

CRYPTO-GRAM
15 gennaio 2009

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA
<<http://www.communicationvalley.it/>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<<http://www.schneier.com/crypto-gram-0703.html>>.

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier "Schneier on Security": <<http://www.schneier.com/blog>>.

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

- La sostituzione di persona
- News
- Falsificare certificati SSL
- Le news su Schneier
- I dati biometrici
- Commenti dei lettori

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

La sostituzione di persona

La sostituzione di persona non è un fenomeno nuovo. Nel 1556 un francese fu giustiziato per aver impersonato Martin Guerre, e di recente degli hacker hanno impersonato Barack Obama su Twitter. La sostituzione di persona non è nemmeno un atteggiamento riservato unicamente agli esseri umani: i tordi, le farfalle Viceroy, e il polpo imitatore (*Thaumoctopus mimicus*) ne fanno uso come tattica di sopravvivenza. Per quanto riguarda gli esseri umani, rilevare una sostituzione di persona è un problema arduo per tre motivi: occorre verificare l'identità delle persone che non conosciamo; interagiamo con altre persone attraverso canali di comunicazione 'stretti'

come il telefono e Internet; e vogliamo che siano sistemi automatizzati a svolgere il compito della verifica al posto nostro.

La classica sostituzione di persona è un inganno commesso da alcune persone ai danni di altre. È pratica tuttora diffusa: si impersonano gli addetti alla nettezza urbana per raccogliere mance, o addetti ai parcheggi pubblici per raccogliere i pedaggi, o si impersona il presidente francese per ingannare Sarah Palin. Impersonare figure quali poliziotti, guardie giurate e funzionari che leggono i contatori è una tattica criminale assai comune.

Questi trucchi funzionano perché tutti noi abbiamo a che fare regolarmente con persone che non conosciamo. Nessuno potrebbe sostituirsi a vostro fratello, al vostro migliore amico o al vostro capo facendola franca, perché conoscete molto bene queste persone. Ma un poliziotto o un addetto al parcheggio? Si tratta semplicemente di qualcuno con un cartellino o un'uniforme. Ma cartellini e tesserini identificativi servono soltanto se si è in grado di verificarli. Sapete esattamente come si presenta un vero tesserino identificativo della polizia? Sapete come distinguere il cartellino di un vero riparatore dell'azienda telefonica rispetto a un documento contraffatto?

Eppure è nella natura umana fidarsi di queste credenziali. Abbiamo una fiducia naturale verso le uniformi, pur sapendo che chiunque potrebbe indossarne una. Quando visitiamo un sito Web, ci serviamo della professionalità della pagina per giudicare se è o non è davvero legittima, anche se chiunque è in grado di tagliare e incollare elementi grafici. Osservate la prossima volta che qualcuno (che non appartenga alle forze dell'ordine) verifica i vostri documenti: moltissime persone li guardano appena.

La sostituzione di persona è ancor più facile quando viene attuata attraverso canali di comunicazione limitati. Al telefono, come è possibile capire se si sta comunicando con qualcuno dell'azienda della vostra carta di credito o con un malvivente che sta cercando di carpire gli estremi del vostro conto e le informazioni di login dell'account? Per email, come è possibile distinguere qualcuno del supporto tecnico della vostra azienda da un hacker che sta cercando di penetrare nella rete aziendale? E come distinguere il sindaco di Parigi da un impostore? Di tanto in tanto qualcuno si scarcera da solo inviando per fax un ordine di rilascio contraffatto. Questa è ingegneria sociale: impersonare qualcuno in modo abbastanza convincente da ingannare la vittima.

Oggigiorno, una gran parte della verifica di identità viene fatta davanti a un computer. I computer sono molto veloci a effettuare calcoli, ma non sono molto efficaci a livello di giudizio e valutazione, e possono venire ingannati. Pertanto è possibile ingannare gli autovelox appiccicando una targa fasulla sopra quella vera, è possibile ingannare i lettori di impronte digitali con un pezzo di scotch, o gli scanner facciali automatizzati utilizzando (no, non me lo sto inventando) la fotografia di un volto messa davanti al proprio. Persino il poliziotto più annoiato non si lascerebbe ingannare da nessuno di questi trucchi.

È per questo che il furto d'identità è un così grave problema oggi. Moltissima autenticazione avviene online e con pochissime informazioni: nome utente, password, data di nascita, numero di Previdenza Sociale, e così via. Chiunque ottenga quelle informazioni può farsi passare per voi di fronte a un computer, che non è in grado di distinguere fra verità e inganno.

Malgrado tutti questi problemi, moltissimi sistemi di autenticazione funzionano la maggior parte del tempo. Funzionano persino cose ridicole come le firme via fax, e possono essere legalmente vincolanti. Ma nessun sistema di autenticazione è perfetto, ed è sempre possibile attuare una sostituzione di persona.

Tale mancanza di perfezione, tuttavia, è accettabile. La sicurezza è un compromesso, e ogni sistema di autenticazione ben progettato mantiene un equilibrio fra sicurezza, facilità d'uso, approvazione del cliente, costi, e così via. Un maggior livello di autenticazione non è sempre il meglio. Le banche accettano questo compromesso quando non si prendono nemmeno la briga di autenticare le firme di assegni per somme inferiori a 25.000 dollari; è più economico gestire la frode dopo il fatto. I siti Web accettano il compromesso quando si servono di password semplici invece di un sistema più sicuro; e i commercianti accettano il compromesso quando non si prendono il disturbo di verificare la vostra firma con quella presente sulla carta di credito. Noi accettiamo questo compromesso quando ci fidiamo di tesserini di polizia, di uniformi della catena Best Buy, di firme inviate per fax, effettuando una verifica rapida e superficiale.

I buoni sistemi di autenticazione, inoltre, mantengono un equilibrio tra falsi positivi e falsi negativi. La sostituzione di persona è soltanto una delle tante maniere per cui questi sistemi possono fallire; possono anche fallire nell'autenticare la vera persona. È meglio che uno sportello Bancomat permetta la frode occasionale piuttosto che impedire ai legittimi correntisti l'accesso al loro denaro. D'altro canto, un falso positivo in un sistema di lancio nucleare è molto più pericoloso: meglio non lanciare i missili.

I sistemi di autenticazione decentralizzati funzionano meglio di quelli centralizzati. Aprite il portafoglio e noterete una gran varietà di oggetti che vengono utilizzati per identificarvi presso varie persone e organizzazioni: la vostra banca, la vostra compagnia di carta di credito, la biblioteca, la palestra, il vostro datore di lavoro; più la patente di guida, documento usato per identificarvi nelle circostanze più disparate. Tutto questo assortimento di tessere è in effetti più sicuro di un'unica carta di identità centralizzata: ogni sistema deve essere penetrato individualmente, e riuscire a penetrare in uno di essi non dà all'aggressore un accesso completo a tutti gli altri. Questa è una delle ragioni per cui sistemi centralizzati come REAL-ID ci rendono meno sicuri.

Infine, ogni buon sistema di autenticazione utilizza meccanismi di difesa in profondità. Dato che nessun sistema di autenticazione è perfetto, devono esservi misure di sicurezza alternative nel caso l'autenticazione non vada a buon fine. È per questo che tutte le risorse e le informazioni di una azienda non sono accessibili da chiunque riesca a introdursi negli uffici dell'azienda con l'inganno. È per questo che le compagnie di carte di credito possiedono sistemi sofisticati che analizzano schemi di spesa sospetti. Ed è per questo che il furto di identità non verrà risolto rendendo le informazioni personali più difficili da rubare.

Possiamo ridurre il rischio derivato dalla sostituzione di persona, ma il problema sarà sempre con noi; la tecnologia non può 'risolverlo' in maniera assoluta. Come qualsiasi tipo di sicurezza, il trucco è quello di equilibrare i compromessi. Se la sicurezza è troppo scarsa, i criminali ritireranno il denaro da tutti i nostri conti correnti. Se la sicurezza è eccessiva, quando Barack Obama telefona per congratularsi con voi per la vostra rielezione, non crederete che sia davvero lui.

Questo articolo è originariamente apparso sul sito del Wall Street Journal:
<<http://online.wsj.com/article/SB123125633551557469.html>>

Martin Guerre:
<http://en.wikipedia.org/wiki/Martin_Guerre>

L'account Twitter di Obama:
<<http://bits.blogs.nytimes.com/2009/01/05/twitter-hit-by-hacker-phishers/>>
oppure <<http://tinyurl.com/9sasw5>>

Un video sul polpo imitatore:
<http://news.nationalgeographic.com/news/2001/09/0920_octopusmimic.html>

Impersonare gli addetti alla nettezza urbana:
<<http://pauldotcommunity.blogspot.com/2008/12/identifying-garbage-men.html>>
oppure <<http://tinyurl.com/5e6b92>>

Impersonare gli addetti ai parcheggi:
<<http://www.jsonline.com/watchdog/pi/36196199.html>>

Impersonare il presidente francese:
<http://news.bbc.co.uk/2/hi/americas/us_elections_2008/7704666.stm>
<<http://news.scotsman.com/world/Full-transcript-Canadian-radio-comedians.4652956.jp>>
oppure <<http://tinyurl.com/94b87y>>

Impersonare poliziotti:
<http://www.schneier.com/blog/archives/2006/01/forged_credenti.html>

Impersonare guardie di sicurezza:
<http://www.schneier.com/blog/archives/2006/05/thief_disguises.html>

Impersonare chi legge i contatori:
<http://query.nytimes.com/gst/fullpage.html?res=9E0CE0D61031F932A35752C1A964958260&_amp>
oppure <<http://tinyurl.com/8r2yoa>>

Fidarsi delle uniformi:
<http://www.schneier.com/blog/archives/2006/05/people_trusting.html>

Impersonare il sindaco di Parigi:
<<http://www.nytimes.com/2008/12/22/opinion/l22kennedy.html>>

Inviarsi via fax un ordine di rilascio contraffatto dalla prigione:
<http://www.schneier.com/blog/archives/2004/11/hacking_faxes.html>

Ingannare gli autovelox:
<<http://www.thesentinel.com/302730670790449.php>>
<<http://www.thenewspaper.com/news/26/2632.asp>>

Ingannare i lettori di impronte digitali:

<<http://www.smh.com.au/travel/woman-fools-japans-airport-security-fingerprint-system-20090102-78rv.html>>

oppure <<http://tinyurl.com/8rdpkj>>

<http://news.yahoo.com/s/afp/20090101/wl_asia_afp/japantechnologyimmigrationcritecurity;_ylt=Aq2hpP614KymOfmXOljiBJ9vaA8F>

oppure <<http://tinyurl.com/8xcakm>>

Ingannare gli scanner facciali:

<http://news.cnet.com/8301-17938_105-10110987-1.html>

Le firme via fax:

<http://www.schneier.com/blog/archives/2008/06/fax_signatures_1.html>

Impersonare i dipendenti della catena Best Buy:

<http://www.schneier.com/blog/archives/2006/05/people_trusting.html>

REAL-ID:

<<http://www.schneier.com/testimony-realid.html>>

Risolvere il furto di identità:

<<http://www.schneier.com/essay-153.html>>

Non credere che si tratti davvero di Barack Obama:

<http://news.bbc.co.uk/2/hi/also_in_the_news/7765574.stm>

<<http://cnews.canoe.ca/CNEWS/WeirdNews/2008/12/04/7628706-ap.html>>

<<http://althouse.blogspot.com/2008/12/hip-to-prank-calls-congresswoman-ileana.html>>

oppure <<http://tinyurl.com/7gq7ks>>

<<http://www.wayodd.com/florida-congresswoman-hangs-up-on-obama-twice-thought-call-was-prank/v/9899/>>

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

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

News

Un articolo davvero interessante sui cecchini.

<http://www.theregister.co.uk/2008/11/28/sniper_feature/>

Allarmismo terroristico: acquistare console Nintendo fasulle aiuta i terroristi:

<http://www.schneier.com/blog/archives/2008/12/buying_fake_nin.html>

Come riconoscere una console Nintendo fasulla:

<http://news.bbc.co.uk/cbbcnews/hi/newsid_7760000/newsid_7767100/7767188.stm>

oppure <<http://tinyurl.com/8a6ult>>

Sono molto combattuto per quanto riguarda questa proposta di addestrare le forze di polizia di New York all'uso di mitragliatrici. Da una parte, mettere in campo questo tipo

di armi non mi sembra una grande idea. Dall'altra, l'addestramento non è mai una cosa negativa.

<http://www.nypost.com/seven/12082008/news/regionalnews/city_cops_prep_for_mu_mbai_143196.htm>

oppure <<http://tinyurl.com/5cwlhw>>

Ottimi commenti di Ed Felten sullo screening comportamentale della TSA:

<<http://freedom-to-tinker.com/blog/felten/low-hit-rate-isnt-problem-tsa-screening>>

oppure <<http://tinyurl.com/4xogro>>

Delle aziende brasiliane di taglio e trasporto legname assoldano hacker per alterare i limiti entro i quali è possibile deforestare:

<http://www.theregister.co.uk/2008/12/12/brazil_hackers_deforestation/>

Brillanti 'dead drop' (nascondigli dove depositare informazioni) utilizzando i DNS:

<http://landonf.bikemonkey.org/code/security/DNS_Dead_Drop.20060128201048.26517.luxo.html>

oppure <<http://tinyurl.com/4r7vrv>>

<http://landonf.bikemonkey.org/code/security/A_Better_DNS_Dead_Drop.20080107.html>

oppure <<http://tinyurl.com/4g9rat>>

Questa intervista con James Bamford sulla NSA merita una lettura:

<<http://sacurrent.com/news/story.asp?id=69490>>

Stesso dicasi per il suo nuovo libro:

<<http://www.amazon.com/exec/obidos/ASIN/0385521324/counterpane/>>

Come aggirare i checkpoint di sicurezza negli aeroporti:

<http://www.schneier.com/blog/archives/2008/12/bypassing_airpo.html>

Un buon articolo sulla paura della 'allergia da noccioline' e sulle reazioni esagerate:

<<http://news.bbc.co.uk/1/hi/health/7773210.stm>>

Nei commenti sul mio blog la discussione è vivace:

<http://www.schneier.com/blog/archives/2008/12/nut_allergy_fea.html>

Dilbert sulla sicurezza informatica:

<<http://www.dilbert.com/strips/comic/2008-12-07/>>

Una vignetta sulla sicurezza - contromisure eccessivamente specifiche alle conferenze stampa del presidente Bush:

<<http://www.news.com.au/common/imagedata/0,,6404759,00.jpg>>

Il Messico vuole creare un registro di tutti i possessori di telefoni cellulari. Quanto è facile rubare un cellulare? In generale, non mi impressionano favorevolmente quelle misure di sicurezza (specie se costose) il cui unico effetto è un cambio di tattica da parte dei malviventi.

<http://www.blacklistednews.com/?news_id=2602>

Sembra che non sia possibile parlare di 'impronte vocali':

<<http://dsc.discovery.com/news/2008/12/04/voice-print-tech.html>>

Reality show sul Dipartimento per la Sicurezza Nazionale sulla rete ABC. Ho visto parte di un episodio: propaganda pura.

<<http://abc.go.com/primetime/homelandsecurity/index>>

Confronto tra la sicurezza delle slot machine elettroniche e delle macchine per il voto elettronico:

<<http://media3.washingtonpost.com/wp-dyn/content/graphic/2006/03/16/GR2006031600213.gif>>

oppure <<http://tinyurl.com/f4an8>>

Altre importanti differenze:

1) Le slot machine vengono utilizzate ogni giorno, 24 ore al giorno. Le macchine per il voto elettronico vengono impiegate al massimo due volte l'anno; spesso anche meno di frequente.

2) Le slot machine hanno a che vedere con il denaro. Le macchine per il voto elettronico si riferiscono a qualcosa di più astratto.

3) La precisione delle slot machine è una questione imparziale. Per qualche motivo che non riesco a comprendere, la precisione delle macchine per il voto elettronico viene vista come una questione politica.

Appena desegretato dalla NSA, questo documento - A History of U.S. Communications Security (Volumes I and II); the David G. Boak Lectures, National Security Agency (NSA), 1973 [Storia della sicurezza delle comunicazioni USA in due volumi] - merita assolutamente di essere letto. Le prime sezioni sono pesantemente corrette, ma il resto è affascinante.

<http://www.governmentattic.org/2docs/Hist_US_COMSEC_Boak_NSA_1973.pdf>

Un altro documento recentemente rilasciato dalla NSA: "American Cryptology during the Cold War" (Criptologia americana durante la Guerra Fredda), di Thomas R. Johnson.

<<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/index.htm>>

La NSA sulle origini della NSA:

<<https://www.nsa.gov/publications/publi00015.cfm>>

Un brevetto della NSA sul rilevamento delle manomissioni di rete:

<<http://www.itworld.com/networking/59610/nsa-patents-way-spot-network-snoops>>

oppure <<http://tinyurl.com/8gh47c>>

<<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fmetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=%22%09+Reifer%22&OS=%22>>

oppure <<http://tinyurl.com/a7xc3x>>

"Securing Cyberspace for the 44th Presidency" (Proteggere il cyberspazio per la 44esima presidenza) a cura del CSIS (Center for Strategic and International Studies).

<http://www.csis.org/component/option,com_csis_pubs/task,view/id,5157/>

Per mancanza di fondi, le telecamere a circuito chiuso non vengono controllate. Questo non deve sorprendere affatto: quando il denaro scarseggia, cose come queste non vengono finanziate. Forse la sorpresa più grande è che la gente pensava che le telecamere a circuito chiuso fossero costantemente monitorate -- in genere non lo sono.

<<http://www.dailymail.co.uk/news/article-1095609/Big-brother-NOT-watching-Cash-strapped-towns-leave-CCTV-cameras-unmonitored.html?ITO=1490>>
oppure <<http://tinyurl.com/5wwdwd>>

Va bene portare a bordo di un aereo della polvere da sparo; basta metterla in un sacchetto di plastica trasparente e diventa magicamente sicura:
<<http://wildbee.org/2008/12/09/carrying-gunpowder-through-airport-security/>>
oppure <<http://tinyurl.com/9tctyg>>

Il taccheggio sta aumentando in questi tempi di crisi economica:
<<http://www.nytimes.com/2008/12/23/us/23shoplift.html>>

O forse no:

<<http://www.slate.com/id/2207504/>>

Ecco un elenco degli oggetti rubati più di frequente: piccole cose costose di lunga durata.

<http://www.schneier.com/blog/archives/2005/06/organized_retai.html>

Matthew Alexander è un ex inquisitore delle Forze Speciali che ha operato in Iraq nel 2006. Il suo pezzo d'opinione sulla tortura è lettura obbligatoria:

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/11/28/AR2008112802242.html>>

oppure <<http://tinyurl.com/648nge>>

Anche questa intervista di Harper's:

<<http://harpers.org/archive/2008/12/hbc-90004036>>

Estratti:

<http://www.schneier.com/blog/archives/2008/12/matthew_alexand.html>

Un'altra intervista:

<<http://paulharrisonline.blogspot.com/2008/12/how-to-break-terrorist.html>>

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

Piano di preparazione al bioterrorismo del CDC del 1999:

<<http://www.cdc.gov/ncidod/dhqp/pdf/bt/13apr99APIC-CDCBioterrorism.PDF>>

Dati reali sui programmi di sicurezza software.

<<http://www.informit.com/articles/article.aspx?p=1315431>>

La contraffazione sta peggiorando: è di qualità inferiore, pertanto è semplice da rilevare, ma si sta diffondendo sempre più.

<http://www.usatoday.com/news/nation/2008-12-28-counterfeiting_N.htm>

Nuovo concorso di crittanalisi dell'FBI:

<http://www.fbi.gov/page2/dec08/code_122908.html>

Questa citazione di Kip Hawley suona come fossero parole mie: "Nella confusione e nell'infinita varietà del viaggio, è possibile ritrovarsi con risultati assurdi in cui l'addetto della TSA dice "Beh, sto semplicemente seguendo le regole", ha detto il signor Hawley. 'Ma se avete un nemico che studia la vostra tecnologia e i vostri procedimenti, e avete una qualche misura per la quale il nemico può scoprire una scappatoia (e sta sempre cercando di scoprirla), allora avrete inserito una vulnerabilità nel progetto".

<<http://www.nytimes.com/2008/12/30/business/30road.html>>

I colpi migliori del 2008:

<<http://blog.wired.com/27bstroke6/2008/12/capers.html>>

Censura su Google Maps:

<http://www.schneier.com/blog/archives/2009/01/censorship_on_g.html>

Segnalare i tifosi di football più turbolenti attraverso messaggi SMS:

<http://www.usatoday.com/sports/football/nfl/2008-12-18-fan-conduct-cover_N.htm>
oppure <<http://tinyurl.com/3n73xr>>

Assegnazione delle risorse: frode finanziaria vs. terrorismo. Abbiamo visto questo problema presentarsi continuamente quando si parla di antiterrorismo: nel tentativo di difenderci contro le minacce più rare, ci rendiamo vulnerabili alle minacce più comuni.

<http://www.schneier.com/blog/archives/2009/01/allocating_reso.html>

Minaccia da trama cinematografica: i terroristi si servono degli insetti.

<<http://blog.wired.com/defense/2009/01/terrorists-coul.html>>

La paura fa vendere libri.

Articolo interessante sul tipo di archivi che il Dipartimento per la Sicurezza Nazionale tiene sui viaggiatori.

<http://current.newsweek.com/budgettravel/2008/12/whats_in_your_government_travel.html>

oppure <<http://tinyurl.com/8h4r9v>>

Twitter è caduto vittima di un dictionary attack perché il sito permetteva un numero illimitato di tentativi di autenticazione. Suvvia, gente, questo è l'ABC della sicurezza.

<<http://blog.wired.com/27bstroke6/2009/01/professed-twitt.html>>

<<http://www.codinghorror.com/blog/archives/001206.html>>

Twitter risponde:

<<http://al3x.net/2009/01/12/the-thing-about-security.html>>

Uno studio di San Francisco sulle telecamere di sicurezza dimostra che non funzionano:

<<http://www.citris-uc.org/news/SFcamerastudy>>

Un altro studio proveniente da Londra sostiene il contrario:

<<http://www.telegraph.co.uk/news/newsttopics/politics/lawandorder/4060443/Seven-of-ten-murders-solved-by-CCTV.html>>

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

Il mio intervento sulle telecamere di sicurezza:

<<http://www.schneier.com/essay-225.html>>

Il punto non è se siano utili o meno, ma se i loro benefici valgono i costi.

Criptare le chiavette USB è un'ottima idea - si perdono con una tale facilità - ma è stupido attaccare la chiave [di decrittazione] al dispositivo:

<<http://www.lep.co.uk/news/Apology-after-prisoners39-health-info.4862265.jp>>

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

Michael Chertoff parodiato da The Onion.

<http://www.theonion.com/content/news/terror_experts_warn_next_9_11>

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

Falsificare certificati SSL

Già sappiamo che MD5 è una funzione hash compromessa. Ora dei ricercatori hanno falsificato con successo certificati firmati con MD5.

Non è che sia questa gran cosa. La ricerca è fantastica: si tratta di un ottimo lavoro e mi piace sempre vedere attacchi crittanalitici impiegati allo scopo di espugnare sistemi di sicurezza del mondo reale. Fare quel tipo di salto è spesso più arduo di quanto pensino i crittografi.

Ma SSL non offre molto in quanto a sicurezza, pertanto comprometterlo non danneggia la sicurezza più di tanto. Quasi nessuno si prende la briga di verificare i certificati SSL, quindi non c'è un gran valore di attacco nell'essere in grado di falsificarli. E, ancor più in generale, i rischi maggiori per le informazioni su Internet si trovano ai punti finali - Trojan e rootkit sui computer degli utenti, attacchi contro database e server, eccetera - e non all'interno della rete.

Se da un lato è vero che i browser effettuano una minima verifica dei certificati SSL, quando trovano un certificato non valido visualizzano una finestra di avviso che tutti, me compreso, ignorano. Esistono fin troppi siti Web validi con pessimi certificati là fuori perché quell'avviso sia di qualche utilità.

Questo commento di Ted Dziuba è troppo vero: "Se siete come me e come ogni altro utente del pianeta, non ve ne può fregare di meno quando un certificato SSL non si convalida. Purtroppo, commons-httpclient è stato scritto da qualche pedante testa di cavolo che non ha mai provato a ottenere pagine Web vere e proprie".

Non perderò molte ore di sonno a causa di questi attacchi. Ma insomma, gente, nessuno dovrebbe usare MD5 ormai...

<http://news.cnet.com/8301-1009_3-10129693-83.html>
<<http://blogs.zdnet.com/security/?p=2339>>
<<http://phreedom.org/research/rogue-ca/>>
<http://www.theregister.co.uk/2008/12/30/ssl_spoofing/>
<<http://gizmodo.com/5120924/researchers-create-web-skeleton-key-with-200-ps3s>>
oppure <<http://tinyurl.com/82t3nv>>
<<http://arstechnica.com/news.ars/post/20081231-theoretical-attacks-yield-practical-attacks-on-ssl-pki.html>>
oppure <<http://tinyurl.com/7jg3ns>>

La ricerca:

<<http://www.win.tue.nl/hashclash/rogue-ca/>>
<<http://events.ccc.de/congress/2008/Fahrplan/track/Hacking/3023.en.html>>
<http://events.ccc.de/congress/2008/Fahrplan/attachments/1251_md5-collisions-1.0.pdf>
oppure <<http://tinyurl.com/9f2dg9>>

La citazione del commento di Dziuba:

<<http://teddziuba.com/2008/12/shut-your-face-commons-httpcli.html>>

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

Le news su Schneier

Sono stato intervistato su "60 Minutes" sulla sicurezza negli aeroporti. Sono particolarmente scioccato da questa citazione dalla pagina della CBS: "...è per questo che è stata creata la TSA: per non dimenticare mai", Hawley ha detto a Stahl". Questo estratto ben riassume molto di ciò che è sbagliato della TSA. Si concentra troppo sulle specifiche delle tattiche che sono state impiegate in passato, e non abbastanza sulla minaccia generale.

<<http://www.cbsnews.com/stories/2008/12/18/60minutes/main4675524.shtml>>

Intervista con il sottoscritto, da CIO Insight:

<<http://www.cioinsight.com/c/a/Expert-Voices/Bruce-Schneier-on-IT-Insecurity/>>

oppure <<http://tinyurl.com/a45xyc>>

Intervista con il sottoscritto, dal CSO Magazine:

<http://www.csoonline.com/article/473663/Bruce_Schneier_More_on_the_Broad_View_of_Security>

oppure <<http://tinyurl.com/7t4qsa>>

L'account "bruceschneier" su Twitter non è il mio. Il mio account è "schneier". Non ho mai postato e non so se lo farò mai.

<<http://twitter.com/bruceschneier>>

<<http://twitter.com/schneier>>

Ho parlato alla conferenza del Cato Institute: "Shaping the Obama Administration's Counterterrorism Strategy" (Delineare la strategia antiterrorismo dell'amministrazione Obama). È stato tutto molto interessante. I video della conferenza sono su Internet.

<<http://www.cato.org/events/counterterrorism/index.html>>

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

I dati biometrici

I dati biometrici possono sembrare una novità, ma in realtà sono la forma di identificazione più antica. Le tigri si riconoscono dall'odore; i pinguini riconoscono i richiami. Gli esseri umani si riconoscono a vista all'interno di una stanza, dalla voce al telefono, dalle firme su un contratto e dalle fotografie sulle patenti di guida. Le impronte digitali sono state impiegate per identificare le persone sulla scena di un crimine da più di cent'anni ormai.

La novità legata ai dati biometrici è che oggi sono i computer a effettuare il processo di riconoscimento: impronte del pollice, scansioni della retina, impronte vocali e pattern di dattiloscrittura. Viene impiegata molta tecnologia in questo ambito, per cercare di

limitare al tempo stesso il numero di falsi positivi (qualcun altro viene erroneamente identificato al vostro posto) e di falsi negativi (per errore, non venite identificati). Generalmente un sistema può scegliere di avere un minor numero di falsi positivi o di falsi negativi; è molto difficile ottenere un minor numero di entrambi.

I dati biometrici possono migliorare decisamente la sicurezza, specialmente se congiunti a un'altra forma di autenticazione come le password. Ma è importante comprenderne anche i limiti oltre che i punti di forza. I punti forti: i dati biometrici sono difficilmente falsificabili. È arduo attaccare una impronta digitale falsa sul proprio dito indice o far apparire la propria retina come quella di qualcun altro. Alcune persone possono imitare le voci, e gli artisti del make-up possono alterare i volti delle persone, ma si tratta di abilità particolari.

D'altro canto, è molto facile rubare i dati biometrici. Lasciamo le nostre impronte su qualunque cosa tocchiamo, la scansione della retina ovunque osserviamo. Con regolarità, gli hacker hanno copiato le impronte di vari funzionari partendo da oggetti che avevano toccato, e le hanno pubblicate su Internet. Non è ancora stato fatto un hack ai danni di un grande database di dati biometrici, ma la possibilità è sempre aperta. I dati biometrici sono identificatori unici, ma non sono segreti.

È un dato biometrico rubato può ingannare certi sistemi. Può essere facile come ritagliare una firma, incollarla su un contratto e poi faxare la pagina a qualcuno. La persona all'altro capo della linea non sa che la firma non è valida perché non l'ha vista appiccicata alla pagina. I login remoti mediante impronta digitale falliscono in maniera analoga. Se non vi è modo di verificare che l'impronta proviene da un lettore vero e proprio e non da un file archiviato su un computer, il sistema è molto meno sicuro.

Un sistema più sicuro è quello di utilizzare un'impronta digitale per sbloccare il proprio telefono cellulare o computer. Dato che esiste un percorso fidato fra il lettore di impronte e l'impronta archiviata che il sistema impiega per effettuare il confronto, un aggressore non può iniettare un'impronta precedentemente immagazzinata così facilmente come il tagliare/incollare una firma. Una foto su un documento di identità funziona allo stesso modo: chi verifica può confrontare il volto di fronte a lui con il volto fotografato sul documento.

Le impronte digitali sui documenti di identità sono più problematiche, perché l'aggressore può cercare di ingannare il lettore di impronte. I ricercatori hanno creato dita finte utilizzando gomma o glicerina. Le aziende hanno risposto costruendo lettori che rilevano anche i pori o una pulsazione.

I dati biometrici funzionano al meglio se il sistema può verificare che tali dati siano venuti da quella persona nel momento della verifica. Il sistema di identificazione biometrica alle porte del quartier generale della CIA funziona perché c'è una guardia armata che controlla che nessuno cerchi di ingannare il sistema.

Naturalmente non tutti i sistemi hanno bisogno di un tale livello di sicurezza. A Counterpane, la compagnia di sicurezza che ho fondato, abbiamo installato lettori della geometria della mano alle porte di accesso del centro operativo. La geometria della mano è un dato biometrico difficile da copiare, e il sistema era chiuso e non permetteva contraffazioni elettroniche. Funzionava molto bene.

Un altro problema con i dati biometrici: non falliscono elegantemente. Le password si possono cambiare, ma se qualcuno si appropria della vostra impronta, è fatta: non potete 'aggiornare' il vostro pollice. Si possono fare dei backup delle password, ma se l'impronta del vostro pollice viene alterata a seguito di un incidente, siete nei guai. Non è necessario che errori e fallimenti siano così notevoli: un lettore di timbro vocale potrebbe non riconoscere qualcuno con il mal di gola, o un lettore di impronte potrebbe non funzionare all'esterno con temperature molto basse. I sistemi biometrici devono essere analizzati alla luce di queste possibilità.

I dati biometrici sono semplici, comodi e -- se impiegati in maniera appropriata -- molto sicuri; solo che non si tratta di una panacea. Comprendere come funzionano e come falliscono è importantissimo per capire quando migliorano la sicurezza e quando no.

Questo articolo è originariamente apparso sul Guardian:

<<http://www.guardian.co.uk/technology/2009/jan/08/identity-fraud-security-biometrics-schneier-id>>

oppure <<http://tinyurl.com/94b6pp>>

È l'aggiornamento di un articolo che scrissi nel 1998.

<<http://www.schneier.com/crypto-gram-9808.html#biometrics>>

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

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

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

Dal 1998 CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo

<<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

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>

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

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 BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

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

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2008 - Bruce Schneier.