

CRYPTO-GRAM
15 marzo 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:

SHA-1 violato

I limiti dell'autenticazione a due fattori

Le ristampe di Crypto-Gram

ChoicePoint

News

Lo hack degli URL in Unicode

GhostBuster

Le News di Counterpane

Note di sicurezza da ogni dove: furto di identità agli armadietti dei campi da golf

Il Canile: Xavety

Sensitive Security Information (SSI)

Commenti dei lettori

** ** ** ** **

SHA-1 violato

SHA-1 è stato seriamente violato. Non una versione a round ridotti. Non una versione semplificata. Proprio SHA-1.

Il team di ricerca di Xiaoyun Wang, Yiqun Lisa Yin, e Hongbo Yu (per la maggior parte dell'Università di Shandong in Cina) ha fatto quietamente circolare uno studio che descrive i loro risultati:

collisioni nello SHA-1 completo in 2^{69} operazioni hash, molto meno del numero di operazioni (2^{80}) dell'attacco brute-force basate sulla lunghezza hash.

collisioni in SHA-0 in 2^{39} operazioni.

collisioni nello SHA-1 a 58 round in 2^{33} operazioni.

Questo attacco va ad aggiungersi ai precedenti attacchi ai danni di SHA-0 e SHA-1, ed è un risultato di crittanalisi davvero, davvero importante. Il primo attacco contro SHA-1 più veloce del brute-force.

Lo scorso settembre scrissi di SHA e del bisogno di rimpiazzarlo. A parte i dettagli del nuovo attacco, ogni cosa che dissi allora è ancora valida. Di seguito riporterò brani da quell'articolo, integrandoli con nuovo materiale ove appropriato.

“Le funzioni one-way hash sono un costrutto crittografico utilizzato in svariate applicazioni. Vengono usate congiuntamente ad algoritmi a chiave pubblica sia per la crittografia che per le firme digitali. Vengono usate per verifiche di integrità. Vengono usate nel processo di autenticazione. Presentano tutta una serie di applicazioni in una grande varietà di protocolli. Molto più degli algoritmi di crittografia, le funzioni one-way hash sono i veri “cavalli da lavoro” della crittografia moderna.

Nel 1990 Ron Rivest inventò la funzione hash MD4. Nel 1992 migliorò la funzione MD4 e sviluppò un'altra funzione hash: MD5. Nel 1993 la National Security Agency pubblicò una funzione hash molto simile alla MD5, chiamata SHA (Secure Hash Algorithm). In seguito, nel 1995, riferendosi a una vulnerabilità appena scoperta e su cui si rifiutò di divulgare informazioni, la NSA effettuò un cambiamento a SHA. Il nuovo algoritmo fu chiamato SHA-1. Oggi SHA-1 è la funzione hash più diffusa, e MD5 è ancora usata nelle applicazioni più vecchie.

Le funzioni one-way hash dovrebbero avere due proprietà. La prima è che sono a senso unico (one way): questo significa che è semplice prendere un messaggio e calcolare il valore hash, ma è impossibile prendere un valore hash e ricreare il messaggio originale (con “impossibile” intendo dire “che non può essere fatto in un intervallo di tempo ragionevole”). La seconda proprietà è che sono libere da collisioni. Ciò significa che è impossibile trovare due messaggi che producano lo stesso identico valore hash. Il ragionamento crittografico che sta dietro a queste due proprietà è piuttosto sottile, ed invito i lettori più curiosi ad approfondire l'argomento sul mio libro “Applied Cryptography”.

Rompere una funzione hash significa dimostrare che una di quelle due proprietà, o entrambe, non sono vere.”

Il mese scorso, tre crittografi cinesi hanno dimostrato che SHA-1 non è esente da collisioni. Ovvero, hanno sviluppato un algoritmo che trova collisioni più velocemente rispetto al brute force.

SHA-1 produce uno hash a 160 bit, cioè ogni messaggio viene “sminuzzato” in numeri da 160 bit. Posto che esiste un numero infinito di messaggi che si combinano ad ogni possibile valore, vi è un numero infinito di collisioni possibili. Ma dato che il numero di hash possibili è così elevato, le probabilità di trovarne uno per caso sono talmente basse da essere trascurabili (una su 2^{80} , per la precisione). Se si sono “hashati” 2^{80} messaggi casuali, se ne troverà una coppia che presenta un hash allo stesso valore. Questo è il sistema “brute force” (forza bruta) di trovare collisioni, e dipende unicamente dalla lunghezza del valore hash. “Rompere” la funzione hash significa essere in grado di trovare collisioni in una maniera più veloce di questa ed è quello che hanno fatto i matematici cinesi.

Loro possono trovare collisioni in SHA-1 in calcoli 2^{69} , circa 2000 volte più velocemente del metodo brute force. Al momento, con la tecnologia attuale, siamo al limite estremo di fattibilità. Il confronto tra due immani calcoli illustra meglio questo punto.

Nel 1999, un gruppo di crittografi costruì un cracker per violare DES. Era in grado di compiere 2^{56} operazioni DES in 56 ore. Costruire il dispositivo costò 250.000 dollari, anche se potevano essere realizzati dei duplicati del costo dell'ordine di 50-75.000 dollari. Estrapolando quella macchina usando la Legge di Moore, una macchina simile costruita oggi potrebbe compiere 2^{60} operazioni in 56 ore e 2^{69} operazioni in tre anni e un quarto. Oppure, una macchina che venisse a costare 25-38 milioni di dollari potrebbe svolgere 2^{69} operazioni nello stesso intervallo di 56 ore.

Sul lato software, il principale calcolo comparabile è una chiave di ricerca 2^{64} condotta da distributed.net e conclusasi nel 2002. Un articolo l'ha messa in questo modo: "Nel corso della competizione, 331.252 utenti hanno partecipato mettendo a disposizione i cicli non utilizzati dei propri processori per scoprire la chiave. Dopo 1757 giorni (4,81 anni), un partecipante in Giappone ha scoperto la chiave vincente". Secondo la Legge di Moore, quel calcolo oggi si sarebbe svolto in un quarto del tempo (o avrebbe richiesto un quarto del numero di computer utilizzati), per cui oggi un numero di operazioni pari a 2^{69} impiegherebbe un tempo otto volte maggiore, o richiederebbe otto volte il numero di macchine.

"L'importanza di questi risultati dipende da chi siete. Se siete un crittografo, si tratta di una cosa enorme. Pur non essendo rivoluzionari, questi risultati rappresentano passi avanti sostanziali in questo campo. Le tecniche descritte dai ricercatori saranno probabilmente destinate ad avere altre applicazioni, e di conseguenza sarà meglio essere in grado di progettare sistemi sicuri. Questo è il modo con cui la scienza crittografica procede: si impara a ideare nuovi algoritmi rompendo altri algoritmi. In più, gli algoritmi provenienti dalla NSA vengono considerati una specie di scienza aliena: giungono da una razza superiore e senza spiegazioni alcune. Una qualsiasi crittanalisi che ha buon esito contro un algoritmo della NSA è un dato interessante nell'eterna questione di quanto siano davvero in gamba là dentro.

Per l'utente medio di Internet queste novità non sono particolarmente preoccupanti. Nessuno violerà firme digitali né leggerà messaggi cifrati tanto presto usando queste tecniche. L'universo elettronico non è meno sicuro di quanto non lo fosse prima di questi annunci.

Ma c'è un vecchio detto all'interno della NSA: "Gli attacchi diventano ogni giorno migliori; non peggiorano mai". Proprio come l'attacco operato questa settimana si serve di altri studi che hanno descritto attacchi contro versioni semplificate di SHA-1, SHA-0, MD4 e MD5, altri ricercatori si serviranno di questi risultati. L'attacco contro SHA-1 continuerà a migliorare mano a mano che altri lo studieranno e svilupperanno tecniche più veloci, ottimizzazioni, ecc. e la Legge di Moore andrà avanti, rendendo anche l'attacco odierno più veloce e raggiungibile.

Jon Callas, CTO di PGP, ha descritto il tutto in modo ancora migliore: "È tempo di camminare, non di correre, verso le uscite di emergenza. Non si vede ancora il fumo, ma gli allarmi antincendio sono già stati lanciati". Si tratta, sostanzialmente, di quel che io sostenevo lo scorso agosto.

"È venuto il momento per tutti di abbandonare SHA-1. Fortunatamente ci sono delle alternative. Il NIST (National Institute of Standards and Technology) offre già degli standard per funzioni hash più lunghe e più difficili da rompere: SHA-224, SHA-256, SHA-384 e SHA-512. Sono già standard governativi e possono già essere usate. Questo è un ottimo tappabuchi, ma mi piacerebbe vedere dell'altro.

Mi piacerebbe vedere il NIST indire e orchestrare una competizione mondiale per la creazione di una nuova funzione hash, così come fecero per fare in modo che il nuovo algoritmo crittografico AES rimpiazzasse DES. Il NIST dovrebbe pubblicare una richiesta di algoritmi e condurre una serie di turni d'analisi, in cui la comunità esamina le varie proposte con lo scopo di stabilire un nuovo standard.

L'autenticazione a due fattori attenua questo problema. Se la vostra password comprende un numero che cambia ogni minuto, o una risposta specifica a un quesito casuale, allora diventa più difficile che qualcun altro la intercetti. Non è possibile trascrivere la parte che cambia sempre. Una password intercettata non servirà a nulla alla successiva autenticazione. Una password a due fattori è più difficile da indovinare. Certo, uno può sempre dare la propria password e il relativo token alla segretaria, ma nessuna soluzione è infallibile.

Questi token sono stati in circolazione per almeno una ventina d'anni, ma hanno ricevuto l'attenzione del mercato di massa soltanto da poco. AOL li sta fornendo. Alcune banche li stanno generando per i propri clienti e molte altre dicono che lo faranno. Pare che finalmente le aziende stiano capendo che le password da sole non offrono una sicurezza adeguata e sperano che l'autenticazione a due fattori risolverà i loro problemi.

Purtroppo, la tipologia degli attacchi è cambiata in questi vent'anni. Ai tempi, le minacce erano soltanto passive: intercettazioni e tentativi di scoperta delle password effettuati offline. Oggi le minacce sono decisamente attive: phishing e cavalli di Troia.

Ecco due nuovi attacchi attivi che si iniziano ad incontrare:

- Attacco di tipo Man-in-the-Middle: un aggressore realizza un finto sito Web di una banca e spinge l'utente verso quel sito. L'utente inserisce la sua password e l'aggressore la sfrutta per accedere al vero sito della banca. Se questo attacco viene ben architettato, l'utente non si accorgerà di non essere nel vero sito Web della sua banca. Poi l'aggressore scollegherà l'utente e farà tutte le transazioni fraudolente che vuole, oppure permetterà all'utente di fare le proprie transazioni insieme alle sue transazioni illegali, nel medesimo tempo.

- Attacco Trojan: l'aggressore installa un Trojan nel computer dell'utente. Quando l'utente si autentica al sito Web della banca, l'aggressore sfrutta il Trojan per inserirsi in remoto nella stessa sessione, in modo da fare tutte le transazioni fraudolente che vuole.

Vedete come la transazione a due fattori non risolve niente? Nel primo caso, l'aggressore può passare la parte sempre variabile della password alla banca insieme alla parte fissa. Nel secondo caso l'aggressore si affida all'utente per autenticarsi.

La vera minaccia è la frode attuata attraverso la sostituzione di persona e le tattiche di sostituzione di persona cambieranno in risposta alle difese. L'autenticazione a due fattori spingerà i criminali a modificare le loro strategie, tutto qui.

Di recente ho visto esempi di autenticazione a due fattori mediante due percorsi di comunicazione differenti: chiamiamola "autenticazione a due canali". Una banca invia un quesito, una richiesta, al telefono cellulare dell'utente via SMS e si aspetta una risposta sempre via SMS. Se si assume che tutti i clienti abbiano un cellulare, allora il processo di autenticazione a due fattori risultante non avrà bisogno di altro hardware. Ancora meglio, la seconda parte dell'autenticazione viaggia attraverso un canale di comunicazione diverso dalla prima e l'intercettazione diviene molto più difficile.

Ma in questa nuova realtà di attacchi attivi, a nessuno importa una cosa del genere. Un aggressore che sfrutta un attacco Man-in-the-middle non avrà problemi dal fatto che è l'utente a gestire la parte SMS del login, perché non può farlo lui. Un aggressore che sfrutta un attacco Trojan non avrà problemi perché si affiderà all'utente per effettuare il login in ogni caso.

L'autenticazione a due fattori non è inutile. Funziona per autenticazioni locali e all'interno di certe reti aziendali. Ma non funzionerà per fare un login remoto attraverso Internet. Prevedo che banche e altri istituti finanziari spenderanno milioni in token da offrire ai loro clienti per effettuare

aperto gli account, facendo finta di essere delle società che cercavano informazioni su potenziali impiegati e clienti. Hanno pagato delle quote da 100 a 200 dollari, rilasciando false informazioni, e avendo così accesso a un tesoro di dati personali fra cui indirizzi, numeri telefonici, e numeri di previdenza sociale”.

-- Dal Presidente e CEO di ChoicePoint, Derek V. Smith: “La Core competency di ChoicePoint sta verificando e autenticando i singoli individui e le loro credenziali”.

Il motivo per cui c'è questa differenza è puramente economico. Il furto di identità è il reato con il tasso di crescita più rapido oggi negli Stati Uniti e rappresenta un gravissimo problema nel resto del mondo. Costa molto caro (in termini economici e di tempo) alle vittime. Non c'è molto che le persone possano fare per fermarlo, visto che molte delle loro informazioni personali non sono sotto il loro controllo, ma stanno nei computer di compagnie come ChoicePoint.

ChoicePoint arriva a proteggere i dati in suo possesso solo fino a un certo punto, e tale punto è il valore che essi hanno per l'azienda. Le centinaia di milioni di persone all'interno dei database di ChoicePoint non sono clienti di ChoicePoint. Essi non hanno il potere di cambiare agenzie di credito. Non hanno alcuna pressione economica da far pesare sul problema. Forse dovrebbero cambiare il nome della compagnia in “NoChoicePoint”.

Il risultato di tutto questo è che ChoicePoint non sostiene i costi del furto d'identità, per cui ChoicePoint non tiene conto di tali costi quando stabilisce la cifra da investire in sicurezza dei dati. In termini economici, si tratta di una “esternalità”.

Lo scopo della regolamentazione è rendere interne le esternalità. La legge SB 1386 lo ha fatto in certa misura, visto che ora ChoicePoint dovrà calcolare il costo della pubblica umiliazione quando deciderà quanto denaro investire in sicurezza. Ma il costo effettivo del fallimento della sicurezza di ChoicePoint è molto, molto più grande.

Finché ChoicePoint non sarà davvero affetta da quei costi -- che questo avvenga attraverso una legge o tramite la responsabilità -- l'azienda non avrà alcun incentivo economico per ridurli. Il capitalismo funziona, non attraverso l'elemosina aziendale, ma grazie al libero mercato. Non vedo altri modi per risolvere il problema.

Articoli di news:

<<http://www.msnbc.msn.com/id/6969799/>>

<<http://www.epic.org/privacy/choicepoint/>>

<http://www.latimes.com/business/la-fi-hacker16feb16_0,1035887.story>

<<http://wired.com/news/privacy/0,1848,66632,00.html>>

<http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1062076,00.html>

oppure <<http://makeashorterlink.com/?P28C16CAA>>

La registrazione 8K di ChoicePoint:

<<http://phx.corporate-ir.net/phoenix.zhtml?c=95293&p=irol-SECText&TEXT=aHR0cDovL2NjYm4uMTBrd2I6YXJkLmNvbS94bWwvZmlsaW5nLnhtbD9yZXBvPXRlbmsmaXBhZ2U9MzMzMzE3MiZkb2M9MCMZhdHRhY2g9b24=>> oppure

<<http://makeashorterlink.com/?P59C23CAA>>

Uno studio interessante di EPIC che offre proposte di riforma della privacy sulla scia di tutte le più recenti violazioni della privacy: ChoicePoint, Lexis/Nexis, Bank of America, DWS, ecc.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902>

Un'analisi davvero impressionante sulla tecnologia RFID di Texas Instruments utilizzata in svariati sistemi di sicurezza, quali immobilizzatori di veicoli e il sistema SpeedPass di ExxonMobil. Errore numero 1: l'algoritmo crittografico è un cipher proprietario a 40 bit.

<<http://rfidanalysis.org/>>

RFID Washer: pio desiderio.

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

Bidoni della spazzatura che vi spiano:

<<http://www.guardian.co.uk/online/story/0,3605,1410921,00.html>>

Chiamo questo genere di cosa "governo incorporato": tecnologie hardware e/o software messe all'interno di un dispositivo per assicurarsi che rispettiamo la legge. Naturalmente anche in questo caso vi sono rischi di sicurezza.

Il Governo degli Stati Uniti vieterà di portare accendini sugli aerei:

<<http://www.washingtonpost.com/wp-dyn/articles/A24774-2005Feb14.html>>

Il Government Accountability Office (GAO) ha pubblicato un rapporto dal titolo: "Aviation Security: Measures for Testing the Impact of Using Commercial Data for the Secure Flight Program" [Sicurezza aerea: Misure per testare l'impatto derivante dall'utilizzo di dati commerciali per il Programma Secure Flight].

<<http://www.gao.gov/cgi-bin/getrpt?GAO-05-324>>

Una ricerca davvero interessante sul riconoscimento a distanza dei dispositivi. Sostanzialmente, lo studio dimostra come è possibile identificare singoli computer attraverso Internet grazie alle irregolarità delle loro frequenze di clock.

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

La riserva d'acqua di Melbourne può essere controllata via Internet:

<<http://theage.com.au/articles/2005/03/07/1110160730005.html>>

Reset di password attivati via comandi vocali:

<<http://www.microsoft.com/speech/solutions/password/default.msp>>

La vera bellezza di questo sistema è che non richiede la presenza di un impiegato del servizio clienti che interagisca con l'utente. Ho visto statistiche che mostrano come il 25% di tutte le chiamate agli help desk provengano da persone che hanno dimenticato la loro password; tali chiamate costano circa 20 dollari l'una e portano via una media di 10 minuti l'una. Un sistema del genere offre una buona sicurezza e un risparmio di denaro. Non è perfetto, ma non lo sono nemmeno le password...

Dati satellitari non militari resi segreti per ragioni di "sicurezza", ma in realtà per nessuna ragione valida:

<<http://spaceflightnow.com/news/n0503/02observing/>>

Un'altra minaccia per la sicurezza che sa molto di trama da film: aerei senza equipaggio:

<http://jef.raskincenter.org/unpublished/next_time_can_be_worse.html>

Ottimo articolo tecnico sui network di bot: come funzionano, chi li usa e come, e il modo per rintracciarli:

<<http://www.honeynet.org/papers/bots/>>

Si tratta di un'analisi affascinante, e dettagliata, su ciò che occorrerebbe per distruggere la Terra: materiali, metodi, realizzabilità, passi necessari. Se da un lato il DHS può considerarlo un manuale

per terroristi e farlo eliminare da Internet, dall'altro le buone notizie sono queste: cancellare il pianeta non è un compito molto facile.

<<http://ned.ucam.org/~sdh31/misc/destroy.html>>

** **

Lo hack degli URL in Unicode

Molto tempo fa ho scritto dei rischi di sicurezza di Unicode. Questo è un esempio del problema.

Qui c'è una dimostrazione: è una pagina Web che sembra essere www.paypal.com, ma non si tratta di PayPal. Tutto fa pensare che sia www.paypal.com, dalla barra dell'indirizzo, al link che si attiva quando ci passiamo sopra con il puntatore.

Lo hack funziona sostituendo un carattere Unicode alla prima "a" in PayPal. Quel carattere Unicode assomiglia a una normale "a", ma non è una "a". L'attacco funziona persino sotto SSL.

Ecco il codice sorgente del link: <<http://www.pаypal.com/>>

La comunità Unicode sta lavorando per ovviare a questi problemi. Hanno una bozza di rapporto tecnico per la quale stanno cercando commenti. Una soluzione richiederà sforzi concertati, poiché vi sono coinvolti diversi tipi di problematiche (in un certo qual modo, l'hack qui descritto è uno dei casi più semplici).

Sito Web demo:

<<http://www.shmoo.com/idn/>>

Ulteriori informazioni:

<http://secunia.com/multiple_browsers_idn_spoofing_test/>

<http://www.boingboing.net/2005/02/06/shmoo_group_exploit_.html>

Il mio articolo originario:

<<http://www.schneier.com/crypto-gram-0007.html#9>>

La bozza del rapporto tecnico Unicode:

<<http://unicode.org/reports/tr36/>>

** **

GhostBuster

Microsoft Research ha sviluppato una cosa chiamata GhostBuster (acchiappafantasma), un programma prototipo che rileva software arbitrariamente persistente e nascosto, come i rootkit, i Trojan e i keylogger. È un'idea davvero elegante, basata su una semplice osservazione: per essere persistente, il rootkit deve esistere sul disco da qualche parte, ma per nascondersi deve mentire ai programmi attivi all'interno del sistema operativo infetto.

Ecco come funziona: l'utente ha il programma GhostBuster su un CD. Inserisce il CD nel lettore e dall'interno del sistema operativo (probabilmente corrotto), il programma di controllo parte:

blocca tutti gli altri programmi utente, svuota le cache, e poi esegue un checksum completo di tutti i file sul disco e una scansione di tutte le chiavi del Registro che possano avviare in automatico il sistema, scrivendo i risultati in un file sull'hard disk.

L'utente poi deve premere il tasto di reset. Il CD avvierà il proprio sistema operativo, e la scansione sarà ripetuta. Qualsiasi differenza fra la seconda e la prima scansione indicherà la presenza di un rootkit o di altro software nascosto, senza il bisogno di sapere di quali particolari rootkit si tratta né i checksum specifici di tutti i programmi installati sul disco.

Semplice. Intelligente. Elegante.

Per ingannare GhostBuster, il rootkit deve: 1) rilevare che un tale programma di controllo è in azione e non mentire ad esso oppure cambiare l'output che viene scritto su disco (in tale limite, questo diventa il problema più grosso per chi progetta il rootkit), 2) integrarsi nel BIOS invece che nel sistema operativo (difficoltoso, diverso da piattaforma a piattaforma, e non sempre possibile), oppure 3) rinunciare ad essere persistente o nascosto. In questo modo non verranno eliminati completamente i rootkit, ma di sicuro è un colpo mortale per i rootkit persistenti.

Ovviamente, il concetto potrebbe essere adottato per qualsiasi altro sistema operativo.

Questa è un'ottima idea, ma c'è un grosso problema: GhostBuster è solo un prototipo di ricerca, per cui non è possibile averne una copia. Ancora peggio, Microsoft non ha progetti per renderlo uno strumento commerciale.

Questa è un'idea troppo buona per essere abbandonata. Microsoft, se mi senti, dovresti rilasciare questo strumento al resto del mondo. Rendilo di dominio pubblico. Rendilo persino open source. È un'ottima idea, ed è giusto che tu ne abbia il merito.

C'è qualche altra compagnia di sicurezza in ascolto? Realizzate e vendete una cosa simile. C'è qualcuno là fuori che cerca una buona idea per un progetto open source? Qui ce n'è una davvero buona.

Nota: non so se Microsoft abbia brevettato o meno quest'idea. Se lo ha fatto e non rilascia il programma, si vergogni. Se non lo ha fatto, buon per lei.

Resoconto tecnico:

<<http://research.microsoft.com/research/pubs/view.aspx?type=Technical%20Report&id=775>>
oppure <<http://makeashorterlink.com/?H3BC12CAA>>

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

Le News di Counterpane

Schneier intervverrà alla Computers, Freedom and Privacy Conference a Seattle il 13 aprile, in una tavola rotonda sui passaporti RFID:
<<http://www.cfp2005.org/>>

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

Commenti dei lettori

Da: "Marc A." <marcusi@mac.com>

Oggetto: Priorità nelle linee GSM

Il GPS è divenuto un meccanismo di sincronizzazione standard per reti di comunicazione SDH/SONET. Chiudere completamente il sistema GPS costringerebbe i multiplexer presenti in tali reti a riportarsi su un clock interno, con dati di precisione che lo farebbero andare fuori sincronia con il resto della rete nel giro di un giorno circa. Questo impedirebbe in modo efficace il funzionamento dei maggiori link di telecomunicazione (+150 Mb/s) per TUTTI gli utenti (compresi i servizi di emergenza) e di conseguenza sarebbe un elemento importante nelle decisioni di un qualsiasi gruppo di risposta all'emergenza informato. Riattivare il meccanismo di Selective Availability [Disponibilità Selettiva] e introducendo il jittering per i ricevitori non-S/A è, quindi, una alternativa maggiormente percorribile.

Per quanto riguarda il GSM, tale sistema ha avuto per anni un meccanismo di impostazione chiamata e di priorità handoff (la stessa funzionalità viene sfruttata durante una chiamata di emergenza al 112), che è in grado di dare precedenza a determinati utenti. Ciò significherebbe non soltanto la possibilità di una disponibilità divisa in livelli di priorità, ma anche l'inibizione totale dell'accesso alla rete, eccetto i servizi di emergenza specificati (polizia, ambulanze, ecc.).

Il 3GPP ha un progetto per implementare tale meccanismo nelle reti WCDMA/UMTS (Multi-Level Precedence and Pre-emption -- MLPP), ma comprende inoltre una struttura di prelazione che sarebbe in grado di escludere un utente da una connessione voce/dati in corso per rendere disponibili le risorse di rete ad un altro utente con maggiore priorità.

Riferendomi agli attentati dinamitardi in Spagna, se da un lato concordo sul fatto che le vittime e il grande pubblico hanno un'esigenza legittima nel richiedere servizi di telecomunicazione in tempi di crisi, dall'altro ritengo che privarli di quella possibilità non significa tecnicamente sconnettere anche i "buoni" allo stesso tempo.

Naturalmente, implementare tutto questo sarebbe semplicemente una cattiva idea. Probabilmente causerebbe un trauma ancor più grande per il pubblico e non farebbe nulla di efficace per colpire dei terroristi ben preparati i quali, anticipando questa mossa, avrebbero pronti dei piani alternativi. Intendevo solamente dare una chiarificazione tecnica: il sistema GSM (quello utilizzato principalmente in Spagna), ben progettato e ingegnerizzato qual è, offre tra le sue funzionalità la selective availability.

Da: Matthew Rubenstein <email@mattruby.com>

Oggetto: Il controllo dei dati personali

Il problema del controllo dei propri dati, una volta che questi escono dalla nostra sfera di controllo, è essenziale per la nostra Era dell'Informazione. La gente continua a rubarsi i dati vicendevolmente. Inevitabilmente, continua a condividerli con altri che sono a loro volta non autorizzati e che rappresentano la vera minaccia. Questo vale per i dati dei media, come gli album musicali e per i dati personali, come le informazioni di identità registrate. Il problema legale, cioè chi ha il diritto di copiare dati, viene affrontato dalla legge sul copyright e viene oggi fatto rispettare con un'aggressività senza precedenti dall'industria dei media e dai governi sotto cui opera. Questo perché le aziende riconoscono che il copyright è il loro principale strumento per mantenere il controllo, e che affronta il cuore del loro problema: chi può copiare i dati che rappresentano il loro intero prodotto e valore commerciale. Anche i dati personali sono copiabili

soltanto da chi ne ha il diritto, a partire dalla sorgente di tali dati: l'individuo. Però non abbiamo la stessa documentazione legale dei nostri diritti, la stessa organizzazione per proteggerli, lo stesso zelo legale per farli rispettare, come fanno i proprietari dei dati aziendali. Il centro dell'intero problema è proprio qui: fare in modo che il nostro sistema legale protegga il nostro copyright sui nostri dati personali con, almeno, la stessa efficacia con la quale protegge i copyright sui dati aziendali. Dovrebbe essere più semplice, visto che le violazioni del copyright personale sono meno frequenti, meno costose per ogni singola violazione, e perpetrate da un gruppo di persone più piccolo in un sistema più centralizzato, un po' come le tradizionali violazioni di copyright nell'epoca precedente la condivisione di file nei sistemi peer-to-peer. Dovremmo ottenere una maggior protezione con un minor sforzo, molto prezioso per noi nel proteggere le nostre vite, più di quanto lo sia anche nella protezione di certi modelli di business passeggeri.

Il nostro copyright è per default una copia singola dei dati personali trasmessi al destinatario. Quella copia può essere duplicata e archiviata solo per la durata e l'ambito della transazione in cui è stata trasmessa. Una volta che quella transazione è completa, non può essere copiata o trattenuta; non può essere copiata per nessun altro destinatario (anche se è all'interno della stessa organizzazione) a meno che non sia strettamente necessaria per completare la transazione originaria. Non può, inoltre, essere archiviata al di là di tali restrizioni. L'ambito dei destinatari e della durata dell'archiviazione, impliciti nella definizione di quella transazione, possono essere richiesti dal mittente della copia, prima del trasferimento e della sua licenza limitata di copyright. Ogni distribuzione che va oltre quei limiti richiederà il permesso esplicito del mittente, e non è trasferibile oltre tale nuova transazione, con le stesse restrizioni della transazione originaria, che si rifletteranno sul nuovo ambito e sulla nuova durata. Un numero finito di gradi di separazione dal possessore del copyright può essere specificato nella transazione originaria, oppure richiesto in un secondo momento, oppure può essere emanata una licenza priva di limitazioni, ma il default è rappresentato dall'ambito e dalla durata del completamento della transazione originaria soltanto. Questi dati ci appartengono: hanno un valore quando vengono condivisi, e stiamo distribuendo un valore troppo grande quando li condividiamo senza restrizioni -- per non parlare del danno enorme quando una ulteriore condivisione (presupposta o meno) li diffonde a macchia d'olio.

Le regole basilari sono preposte per proteggere i nostri dati personali con la legge sul copyright. Le leggi europee sulla privacy già dimostrano come le aziende possano prosperare senza necessariamente avere un accesso completo ai dati personali di tutti. Le tipologie di furto di identità che stiamo sperimentando, come il crack di T-Mobile, o come gli scandali ChoicePoint e SIAC di cui si è saputo questo mese, stanno certamente contribuendo a un'ondata globale di richiesta di protezione dei diritti. Insieme allo spam, al phishing e ad altri tipi di furto di identità, c'è sicuramente il presupposto per un enorme supporto di pubblico ai fini di ottenere un mandato di protezione governativa che colpirebbe al cuore tutti questi attacchi. Il Copyright è già un diritto: occorre che il governo che paghiamo inizi a proteggerlo, e a proteggerci.

Da: Jake Appelbaum <jacob@appelbaum.net>
Oggetto: Hacking ai danni di T-Mobile

Verso la fine dello scorso anno, ero in contatto con il CSO di T-Mobile a causa di una grave falla nella loro piattaforma voicemail. Agli inizi di febbraio 2005 la vulnerabilità era ancora presente. Usando il mio sistema PBX personalizzato sono in grado di entrare in una qualsiasi delle loro caselle voicemail _per default_. Quando ho spiegato la cosa al loro CSO, egli mi disse che erano a conoscenza del problema, che non avevano intenzione di porvi rimedio in un intervallo di tempo ragionevole, e poi mi offrì un posto di lavoro. Ottenere un'offerta di lavoro che aveva tutta l'aria di essere un incubo mi fece un po' sorridere, ma come cliente ero esterrefatto.

Così ho svolto una piccola indagine su più di 30 compagnie di telefonia fissa e cellulare negli USA e nel Canada. Il risultato: T-Mobile era la più vulnerabile a questo tipo di exploit per quanto riguarda la sicurezza del sistema voicemail. Loro lo sanno e non gliene importa niente.

Come funziona è piuttosto semplice. Si tratta al tempo stesso di un attacco denial-of-service verso l'utente (che non può avere accesso alla propria voicemail finché la state usando voi) e di una grave violazione della privacy.

In ogni caso, falsificate l'ANI (Automatic Number Identification) del vostro bersaglio, chiamate il suo numero di accesso open tree e voilà, accesso garantito. Ora siete voi l'utente, e potete creare impostazioni, mandare messaggi impersonando qualcun altro e, sostanzialmente, avete il totale controllo dell'account. Assolutamente terribile.

Il CSO sembrava credere che la privacy e la sicurezza non vanno a braccetto; mi è sembrato minimizzare l'intero episodio come fosse una problematica di pura privacy soltanto.

Da: charles werbick <heihosha@yahoo.com>
Oggetto: La fine di Carnivore

L'FBI ha avuto un altro incentivo, oltre alla convenienza economica, per terminare Carnivore in favore di soluzioni software di terze parti per la sorveglianza via Internet.

Carnivore era soggetto a supervisione governativa. All'FBI era richiesto di stendere un rapporto trimestrale per il Congresso, descrivendo la natura e la portata delle loro attività di spionaggio via rete. Ora che Carnivore non c'è più, la sorveglianza continua senza alcuna supervisione. Quello da cui si sono realmente liberati sono gli occhi attenti dei nostri rappresentanti a Washington.

Da: Michael Hammer <MHammer@ag.com>
Oggetto: La maledizione della "Domanda Segreta"

La sua speranza che le cose sarebbero più difficili se si dimenticasse la risposta alla domanda segreta è in realtà una falsa speranza. Ho avuto di recente questa esperienza quando ho ricevuto la mia nuova carta AMEX. Quando ho visitato il sito per attivare la carta, ecco la "domanda segreta" (il compleanno di mia madre). Avendo precedentemente inserito una stringa casuale e non ricordandomi che cosa avessi scritto, ho dovuto chiamare il numero verde. Le stupide opzioni vocali automatizzate volevano che io inserissi il numero della carta e poi il compleanno di mia madre. Alla fine ho parlato con un operatore vero e proprio.

E qui arriva il bello. L'operatrice voleva sapere il mio indirizzo a scopo di verifica. Poi voleva il codice a 4 cifre sulla carta (quello sopra il numero della carta). Tutto qui.

Per cui se qualcuno avesse rubato la carta, avrebbe avuto la possibilità di attivarla semplicemente possedendola e sapendo il mio indirizzo (che è sulla custodia porta-carta).

Il processo diventa di gran lunga meno sicuro quando uno non conosce la risposta alla domanda segreta.

Da: Anonimo
Oggetto: Risposta a: Una banca denunciata per una transazione non autorizzata

Le banche non possono essere responsabili per clienti che non trattano le loro informazioni di login in maniera appropriata, nello stesso modo in cui uno staff IT non può essere responsabile per quegli utenti che divulgano le loro informazioni di login aziendale. Possiamo cercare una frode basata su molte cose, ma a parte verificare personalmente ogni transazione, non vedo alcuna soluzione ragionevole a questo problema. Vi sono delle tecnologie che permettono ai clienti di verificare elettronicamente le transazioni che stanno per applicare ai loro conti, ma il problema di queste tecnologie è che richiedono l'interazione con il cliente -- se questi non ferma la transazione, essa procederà; se non si autenticano quel giorno o non possono raggiungere un computer, allora le transazioni procederanno comunque.

Una transazione proveniente dal conto online di qualcuno appare legittima ai sistemi bancari se viene accompagnata da valide credenziali di autenticazione. La buona notizia è che queste transazioni possono essere tracciate e fatte risalire a indirizzi IP, che è senz'altro di aiuto nella ricerca di un crimine. Grandi banche come la BOA sono famose per non essere di aiuto nel caso un cliente subisca una frode sul proprio conto corrente, ma non tutte le banche si comportano così. La vera soluzione per le banche sarebbe quella di educare maggiormente i propri clienti in materia di sicurezza, anche se ciò comporterebbe tenere dei corsi e persino inserire nella pagina Web della banca il link a un sito di un certo esperto di sicurezza...

Da: "Steven Shaer" <steves@videosave.net>
Oggetto: Secure Flight

Lo scopo di Secure Flight è quello di proteggere l'industria delle compagnie aeree da un altro disastro che la danneggerebbe e che di conseguenza indebolirebbe l'intera nazione. Se accadesse un altro dirottamento come quello dell'11 settembre e un conseguente calo del traffico aereo, la già fragile industria delle compagnie aeree andrebbe in mille pezzi e smetterebbe di esistere così come la conosciamo. Non sarebbe una buona cosa. Spostare i terroristi verso i centri commerciali è un sistema per evitarlo.

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

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.