Daniel Baas è stato arrestato per essersi introdotto nel database della Acxiom Corp. ed aver sottratto i dati dei clienti. Acxiom è una compagnia

Commenti dei lettori

Da: Bruce McNair <bmcnair@novidesic.com>

Oggetto: Come reagire

Ritengo sia terribile che qualcuno rilasci intenzionalmente delle informazioni sbagliate ad agenzie governative o a chi raccoglie dati aziendali, come suggerito da Richard. Quando lo stato del New Jersey richiede il mio numero di previdenza sociale per il rinnovo della patente o per le varie registrazioni del veicolo, non mi sognerei mai di rilasciare informazioni errate. Certo, sono sempre di fretta, per cui la mia scrittura potrebbe non essere la più leggibile...

E sebbene faccia un po' di confusione ogni tanto, è rarissimo che scambi qualche cifra accidentalmente. Sto sempre attento ad inserire i numeri corretti -- non vorrei certo aggravare il problema di decifrare la mia scrittura. Tuttavia i numeri che scrivo tendono ad assomigliare alle lettere greche minuscole che i miei professori amavano usare. Ha presente? Eta e zeta, e tutte quelle altre che sembrano serpenti presi da spasmi addominali.

Proprio come i cassieri che insistono nel voler catturare elettronicamente la firma sulla carta di credito, agli impiegati della Motorizzazione non interessa quel che viene scritto, basta che possano mostrare al loro capo che non hanno fatto passare nessuno senza fargli compilare i moduli.

Fra l'altro, come si scrivono in cifre romane i numeri dell'ordine di 10 all'ottava? Ho verificato che i moduli della Motorizzazione non fanno espressa richiesta di leggibilità, ma non richiedono nemmeno che i numeri di previdenza sociale vengano scritti obbligatoriamente in numeri arabi.

Da: Pekka Pihlajasaari <pekka@data.co.za>

Oggetto: Come reagire

L'istigazione a un reato quasi sicuramente è un illecito penale e non dovrebbe essere difficile provarlo. Sono d'accordo che la via più facile è spesso quella di rilasciare dati scorretti, ma non credo che l'alterazione dei dati, deliberata o meno, corregga le aspettative latenti da parte di chi offre un servizio, e di certo è un ulteriore incentivo a richiedere una prova dell'identità di una persona per confermare la correttezza delle informazioni.

Ieri stavo lasciando il parcheggio di un centro commerciale e mi sono accorto di aver perduto la ricevuta del parcheggio dopo che era stata convalidata dal terminale. Però avevo ancora il secondo scontrino facoltativo di pagamento, e l'ho mostrato come prova di pagamento, così che mi fosse permesso uscire. Al personale di sicurezza mi sono rifiutato di fornire più informazioni personali di quanto mi sembrasse necessario, e non mi è stato dato il permesso di uscire.

Il capo della sicurezza mi ha detto che gli scontrini di pagamento possono essere scritti anche dopo il fatto, e possono venire usati per evitare di pagare il pedaggio dopo una sosta prolungata nel parcheggio. Il pretesto per la richiesta di documenti è quello di contrastare il comprensibile rischio di furti d'auto (spesso vi sono dei cartelli all'ingresso dei centri commerciali che invitano a non lasciare le ricevute del parcheggio all'interno delle auto). Il capo della sicurezza ha affermato che si trattava di una misura atta a dimostrare il loro zelo e che avrebbero così mantenuto la loro dichiarazione di diniego di responsabilità.

Alla fine la polizia ha raggiunto il parcheggio ed ha confermato la mia identità quale proprietario del veicolo, che era appunto mio. Ho perso circa 90 minuti, e forse il capo della sicurezza in futuro ci penserà due volte prima di seccare un cliente e di avere un'auto che blocca una delle uscite.

Da: "Balog Pal" <pasa@lib.hu>
Oggetto: Verifica di un tesserino

- > Note di sicurezza da ogni dove: verifica di un tesserino [...]
- > Impiegato: Questa è la mia faccia, vede? La porto sulla mia testa!
- > Addetto alla sicurezza: Mi occorre un altro documento d'identità con una sua foto
- > per confrontarla con questa.
- > Questa è un'ottima storia, perché ci illustra fino a quale livello guardie e addetti
- > alla sicurezza possano essere ignoranti su come funzioni realmente la sicurezza.

Questa storia mi ha procurato una bella risata. Ad ogni modo non mi sento di condividere tutti i suoi commenti. Quella guardia poteva anche essere incompetente, e ciò che ha detto non lasciava molti dubbi in proposito. Ma se io fossi stato in lui, avrei chiesto anch'io un documento d'identità.

Altrimenti si lascerebbe aperta la possibilità di un facile attacco. Se possiedo dei lineamenti molto simili ad un impiegato, tutto quel che mi occorre sapere è il suo numero identificativo. Una cosa tutt'altro che segreta. Poi mi invento la storia del tesserino perduto e penetro nell'edificio. Se viene richiesta una patente di guida, la guardia può essere (più) sicura che io sono davvero quell'impiegato, confrontando il nome e il documento d'identità. Per far sì che il mio attacco vada in porto, dovrei perlomeno raccogliere tutta una serie di dati personali dell'impiegato che ho deciso di impersonare, e realizzare un documento fasullo, oppure rubarlo.

Da: "Anderson, Kevin" <kevina@datapower.com>
Oggetto: Verifica di un tesserino

Apparentemente la guardia può sembrare stupida, ma è altrettanto possibile che l'impiegato sia davvero qualcuno che si è introdotto la notte prima nel sito della compagnia e abbia scambiato la fotografia dell'impiegato con la sua. Un'altra forma di autenticazione che facesse corrispondere nome, foto e indirizzo sarebbe un buon controllo di sicurezza. In questo caso una guardia dovrebbe SEMPRE controllare un documento d'identità per confrontare i dati con quelli inseriti nei registri aziendali (secondo criteri imposti da altri che si spera essere più competenti della guardia in quanto a sicurezza). È preferibile che la guardia esegua pedestremente tutti i passi necessari a un controllo di sicurezza che iniziare a stabilire quali passi debbano essere saltati secondo le occasioni. Se la guardia fosse un firewall e a volte saltasse la processazione di alcuni filtri, lo definiremmo un bug e ripareremmo il problema.

Da: "Heber Watts" <hewatts@comcast.net>
Oggetto: La precisione del database NCIC (National Crime Information Center)

Di recente ho letto il suo articolo, "La precisione del database NCIC (National Crime Information Center)" nel numero di Crypto-Gram del 15 aprile 2003. L'unico errore che ho trovato in questo articolo è il seguente.

Lei scrive che:

1. "Il Privacy Act del 1974 obbliga l'FBI a compiere ragionevoli sforzi per assicurare la precisione e la completezza delle voci di questo database. Il mese scorso, il Dipartimento di Giustizia ha esonerato il sistema dai requisiti di precisione richiesti per legge".
2. "Non solo si tratta di cattiva pratica sociale, ma è anche cattiva sicurezza. Un database con più errori è molto meno utile di un database che ha già molti errori, e un database di sicurezza pieno di errori ha molte più probabilità di prendere di mira gli innocenti che di lasciare i colpevoli a piede libero".

Queste affermazioni sembrano presupporre che non vi sia alcuna supervisione sull'accuratezza delle informazioni inserite nel database. Il grosso problema relativo ai requisiti del Privacy Act del 1974 è che nessuno avrebbe potuto prevedere il volume di informazioni che sarebbero state inserite nel database NCIC. Lei ha assolutamente ragione nell'affermare che il database è enorme e che è stata proprio la sua enormità ad essere fonte di problemi. È stato impossibile per l'FBI garantire l'accuratezza delle informazioni inserite da più di 80.000 agenzie partecipanti alla cosa. L'onere di garantire questa accuratezza adesso è di ogni singolo stato. E a questo dovere si aggiunge l'onere della responsabilità.

Non è possibile che un'unica agenzia centralizzata riesca a garantire l'accuratezza delle informazioni contenute in un database così vasto. Inoltre, gli agenti di polizia non eseguono arresti dichiarando qualcuno "colpevole" in base a quanto riportato nel database. I mandati forniscono "ragionevoli elementi di prova per procedere all'arresto". Per esempio, un agente di polizia del Maryland ferma un automobilista, esegue un controllo su NCIC e riceve una conferma: il database dichiara che l'individuo è ricercato in California. L'agente di polizia tratterà l'automobilista e l'operatore del commissariato del Maryland contatterà immediatamente l'ufficio della California che trattiene il mandato. L'agenzia della California ha un determinato lasso di tempo a disposizione per confermare la validità del mandato e che verranno nel Maryland a prelevare il ricercato e a riportarlo in California (estradizione). Se la California non intende riprendersi il ricercato, o non può "convalidare" il mandato nei tempi richiesti, la persona viene rilasciata e non viene effettuato alcun arresto.

Le singole agenzie partecipanti hanno l'obbligo di avere dei sistemi sul posto in grado di confermare l'accuratezza delle informazioni che inseriscono nel sistema. Inoltre, le informazioni del NCIC hanno un valore probatorio molto limitato. Il suo maggior valore probatorio si evince in casi come l'esempio sopra riportato. Se il mandato della California riguardante quell'automobilista non avesse potuto essere convalidato o se la California non avesse avuto intenzione di procedere con l'estradizione, e l'automobilista avesse deciso di denunciare l'agente di polizia del Maryland per arresto illegale, l'agente del Maryland avrebbe potuto difendersi dichiarando di aver trattenuto la persona soltanto il tempo necessario alla convalida del mandato che la California aveva inserito nel sistema NCIC. L'agente di polizia del Maryland sarebbe stato tutelato perché le sue azioni sono state ragionevoli e accorte. In questo caso la California ha la responsabilità di garantire che ogni mandato sia valido e di informare il sistema su quanto lontano hanno intenzione di spingersi in trasferta per prelevare il ricercato. Tecnicamente sono responsabili di mantenere un mandato non valido o di non dichiarare con chiarezza quanto lontano sono disposti a spingersi per prelevare il ricercato.

Tutto questo, agli occhi degli esperti di information technology, non brilla molto per efficienza, ma è un'ottima salvaguardia. Le persone non vengono trattenute per un eccessivo lasso di tempo, né vengono arrestate illegalmente su larga scala, grazie a queste tutele. Vi sono ancora parecchi errori, come ad esempio i refusi, ma tali inconvenienti possono essere controllati attraverso ulteriori indagini. Il sistema non è perfetto, ma non è nemmeno completamente esposto.

Da: Saul Backal <saul@meganet.com>, Ralph Lotkin <lotkinlaw@aol.com>
Oggetto: Meganet

La Meganet Corporation è l'inventore e il proprietario della tecnologia di crittografia definita VME, Virtual Matrix Encryption, un algoritmo crittografico simmetrico a un milione di bit a cui è stato attestato il brevetto n. 6.219.421 (US Patent) il 17 aprile 2001. Malgrado tale attestazione, e malgrado la presenza di importanti clienti in tutto il mondo, certe figure della "cripto-comunità" continuano a mostrare disprezzo per la Meganet Corporation e sminuiscono VME senza aver nemmeno dato uno sguardo più approfondito a tale tecnologia.

A nostro parere, sia la Meganet Corporation, sia VME, sono state malgiudicate. Tutto quel che chiediamo e che si esamini con serietà la nostra tecnologia. Quel che desideriamo ottenere è che la comunità di crittografi giudichi obiettivamente Meganet e VME.

Qual è stata la ragione di tutte le critiche? La prima risposta è: abbiamo involontariamente commesso alcuni errori di business. E, da parte sua, la comunità si è affrettata a giudicare basandosi su quegli errori invece che su un'analisi oggettiva e approfondita dei meriti.

La Meganet Corporation ha iniziato con un nucleo operativo di due persone. La tecnologia era buona, ma non esisteva nessuna forza di marketing professionale, perciò, non avendo fra noi nessun esperto uomo d'affari, abbiamo ingenuamente scelto l'azienda di marketing sbagliata, una compagnia che affermava di essere leader nel marketing, ma che si è rivelata essere tutt'altro. La documentazione tecnica di VME è stata frammentata per creare documenti di marketing rivolti a un'industria che questi non conoscevano né comprendevano, e naturalmente i risultati sono stati disastrosi. Chi leggeva quel materiale screditava VME senza nemmeno prenderne visione o effettuare dei seri collaudi. La cosa più triste è che, a quanto sappiamo, nessuno di quegli esperti ha mai analizzato il nostro algoritmo, il codice sorgente, il brevetto, né ci ha mai contattato.

Quindi, che cosa ha fatto Meganet di sbagliato? Abbiamo utilizzato il team sbagliato per il marketing, un team che non ha la minima conoscenza dell'industria o della tecnologia. Un errore che molte neonate compagnie possono commettere agli inizi. Col senno di poi, a quell'errore speriamo di aver posto rimedio.

In secondo luogo, Meganet è stata criticata per la sua decisione di non rivelare pubblicamente il codice sorgente di VME. Tuttavia, abbiamo fatto questo per riservarci la possibilità di ricavare un guadagno vendendo la nostra tecnologia e per impedire ad altri di farne copie illegali o di incorporare la nostra proprietà intellettuale nella loro. In "Applied Cryptography", Bruce Schneier afferma che questa non-divulgazione altro non è che "sicurezza mediante segretezza" e che è una cosa inaccettabile. Ciò nonostante, trattando gli algoritmi RC4 e RC5 del professor Shamir, Schneier non ha fatto presente a Shamir gli stessi obblighi di divulgazione; a quanto pare perché Shamir è uno stimato professore, e quindi è stato dispensato. RC4 e RC5 sono diventati algoritmi tradizionali. Perché sono stati tenuti privati? A nostro parere perché il professor Shamir cercava di ottenere profitti dalla vendita della sua tecnologia, a differenza di RSA, che nei primi otto anni della sua esistenza ha visto il mondo intero utilizzare la sua tecnologia liberamente, anche se possedeva un brevetto. A quanto sappiamo, ci sono voluti due decenni circa a RSA prima di ricavare dalla propria tecnologia un profitto decoroso. Mentre RC4 e RC5 hanno portato rapidi guadagni.

Di conseguenza non siamo d'accordo sul fatto che il nostro rifiuto a divulgare il codice sorgente sia stato e continui ad essere un errore. Ma soprattutto, l'applicazione VME è stata a disposizione gratuitamente (in versioni dimostrative) per sette anni. Perciò domandiamo ancora: "Qualcuno degli esperti ha mai esaminato in modo approfondito la documentazione relativa al brevetto e all'algoritmo?" Qualcuno ci ha mai contattato? Per quanto ci è dato vedere, la risposta è "No".

Forse è più facile dichiarare che VME è una "burla", che non prendere in esame un nuovo approccio alla crittografia. E inoltre, disassemblare il codice eseguibile di VME, che consta di 160 miseri KB circa, dovrebbe essere un compito molto semplice per gli esperti di crittografia. Se la "sicurezza mediante segretezza" è di per sé negativa, come mai un'industria che pullula di esperti non è in grado di decompilare un codice eseguibile di 160KB per dimostrare che VME è una "burla" o di risolvere ripetute sfide a farlo?

Bisogna dire che in molti hanno avuto da ridire a riguardo delle sfide che abbiamo periodicamente allestito invitando hacker e appassionati di crittografia. Quelle gare sono state accusate di essere "disoneste", "false" e "infondate". Non siamo d'accordo. Abbiamo fornito l'applicazione che criptava il file. Abbiamo anche fornito il testo cifrato e, alla fine della sfida,

Counterpane Internet Security, Inc., è 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) 2003 by Bruce Schneier.