

implementa vive in un mondo ben diverso, dove nulla è perfetto e dove l'esperienza mostra come moltissimi sistemi crittografici vengano distrutti a causa di problemi che nulla hanno a che fare con la matematica. Questo libro riguarda i metodi di applicazione delle funzioni crittografiche in una situazione reale, in modo tale per cui si possa davvero ottenere un sistema sicuro.

Questo è il libro che avremmo voluto avere più di dieci anni fa quando iniziammo le nostre carriere nel mondo della crittografia. Esso riunisce le nostre esperienze su come progettare sistemi crittografici in modo corretto. In un certo senso si tratta di un seguito di "Applied Cryptography", ma è maggiormente incentrato su problemi pratici e su come costruire un sistema sicuro, piuttosto che sulla mera progettazione di un protocollo crittografico.

Nota: questo libro non è il mio libro sulla sicurezza generale di cui feci menzione nel numero di Crypto-Gram del novembre 2002. Quel libro sarà pubblicato il prossimo settembre da Copernicus Books.

Il sito web dedicato al libro (comprende l'indice e la prefazione):

<<http://www.counterpane.com/book-practical.html>>

Per ordinare il libro su Amazon:

<<http://www.amazon.com/exec/obidos/ASIN/047122894X/counterpane>>

Per ordinare la versione economica, sempre su Amazon:

<<http://www.amazon.com/exec/obidos/ASIN/0471223573/counterpane>>

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

Le ristampe di Crypto-Gram

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

Vulnerabilità di SNMP:

<<http://www.counterpane.com./crypto-gram-0203.html#1>> (originale)

<<http://www.communicationvalley.it/marzo02.htm#a1>> (traduzione in italiano)

La fattorizzazione di Bernstein: una svolta?

<<http://www.counterpane.com./crypto-gram-0203.html#6>> (originale)

<<http://www.communicationvalley.it/marzo02.htm#a7>> (traduzione in italiano)

Richard Clarke sulle lezioni sull'11 settembre:

<<http://www.counterpane.com./crypto-gram-0203.html#7>> (originale)

<<http://www.communicationvalley.it/marzo02.htm#a8>> (traduzione in italiano)

Realizzare una patch di sicurezza:

<<http://www.counterpane.com/crypto-gram-0103.html#1>>

Le assicurazioni e il futuro della sicurezza dei network:

<<http://www.counterpane.com/crypto-gram-0103.html#3>>

La "morte" degli IDS:

<<http://www.counterpane.com/crypto-gram-0103.html#9>>

SSL risolve il problema di sicurezza relativo al trasferimento di informazioni sensibili fra i browser e i web server. Principalmente, viene impiegato per proteggere transazioni con carte di credito; la gente è preoccupata che gli hacker possano rubare i numeri delle carte di credito mentre si naviga in rete. Ormai dovrebbe essere ovvio che gli hacker non rubano questi numeri uno alla volta, ma in blocco, nell'ordine del migliaio o addirittura del milione, irrompendo in reti malamente protette. Molti piccoli siti di e-commerce non si servono di SSL per proteggere le transazioni con carte di credito; anche qui, semplicemente, questo tipo di attacco non avviene.

Ammetto che la mia affermazione citata da Reuters è un po' un'esagerazione. SSL viene utilizzato per proteggere informazioni personali nelle comunicazioni fra clienti e banche on-line o società di intermediazione, fra impiegati e datori di lavoro, fra clienti e compagnie di assicurazione, ecc., ma SSL viene usato in larga misura per questioni di immagine. I veri rischi per i dati personali risiedono nei grandi database agli estremi, non nelle comunicazioni fra di loro. Non sto scartando SSL considerandolo irrilevante, ma non mi preoccuperei più di tanto nel caso venisse attaccato. La sicurezza è forte quanto l'anello più debole della catena, e SSL non è certo l'anello più debole.

Attacchi side-channel:

<<http://citeseer.nj.nec.com/rd/74014494%2C317736%2C1%2C0%2CDownload/http%3AqSqqSqwww.cs.berkeley.eduqSq%7EdawqSqpapersqSqsidechan-final.ps>>

La documentazione sulla ricerca:

<http://lasecwww.epfl.ch/memo_ssl.shtml>

L'articolo dell'agenzia Reuters:

<http://story.news.yahoo.com/news?tmpl=story&ncid=582&e=1&cid=582&u=/nm/20030221/wr_nm/tech_encryption_dc>

oppure <<http://tinyurl.com/7fpi>>

La discussione su Slashdot:

<<http://slashdot.org/article.pl?sid=03/02/20/1956229&mode=thread&tid=93&tid=172>> oppure <<http://tinyurl.com/7fpn>>

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

Il Canile: qualche altra azienda di crittografia

Sono continuamente sbalordito dalla quantità di queste fantomatiche aziende. Grazie a tutti coloro che mi hanno inviato i seguenti candidati alla rubrica del Canile.

Vadium Technology. Possiedono un one-time pad. Devo aggiungere altro?

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

PMC Ciphers. La descrizione della teoria è talmente intrisa di pseudo-crittografia che rende la lettura molto divertente. Le varie ipotesi vengono presentate come conclusioni. La ricerca attuale viene ignorata o esposta in maniera inesatta. Il primo link è uno studio tecnico con quattro riferimenti, tre dei quali scritti prima del 1975. Chi ha bisogno di trent'anni di ricerca crittografica quando si può avere la teoria della cifratura polimorfica?

<http://www.ciphers.de/products/polymorphic_cipher_theory.html>

<http://www.ciphers.de/products/bpp_disk.html>

hierocryptX Technologies. Il lungo file PDF che descrive la loro "teoria della cifratura polimorfica", sfortunatamente, non è più disponibile. Il sito web è ricco di dichiarazioni straordinarie - ma non circostanziate - riguardo a questa teoria. Ma che ha di così speciale

semplicemente scambiandosi i passaporti.

<<http://email.ni.com.au/Click?q=aa-gBTeQXUc2wTVI8iWEhuEcIDY>>

Potete giocare al "riconoscimento facciale automatico" anche a casa vostra. Qui vi sono due immagini di Khalid Shaikh Mohammed, recentemente arrestato. Si tratta della stessa persona?

<<http://a799.g.akamai.net/3/799/388/e7f109f5666287/www.msnbc.com/news/1808398.jpg>>

<<http://i.cnn.net/cnn/2003/WORLD/asiapcf/south/03/02/pakistan.arrests/story.ksmohammed.ap.jpg>>

Ancora su hacking e telefoni cellulari:

<<http://zdnet.com.com/2100-1105-986083.html>>

Il pioniere informatico, nonché campione della sicurezza informatica, Roger Needham è scomparso. Ne sentiremo la mancanza.

<<http://nytimes.com/2003/03/06/obituaries/06NEED.html>>

<<http://www.theregister.co.uk/content/4/29535.html>>

Due intraprendenti criminali giapponesi hanno usato sniffer per tastiere per raccogliere informazioni e password di conti bancari, e si sono serviti di queste informazioni per rubare 136.000 dollari.

<<http://wireservice.wired.com/wired/story.asp?section=Technology&storyId=669766>> oppure <<http://tinyurl.com/7fr2>>
<<http://www.yomiuri.co.jp/newse/20030307wo23.htm>>

Insieme a John Thompson, il CEO di Symantec, ho discusso sulla Strategia Nazionale per rendere sicuro il Cyberspazio nell'ambito del San Jose Mercury News. Il mio articolo non dovrebbe essere una novità per i lettori di Crypto-Gram:

<<http://www.bayarea.com/mld/mercurynews/5337537.htm>>

L'articolo di Thompson:

<<http://www.bayarea.com/mld/mercurynews/5337538.htm>>

** **

Le news di Counterpane

Schneier terrà il discorso di presentazione alla 2003 Computers, Freedom, and Privacy conference, a New York, il 2 aprile alle 8:30.

<<http://cfp2003.org/cfp2003/>>

Schneier terrà un discorso di presentazione all'IBM Almaden Institute Symposium on Privacy a San Jose. Parlerà del rapporto fra privacy e tecnologie. 10 aprile, ore 9:00. La registrazione è a inviti.

<<http://www.almaden.ibm.com/institute/>>

Schneier interverrà alla RSA Conference a San Francisco. Sarà moderatore della tavola rotonda dei Crittografi lunedì 14 aprile (ore 17 - 18). Mercoledì 16 aprile alle 9:00 interverrà sul tema "Security Proxies e Agenda" e giovedì 17 aprile alle 10:00 tratterà delle strategie su come concepire la sicurezza informatica.

<<http://www.rsaconference.net/rsa2003/>>

** **

Note di sicurezza da ogni dove: le formiche di bosco

La formica di bosco (*Pheidole dentata*) sopravvive in aree dominate da colonie di formiche di fuoco, malgrado queste colonie tendano ad essere cento volte più grandi e malgrado siano delle pessime "vicine di casa". Il trucco messo in atto dalla formica di bosco è il contrattacco: essa possiede una popolazione permanente (il 10% circa) di formiche di casta guerriera che non fanno altro che pattugliare accompagnando le formiche operaie. Ogni volta che queste formiche avvistano una formica di fuoco, esse la attaccano, poi mettono un po' del suo odore su se stesse e corrono a casa, lasciando una scia di quell'odore. Il formicaio viene messo in allarme, così come ogni altra formica operaia o guerriera che incrociano sulla via. Un gruppo numeroso di queste formiche di bosco arriva di lì a poco e uccide la formica di fuoco e poi si mette in cerca di possibili formiche di fuoco sopravvissute. Le formiche guerriere continueranno a circondare l'area per ore, cercando e uccidendo qualsiasi formica di fuoco che capiti a tiro. Concentrando al massimo ogni possibile sforzo in questo tipo di contrattacco, le formiche di bosco si assicurano che nessuna formica di fuoco possa tornare al proprio formicaio con informazioni accurate su dove vivono le formiche di bosco.

** *** *****

Contraffazione del brevetto SSL

Leon Stambler dichiara che almeno due dei brevetti U.S. in suo possesso comprendono il protocollo SSL. Ha spillato milioni di dollari a varie aziende con la minaccia di denunciarle. Ma VeriSign e RSA hanno deciso di combatterlo in tribunale, e hanno vinto la causa.

Questa causa è andata avanti per più di un anno, e molte persone mi hanno chiesto se i brevetti siano validi o meno. Ma in tutta onestà non ho avuto (e non ho ancora) la forza di leggere i brevetti veri e propri. Sono otto brevetti -- centinaia e centinaia di pagine scritte in un denso gergo giuridico. Vi sono più di un centinaio di dichiarazioni, alcune delle quali sono talmente generiche che possono essere applicate a qualsiasi protocollo di autenticazione. C'è voluta una falange di esperti in legge per venire a capo della questione, e sono lieto di affermare di non essere stato scelto -- e di non aver nessuna intenzione di esserlo -- da nessuno di loro.

Ma l'intera vicenda mi è sembrata sospetta. Stambler inizialmente consegnò la sua richiesta di brevetto nel 1992, ma alcuni dei brevetti non furono pubblicati prima del 1998 e del 1999. Il protocollo SSL fu sviluppato nel 1994 (il relativo brevetto venne assegnato nel 1997). Questo è ciò che viene chiamato "submarine patent" (lett. "brevetto sottomarino"), reso possibile da una caratteristica del sistema di brevetti statunitense chiamata "continuazione". Per qualsiasi tecnologia che si è brevettata, si tengono sempre uno o due brevetti "aperti", cioè li si mantiene nel processo di assegnazione di un brevetto. Quando si registra un brevetto, occorre redigere un documento di esposizione che ne descrive la tecnologia. Tale documento non può venire modificato in futuro, ma le rivendicazioni sui brevetti sì. Ed è piuttosto semplice ritardare il processo di registrazione di un brevetto grazie ad espedienti procedurali. Così si ritardano alcuni brevetti di "continuazione" (estensioni del proprio brevetto iniziale). Ora supponete di notare qualcosa di molto differente da ciò che si è brevettato, ma collegato ad esso in qualche modo (come il protocollo SSL). Si cercherà dunque di riscrivere le rivendicazioni del brevetto di "continuazione" per far rientrare questo nuovo elemento. Far approvare le nuove rivendicazioni è un processo di negoziazione fra voi e l'ufficio brevetti, e l'ufficio brevetti non è necessariamente a conoscenza di ciò che state cercando di ottenere, per cui è assai probabile far approvare quelle rivendicazioni. Di seguito si registra il brevetto di "continuazione", unitamente alle rivendicazioni che coprono direttamente quel nuovo elemento, e poi si minacciano denunce.

L'esame di un brevetto non è segreto; ciò che viene chiamato il faldone del brevetto contiene tutte le bozze, la corrispondenza e ogni altra documentazione cartacea legata al brevetto prima che fosse registrato. Chiunque può ottenere un faldone relativo ad ogni brevetto registrato dall'ufficio brevetti, anche se occorre essere preparati a pagare una certa cifra in fotocopie, visto che alcuni incartamenti possono essere costituiti da migliaia di pagine.

alle persone di prepararsi a correre velocemente ai ripari per quanto concerne quella vulnerabilità. Per esempio: aspettatevi una patch alla JVM di Internet Explorer in 4 settimane, la natura dell'impatto potrebbe essere X, Y, Z. Ciò potrebbe dare tempo alle persone di trovare risorse per risolvere il problema e di prendere decisioni in merito ai rischi connessi all'attuare i controlli, senza però offrire all'opinione pubblica un accesso troppo vasto ai dettagli, che solleciterebbe gli exploit prima della riduzione dell'esposizione. Anche se, lo ammetto, se i dettagli diventassero tentatori, questo porterebbe ad una richiesta di esposizione totale.

Come spesso accade, un ambiente normale è formato da sfumature di grigio; diventa bianco e nero quando lo si divide in diverse dimensioni.

Da: Ben Day <day@programmer.net>
Oggetto: Serrature ed Esposizione Totale

Intendevo commentare in merito alla sua analogia fra le vulnerabilità dei sistemi a passe-partout e i paradigmi di sicurezza digitale, di cui si è fatto portavoce. Se da una parte trovo del tutto persuasivo il caso della sicurezza elettronica "open source" (se mi è permesso chiamarlo così), dall'altra vi sono alcuni problemi nell'applicazione di questo modello alla sicurezza "fisica". Ciò non significa necessariamente che io non sia d'accordo con la sua critica sull'affidamento della segretezza nella comunità dei fabbri, tuttavia non credo che avrebbe gli stessi benefici risultati che ha nel mondo della sicurezza digitale, vale a dire costringere le persone a servirsi di meccanismi di sicurezza migliori e meno penetrabili; questo a causa delle eventualità insite nella sicurezza delle serrature. Mi spiego meglio.

Lo studio di Matt Blaze credo sia meno interessante di quel che sembra: le serrature sono incredibilmente facili da scassinare -- chiunque può trovare on-line la famosa guida MIT per scassinatori ad opera di "Ted the Tool" e, dopo un'ora o due di pratica, può iniziare a forzare porte e lucchetti con l'aiuto di oggetti casalinghi. Le serrature dotate di passe-partout sono ancora più semplici da scassinare, dato che molti dei piedini sono solitamente tagliati in due punti e possono quindi essere posizionati da ambo i lati del taglio. Lisciare una specifica chiave per ottenere un passe-partout è come accendersi una sigaretta con un lanciafiamme quando si ha in tasca un accendino, anche se sono sicuro che siano state fatte entrambe le cose, a scopo di intrattenimento.

Per quanto riguarda l'analisi di Blaze (e la sua) sulla vulnerabilità, però, le cose si complicano quando ci chiediamo PERCHÉ il 90% delle serrature sono cilindri e sono così semplici da scassinare (o da aggirare usando altri trucchi, come lo schema a passe-partout), quando esistono meccanismi di chiusura essenzialmente impenetrabili e resistenti ad altri exploit di tipo non distruttivo. La risposta è: VENGONO INTENZIONALMENTE COSTRUITE PER ESSERE FORZATE. Lei e Blaze fate l'errore cruciale di assumere che lo scopo delle serrature sia quello di impedire l'ingresso senza l'apposita chiave, ma nella realtà dei fatti, nella maggior parte dei casi le serrature vengono costruite in modo che possano essere aperte -- da persone provviste di una certa abilità, ma senza doti particolarmente rare -- anche senza una chiave. Questo avviene semplicemente perché la gente vuole evitare che le serrature di casa propria o del proprio armadietto a scuola vengano perforate e sostituite ogni volta che qualcuno smarrisce le chiavi o si chiude dentro. Moltissime automobili costruite dagli anni Novanta in poi montano delle serrature di tipo Illco non scassinabili (queste ricevono le chiavi con protuberanze morbide e arrotondate invece di denti aguzzi o squadrati) -- ma ciò accade perché quando si chiudono dentro l'auto le proprie chiavi, nessuno penetra nella vettura forzando la serratura, ma agisce direttamente sulla portiera. Se venissero eliminate le scappatoie con le quali si possono forzare le portiere delle auto, le garantisco che le serrature diverrebbero scassinabili - le automobili, paradossalmente, devono essere costruite in modo tale che sia possibile penetrarvi.

È a questo punto che l'approccio "open source" diventa insidioso. Se lo scassinare serrature dovesse diventare "di dominio pubblico" nel senso di un know-how esteso a tutti (in modo che

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza informatica 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 la rivista interessante. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è il fondatore e CTO di Counterpane Internet Security, Inc., autore di "Secrets and Lies" e di "Applied Cryptography" e inventore degli algoritmi Blowfish, Twofish e Yarrow. È membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia.

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 Counterpane Internet Security, Inc.