

2) La crittografia di comunicazioni telefoniche non è molto efficace. Ogni volta che le forze dell'ordine hanno trovato della crittografia, non hanno avuto problemi ad aggirarla. Presumo che i locali commissariati di polizia non abbiano, per fare un esempio, i mezzi per decodificare chiavi DES con attacchi brute-force. Ritengo quindi che in quei casi la crittografia vocale sia stata piuttosto facile da aggirare.

Questi due punti possono essere facilmente spiegati dal fatto che i telefoni sono dispositivi chiusi. Gli utenti non possono scaricare del software al loro interno come si fa con i computer. Nessuno può scrivere un programma gratuito di crittografia per telefoni. Perfino i produttori di software considererebbero troppo costoso aggiungere una funzionalità del genere per un sistema telefonico che non per un sistema informatico.

Questo significa che la sicurezza telefonica è un campo ristretto. I telefoni criptati sono costosi. Questi telefoni sono realizzati da aziende che credono nella segretezza. La crittografia telefonica non viene sottoposta ad esami critici; il software non è soggetto a peer review (la valutazione da parte di un comitato di esperti in fase di pre-release, ndr). Il fatto che il risultato sia una ristretta serie di prodotti per la sicurezza telefonica costosi e mediocri non dovrebbe sorprendere.

Per decenni si è discusso se l'apertura sia un bene o un ostacolo alla sicurezza. Per noi esperti di sicurezza è ovvio che la segretezza danneggia la sicurezza, ma risulta così poco immediato per l'opinione pubblica che dobbiamo continuamente difendere la nostra posizione. Questo rapporto sulle intercettazioni dimostra incontrovertibilmente che il pensare alla sicurezza mediante una metodologia chiusa -- cioè il realizzare prodotti di sicurezza con il classico atteggiamento "fidatevi di noi perché sappiamo queste cose" -- non funziona. Il governo degli Stati Uniti non ha trovato alcun prodotto per la crittografia telefonica che non sia stato in grado di superare.

Il testo del rapporto:

<<http://www.uscourts.gov/wiretap02/2002wttxt.pdf>>

Il mio articolo su segretezza e sicurezza:

<<http://www.counterpane.com./crypto-gram-0205.html#1>>

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

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.

Segretezza, sicurezza e oscurità:

<<http://www.counterpane.com./crypto-gram-0205.html#1>> (originale)

<<http://www.cryptogram.it/maggio02.htm#a1>> (traduzione in italiano)

Ingannare i rilevatori di impronte digitali:

<<http://www.counterpane.com./crypto-gram-0205.html#5>> (originale)

<<http://www.cryptogram.it/maggio02.htm#a5>> (traduzione in italiano)

Che cosa può insegnare alla sicurezza della rete la storia militare, seconda parte:

<<http://www.counterpane.com/crypto-gram-0105.html#1>>

L'inutilità della protezione dalla copia digitale:

<<http://www.counterpane.com/crypto-gram-0105.html#3>>

Se lo scenario riguardante gli abusi postali scaturito da Slashdot è una cosa divenuta possibile solo di recente, è invece da molto più tempo che si possono molestare gli abbonati telefonici che possiedono fax automatici. Provate ad inserire "request catalog fax" o "request whitepaper fax".

Da: "Stéphane Doyon" <s.doyon@videotron.ca>
Oggetto: L'intervento umano come misura di sicurezza

Dallo scorso numero di Crypto-Gram: -- Le singole compagnie che producono questi cataloghi potrebbero tutelarsi aggiungendo una verifica ai propri form che richieda un intervento umano. L'idea è quella di aggiungere un passaggio che una persona può compiere tranquillamente, ma non una macchina. La tecnica più diffusa è quella di produrre un'immagine di testo che la tecnologia OCR non riesca a riconoscere, ma l'occhio umano sì, e di richiedere che il testo visualizzato venga ricopiato all'interno del form. Questi sistemi hanno cominciato ad apparire in vari siti Web per evitare proprio le registrazioni in automatico. Li ho visti, ad esempio, su Yahoo e PayPal. --

Vorrei però far notare che questa tecnica è assai frustrante per chi, come me, è un non vedente. Si tratta dell'ennesima barriera all'accessibilità del web. (Ovviamente non faccio molti ordini di cataloghi cartacei, ma questa tecnica mi ha bloccato un paio di volte per altre transazioni...).

Da: "Steven M. Bellovin" <smb@research.att.com>
Oggetto: Sicurezza nei campi da gioco

Dallo scorso numero di Crypto-Gram: -- Un paio di settimane fa stavo ascoltando una partita di baseball alla radio. Lo speaker stava parlando delle nuove misure di sicurezza antiterrorismo in vigore dentro al campo di gioco. Una di esse, ha detto, proibisce agli spettatori di portare con sé bottiglie e lattine all'interno dello stadio. --

Ritengo che questa sia una valida misura di sicurezza, ma il terrorismo non c'entra. Si sta cercando di proibire alle persone di introdurre oggetti piccoli e pesanti che possono essere facilmente lanciati -- un problema che si è già manifestato. (Alcuni anni fa, quando John Rocker era "ospite non gradito" fra i tifosi dei New York Mets, l'arma preferenziale erano le pile).

La non comprensione del modello di minaccia può far sembrare assurdi molti rischi di sicurezza. Immaginatoci che cosa possa pensare del blinding step della RSA uno che non ha mai sentito parlare di timing attacks.

Da: Erwann Abalea <erwann.abalea@certplus.com>
Oggetto: Sicurezza nei campi da gioco

Questo tipo di misura di sicurezza è già stato applicato in Francia, e forse anche in Inghilterra, negli stadi di calcio. Il problema riguarda davvero la sicurezza e non è tanto legato al controllo di un mercato, dato che in quegli stadi non vengono vendute bevande. Il problema è che certi hooligan usano bottiglie, lattine e altri simili oggetti per colpire le altre persone, oppure li lanciano verso il campo da gioco per colpire i giocatori o gli arbitri.

Da: "Jon Woodcock" <jpwoodcock@yahoo.co.uk>
Oggetto: Ordini di priorità non legati alla sicurezza

Il suo pezzo sul baseball mi ha fatto venire in mente un altro abuso dell'argomento "terrorismo" per giustificare azioni motivate da ordini di priorità tutti personali. Il sindaco di Chicago ha recentemente disposto la chiusura di un aeroporto locale che non era di suo gradimento: la sua giustificazione: "sicurezza nazionale". La saga continua all'indirizzo: <<http://www.aopa.org/whatsnew/newsitems/2003/030403meigs.html>>

Da: "Vladimir G. Ivanovic" <vladimir@acm.org>
Oggetto: Sicurezza negli aeroporti

<<http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05jan03-e.pdf>>
oppure <<http://tinyurl.com/9c46>>

Dopo aver letto la prima sessantina di pagine del rapporto, mi stupisce che le indicazioni della Commissione possano essere di un qualche effetto contro le minacce di sicurezza (aeroplani come missili) di ieri. Le minacce di ieri hanno avuto successo perché le procedure di sicurezza in vigore al momento erano pensate per essere efficaci contro minacce ancora più vecchie (dirottamenti). Qui qualcosa non va.

Se fossi un terrorista, non utilizzerei affatto dei taglierini. Proverei con qualcosa di diverso. Anzi, perché prendere di mira gli aerei? Una nave da crociera, uno stadio, un ponte con il traffico dell'ora di punta, uno stabilimento chimico, tutti questi bersagli sarebbero ottimi per le prime pagine dei giornali.

Da: Nathan Rosenblum <flander@smurf.to>
Oggetto: Il signor al-Hussayen

Dallo scorso numero di Crypto-Gram: -- Simpatizzanti dei terroristi sauditi studiano la sicurezza informatica nelle università americane. "Dopo aver studiato nel Texas e nell'Indiana, al-Hussayen ha iniziato il programma dottorale dell'Università dell'Idaho in informatica nel 1999, con una specializzazione in sicurezza informatica e tecniche di intrusione, secondo le accuse".

<<http://www.washingtonpost.com/wp-dyn/articles/A12758-2003Mar11.html>> --

Indicare il signor al-Hussayen come un "simpatizzante di terroristi" è improprio. Tutt'al più, Sami è sospettato di aver a che fare con organizzazioni che contribuiscono al terrorismo. Si dovrebbe notare che le accuse vere e proprie contro di lui parlano di violazioni inerenti al visto e partono dal fatto che egli, presumibilmente, non abbia indicato appartenenza ad alcuna organizzazione quando ha fatto richiesta di visto. In più, egli è accusato di aver lavorato per la IANA durante i suoi studi all'Università dell'Idaho (a chi possiede un visto per studenti non è permesso svolgere nessuna attività al di fuori dell'ambito di studio).

Se da una parte faccio fatica a credere che il mio ex collega abbia coscientemente aiutato un'organizzazione di supporto al terrorismo tramite le presunte transazioni finanziarie o attraverso lo sviluppo di siti web, d'altra parte non è un fatto così impossibile. Ad ogni modo, credo sia più corretto scrivere "sospettato" e non "simpatizzante di terroristi". Anche se Sami al-Hussayen fosse condannato sulla base delle accuse contro di lui, e fosse costretto a partire per l'Arabia Saudita con la sua famiglia, non sarebbe comunque possibile caratterizzarlo come un "simpatizzante di terroristi" su quelle basi. Sami non verrà processato sulla base di accuse legate al terrorismo.

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

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.