

CRYPTO-GRAM  
15 febbraio 2010

Scritta da Bruce Schneier  
Chief Security Technology Officer di BT  
e-mail: [schneier@schneier.com](mailto:schneier@schneier.com)  
Web: <<http://www.schneier.com>>

Edizione italiana curata da Communication Valley, Business Unit di Security Reply.  
<<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-0910.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:

- Migliorare l'intelligence
- L'anonimato e Internet
- News
- La sicurezza e lo spostamento delle funzioni (function creep)
- I semifinalisti del concorso 'un nuovo logo per la TSA'
- L'attacco cinese contro Google
- Le news su Schneier
- Un nuovo attacco contro Threefish
- Commenti dei lettori

\*\* \*\*

Migliorare l'intelligence

Il presidente Obama, nel suo recente discorso, ha giustamente posto l'accento su come migliorare le carenze dell'intelligence che hanno fatto sì che Umar Farouk Abdulmutallab passasse inosservato, invece che sulle tecnologie mirate ai dettagli del suo piano d'attacco. Ma se l'istinto di Obama è nella giusta direzione, riformare l'intelligence e adattarla a questo nuovo secolo, con le sue nuove minacce, è un compito assai più arduo di quanto possa piacere al presidente. Non servono nuove tecnologie, nuove leggi, nuovi sovrani della burocrazia; e

nemmeno nuove agenzie, per l'amor del cielo. Ciò che impedisce la condivisione di informazioni fra le organizzazioni di intelligence è la cultura della generazione che ha edificato quelle stesse organizzazioni.

Il sistema di intelligence statunitense è un apparato in continua, irregolare estensione, e che racchiude l'FBI e il Dipartimento di Stato, la CIA e la National Security Agency, e il Dipartimento per la Sicurezza Nazionale (esso stesso è il risultato della fusione di due dozzine di organizzazioni diverse) designato e ottimizzato per combattere la Guerra Fredda. A quel tempo l'unico, gigantesco avversario era l'Unione Sovietica: più burocratica che mai, con un budget enorme, e capace di operazioni di spionaggio veramente sofisticate. L'America doveva difendersi contro avanzate operazioni di intercettazione elettronica, con gli agenti sovietici che cercavano di corrompere o sedurre gli agenti americani, e una capacità di raccolta di intelligence a livello mondiale che si attaccava a ogni nostra parola.

In quell'ambiente la segretezza era fondamentale. Le informazioni dovevano essere protette da guardie armate e da doppie recinzioni, condivise soltanto fra coloro che avevano le giuste autorizzazioni di sicurezza e che dovevano essere specificatamente messi al corrente; ed era preferibile non trasmettere alcuna informazione piuttosto che trasmetterla in modo non sicuro.

Gli avversari di oggi sono diversi. Esistono ancora governi a caccia dei segreti americani, come la Cina. Ma si tratta di segreti molto più spesso aziendali che non militari, e la maggioranza delle altre organizzazioni di interesse sono come al Qaeda: decentralizzate, mal finanziate e incapaci delle intricate operazioni spia-contro-spia che poteva architettare l'Unione Sovietica.

Contro avversari del genere la condivisione delle informazioni è più importante della segretezza. Le nostre organizzazioni di intelligence devono scambiare strategie ed esperienza con l'industria, e devono condividere informazioni fra le parti che le costituiscono. I complotti terroristici odierni sono affari ad hoc e male organizzati, e quei punti che è così importante connettere prima di un attacco potrebbero trovarsi su scrivanie differenti, in edifici diversi, in mano a organizzazioni diverse.

I critici di questa posizione hanno fatto notare che esistono leggi che proibivano la condivisione fra agenzie ma, come ha scoperto la 9/11 Commission, la legge permette molta più condivisione di quanto si stia facendo attualmente. Questa condivisione non avviene in gran parte a causa di rivalità fra agenzie, della dipendenza da sistemi di informazione obsoleti, e di una cultura di segretezza. Ciò di cui abbiamo bisogno è una comunità di intelligence che si scambia idee, spunti e fatti sulla propria versione di Facebook, di Twitter e delle wiki. Occorre l'organizzazione in senso ascendente che ha fatto diventare Internet la più grande collezione di scibile umano e di idee mai realizzata.

Il problema è molto più sociale che tecnologico. Insegnare a vostra madre a mandare SMS e a vostro padre a usare Twitter non li rende parte della generazione di Internet, e dare a tutti quei combattenti della Guerra Fredda lezioni di blogging non cambierà la loro mentalità né la loro cultura. Il motivo per cui questo continua a rappresentare un problema, il motivo per cui il presidente George W. Bush non ha potuto cambiare le cose persino dopo che la 9/11

Commission arrivò alle stesse conclusioni alle quali è arrivato oggi il presidente Obama, è generazionale. Internet è il più grande divario generazionale dopo il rock and roll, e questo è vero sia all'interno del governo che fuori. Potrebbe essere necessario attendere che i veterani delle varie agenzie vadano in pensione e che siano sostituiti da persone cresciute insieme a Internet.

Una versione di questo editoriale di opinione è precedentemente apparso sul San Francisco Chronicle.

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/14/ED0L1BIFK6.DTL>>  
oppure <<http://tinyurl.com/y8cjsoq>>

L'idea che l'intelligence statunitense avrebbe dovuto 'collegare i vari punti' e fermare Abdulmutallab continua a resistere. Ma la realtà è molto più complessa, ed è facile collegare i punti dopo il fatto.

<[http://www.schneier.com/blog/archives/2010/01/the\\_abdulmutall.html](http://www.schneier.com/blog/archives/2010/01/the_abdulmutall.html)>

Nel 2002 avevo parlato delle carenze dell'intelligence.

<<http://www.schneier.com/crypto-gram-0206.html#1>>

Un'altra opinione:

<<http://online.wsj.com/article/SB10001424052748704586504574654261998633746.html>>

oppure <<http://tinyurl.com/ydjso9g>>

\*\* \*\*

## L'anonimato e Internet

L'identificazione universale viene dipinta da alcuni come il Sacro Graal della sicurezza su Internet. L'anonimato, dicono, è qualcosa di negativo, e se lo aboliamo possiamo garantire che soltanto le persone a posto abbiano accesso alle proprie informazioni. Sapremo chi ci invia lo spam e chi cerca di penetrare nelle reti aziendali. E quando verranno rilevati attacchi denial-of-service su vasta scala (come quelli contro l'Estonia, la Georgia o la Corea del Sud), sapremo chi è il responsabile e agiremo di conseguenza.

Il problema è che non funzionerà. Qualsiasi concezione di Internet deve permettere l'anonimato. L'identificazione universale è impossibile. Anche l'attribuzione (sapere chi è il responsabile di determinati pacchetti che viaggiano nella rete) è impossibile. Tentare di costruire un sistema del genere è inutile, e non farà altro che offrire a criminali e hacker nuovi modi per nascondersi.

Immaginate un mondo magico in cui ogni pacchetto che viaggia su Internet potesse essere tracciato fino a scoprirne l'origine. Anche in un mondo simile, i nostri problemi di sicurezza Internet non verrebbero risolti. Esiste un enorme divario tra il provare che un pacchetto sia venuto da un determinato computer e che il pacchetto sia stato diretto da un determinato individuo. Questo è esattamente il problema che abbiamo con i botnet o con i pedofili che archiviano materiale pedopornografico sui computer di persone innocenti. In questi casi

conosciamo la provenienza dei pacchetti DDoS e dello spam: arrivano da macchine normali e legittime che sono state hackerate. L'attribuzione non è così preziosa come si pensa.

Implementare una Internet senza anonimato è molto difficile, ed è una soluzione che genera a sua volta altri problemi. Per arrivare ad avere un'attribuzione perfetta avremmo bisogno di agenzie (organizzazioni vere e proprie) che forniscano credenziali di identità per accedere a Internet basate su altri sistemi di identificazione: passaporti, documenti d'identità nazionali, patenti di guida, ecc. Sistemi di identificazione meno efficaci, basati su documenti come le carte di credito, si possono facilmente ingannare. Non abbiamo nulla che si avvicina nemmeno lontanamente a questa infrastruttura di identificazione globale. In più, centralizzare le informazioni in questo modo in realtà è nocivo per la sicurezza, poiché rende il furto di identità un reato molto più remunerativo.

E realisticamente, una qualunque Internet teoricamente ideale dovrebbe permettere l'accesso alle persone anche in mancanza delle loro magiche credenziali. La gente continuerà a usare Internet collegandosi da terminali pubblici e in casa di amici. Vi saranno persone che smarriranno i loro magici token di accesso a Internet proprio come oggi smarriscono la patente o il passaporto. I meccanismi legittimi per aggirare il problema in questi casi daranno ancora più opportunità a criminali e hacker per sabotare il sistema.

Ma la cosa più importante è che la tecnologia che permette questa attribuzione magica non esiste. I bit sono bit, non hanno informazioni di identità appiccate sopra. Ogni sistema software che abbiamo mai inventato è stato hackerato con successo, ripetutamente. Molto semplicemente, non abbiamo l'esperienza e le capacità di costruire un sistema di attribuzione infallibile.

Non che importi davvero, comunque. Anche se tutti fossimo in grado di tracciare perfettamente ogni pacchetto, fino alla persona che lo ha originato e non solo fino al computer, l'anonimato sarebbe ancora possibile. Basterebbe un solo individuo che mettesse in piedi un server anonimo. Se io volessi inviare un pacchetto in forma anonima a qualcun altro, lo farei passare da quel server. Per un livello di anonimato ancora maggiore, potrei farlo passare attraverso più server. Questo processo viene chiamato 'onion routing' (lett. 'routing a cipolla' ovvero a strati) e, con un numero sufficiente di utenti e con la crittografia giusta, è in grado di ristabilire l'anonimato in qualunque sistema di comunicazione che lo vieta.

I tentativi di bandire l'anonimato da Internet non avranno effetto su chi è abbastanza esperto da aggirare l'ostacolo, costeranno miliardi di dollari, e avranno un impatto del tutto irrilevante sulla sicurezza. Ciò che produrranno tali tentativi sarà condizionare l'accesso alla libertà di espressione da parte dell'utente medio, comprese quelle persone che sfruttano l'anonimato su Internet per sopravvivere: i dissidenti in Iran, Cina e altrove.

Esigere un'identificazione e attribuzione universali è l'obiettivo sbagliato. Occorre accettare il fatto che su Internet esisterà sempre il pensiero espresso in forma anonima. Occorre accettare che non si saprà mai esattamente da dove è pervenuto un pacchetto. È necessario occuparsi dei problemi che si possono risolvere: software che siano sicuri a prescindere dai pacchetti ricevuti, sistemi di identificazione che siano sufficientemente sicuri di fronte ai possibili rischi.

Possiamo fare di meglio in tutti questi settori di quanto stiamo facendo oggi, e se ci impegniamo su questi fronti riusciremo a migliorare la sicurezza molto di più che non cercando di sistemare problemi insolubili.

L'intero problema dell'attribuzione è molto simile alla questione anticopia/gestione dei diritti digitali (DRM). Così come è impossibile rendere incopiabili determinati bit, è altrettanto impossibile sapere la provenienza di certi bit. I bit sono bit. Non nascono con restrizioni d'uso incorporate, non nascono con informazioni sull'autore incorporate. Ogni tentativo di superare questo limite è destinato a fallire, e dovrà essere sempre più protetto da contromisure da stato di polizia, quelle contromisure che l'industria dell'intrattenimento esige affinché le protezioni anticopia funzionino. È il metodo cinese: polizia, informatori, paura.

Così come l'industria dell'intrattenimento deve comprendere che l'universo digitale richiede un modello di business diverso, le forze di polizia e altri devono capire che i vecchi concetti di identificazione non funzionano su Internet. Nel bene e nel male, che piaccia o no, vi sarà sempre l'anonimato su Internet.

Questo articolo è originariamente apparso su Information Security, come parte di un botta-e-risposta con Marcus Ranum. Si può leggere la risposta di Marcus sotto il mio articolo.

<[http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14\\_gci1380347,00.html](http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1380347,00.html)>

oppure <<http://tinyurl.com/ydvm725>>

Commenti contro l'anonimato:

<[http://www.theregister.co.uk/2009/10/16/kaspersky\\_rebukes\\_net\\_anonymity/](http://www.theregister.co.uk/2009/10/16/kaspersky_rebukes_net_anonymity/)>

oppure <<http://tinyurl.com/yknbuh2>>

<<http://curiouscapitalist.blogs.time.com/2010/01/30/drivers-licenses-for-the-internet/>>

oppure <<http://tinyurl.com/yfjq7up>>

Conservare materiale pedopornografico su computer di persone innocenti:

<[http://www.huffingtonpost.com/2009/11/09/internet-virus-frames-use\\_n\\_350426.html](http://www.huffingtonpost.com/2009/11/09/internet-virus-frames-use_n_350426.html)>

oppure <<http://tinyurl.com/yg8jaka>>

Lo 'Onion routing':

<[http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci775657,00.html?int=off](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci775657,00.html?int=off)>

oppure <<http://tinyurl.com/y9onwrt>>

\*\* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \*

News

Abile stratagemma di un artista della fuga per evadere dal carcere.

<[http://www.schneier.com/blog/archives/2010/01/prison\\_escape\\_a.html](http://www.schneier.com/blog/archives/2010/01/prison_escape_a.html)>

Sicurezza e sostenibilità nella costruzione di edifici.

<<http://www.facilitiesnet.com/security/article/Green-Building-Goals-and-Security-Initiatives-Can-Find-Common-Ground--11349>>

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

L'intercettazione nell'ex Unione Sovietica:

<[http://www.schneier.com/blog/archives/2010/01/eavesdropping\\_i.html](http://www.schneier.com/blog/archives/2010/01/eavesdropping_i.html)>

Non so se tutta questa discussione sulle violazioni della privacy da parte di dipendenti di Facebook sia vera, ma mi pare assolutamente ragionevole che tutto Facebook sia conservato in un unico grande database accessibile e modificabile da persone autorizzate. E ha anche senso che sviluppatori e altri necessitino la possibilità di assumere l'identità di chiunque.

<<http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/?full=yes>>

oppure <<http://tinyurl.com/yaxu5j5>>

I problemi del profiling ai checkpoint di sicurezza.

<[http://news.bbc.co.uk/2/hi/uk\\_news/magazine/8452260.stm](http://news.bbc.co.uk/2/hi/uk_news/magazine/8452260.stm)>

Il labro è un pesce che punisce gli imbroglioni:

<[http://scienceblogs.com/notrocketscience/2010/01/cleaner\\_fish\\_punish\\_cheats\\_who\\_offend\\_their\\_customers.php](http://scienceblogs.com/notrocketscience/2010/01/cleaner_fish_punish_cheats_who_offend_their_customers.php)>

oppure <<http://tinyurl.com/yhw9da4>>

È un classico attacco di 'fishing'.

Ottime immagini di un ATM skimmer (dispositivo che viene applicato sopra la feritoia in cui si inserisce il bancomat allo sportello automatico per sottrarre il PIN e le informazioni del conto corrente). Non lo avrei mai notato altrimenti, che è appunto lo scopo di questi aggeggi.

<<http://www.krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/>>

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

Un buon articolo sulla sicurezza nel Web.

<<http://www.smashingmagazine.com/2010/01/14/web-security-primer-are-you-part-of-the-problem/>>

oppure <<http://tinyurl.com/ylzrq3m>>

Transport Canada sulle sue nuove normative di sicurezza. Okay, in realtà si tratta del Rick Mercer Report.

<<http://www.youtube.com/watch?v=yZfbTIYpKYo>>

Penny shooter business card, ovvero una tessera per sparare monetine. Ovviamente ciò significa che la TSA inizierà a vietare i portafogli sugli aerei.

<<http://www.youtube.com/watch?v=5KNZZ9qDJtQ>>

La polizia britannica sta considerando l'utilizzo di dispositivi spia automatizzati per effettuare sorveglianza 'di routine'.

<<http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones>>

Una nuova tecnologia potrebbe scansionare la merce imbarcata per rilevare la presenza di materiale nucleare e di esplosivi convenzionali.

<<http://www.technologyreview.com/blog/arxiv/24694/>>

L'8 gennaio è stata la giornata mondiale della privacy.

<<http://dataprivacyday2010.org/>>

Celebriamola firmando la Dichiarazione di Madrid sulla privacy, come privati o come organizzazioni.

<<http://thepublicvoice.org/madrid-declaration/>>

Che livello di unicità possiede il nostro browser? Possiamo venire tracciati semplicemente grazie alle sue caratteristiche particolari? È quel che la EFF sta cercando di scoprire. Il suo sito, Panopticlick, analizzerà le caratteristiche della configurazione del vostro browser e vi dirà il suo livello di unicità. Ho fatto il test personalmente, e il mio browser risulta essere l'unico fra i 120.000 browser testati fino a quel momento. Sono i plug-in del mio browser a renderlo unico: nessun altro ha la mia stessa identica configurazione. L'elenco dei miei font di sistema è quasi unico: soltanto un'altra persona possiede la mia stessa configurazione. (Mi pare strano, però, visto che ho un portatile Sony comprato una settimana fa con installato Windows 7, e non ho toccato nulla dei font di sistema). La EFF dà qualche suggerimento per difendersi, nessuno dei quali molto soddisfacente.

<<http://panopticlick.eff.org/>>

<<http://arstechnica.com/tech-policy/news/2010/01/even-without-cookies-a-browser-leaves-a-trail-of-crumbs.ars>>

oppure <<http://tinyurl.com/yagts94>>

<[http://www.schneier.com/blog/archives/2010/01/tracking\\_your\\_b.html#c410841](http://www.schneier.com/blog/archives/2010/01/tracking_your_b.html#c410841)>

Deconfliction: vale la pena guardare questo video.

<<http://www.youtube.com/watch?v=g39xIewgGaM>>

Falla di sicurezza delle carte di credito/debito online:

<<http://www.lightbluetouchpaper.org/2010/01/26/how-online-card-security-fails/>>

oppure <<http://tinyurl.com/ykwyp4e>>

<<http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf>>

Il sito Web The Foreign Policy ha il suo elenco di minacce da trama cinematografica: terroristi muniti di mitragliatrici su parapendii, sciame di insetti che trasmettono malattie, una 'bomba sporca' creata dai pezzi di un rilevatore di fumo, complotti perpetrati attraverso giochi online, la catena alimentare contaminata con il botulino. Il sito dà un po' di corpo a queste minacce, ma non è nulla che i lettori abituali di questa newsletter e del mio blog non possano immaginare per proprio conto. Forse dovrebbero varare un loro concorso sulla miglior minaccia da trama cinematografica.

<[http://www.foreignpolicy.com/articles/2010/01/27/the\\_world\\_s\\_most\\_bizarre\\_t\\_error\\_threats](http://www.foreignpolicy.com/articles/2010/01/27/the_world_s_most_bizarre_t_error_threats)>

oppure <<http://tinyurl.com/y8mfmrz>>

Terrorizzare il Senate Intelligence Committee.

<[http://www.schneier.com/blog/archives/2010/02/scaring\\_the\\_sen.html](http://www.schneier.com/blog/archives/2010/02/scaring_the_sen.html)>

Dieci vignette sulla sicurezza aeroportuale.

<<http://www.telegraph.co.uk/travel/picturegalleries/7091780/Matt-on-travel-airport-security.html>>

oppure <<http://tinyurl.com/y8qshyw>>

Ricerca interessante sui limiti delle ispezioni visive. Questo ha delle ripercussioni sulla ricerca di materiale di contrabbando negli aeroporti.

<[http://www.cell.com/current-biology/abstract/S0960-9822\(09\)02122-8](http://www.cell.com/current-biology/abstract/S0960-9822(09)02122-8)>

<<http://www.npr.org/templates/story/story.php?storyId=122561355>>

Non è un tantino imbarazzante che si riporti un sedicente 'esperto in antiterrorismo' per aver detto queste cose? "Bill Tupman, un esperto in antiterrorismo dell'Università di Exeter, ha dichiarato a BBC News: 'Il problema è tentare di prevedere la mente del tipico complottista di Al-Qaeda; potrebbero fare tante di quelle cose. Ed è inoltre necessario rassicurare il pubblico che stiamo cercando di superare in astuzia quel complottista di Al-Qaeda, e che siamo in procinto di proteggere tutti da qualsiasi minaccia". Io credo che sia necessario convincere il pubblico che debba rifiutarsi di lasciarsi terrorizzare. Quel che più mi frustra della vicenda di Abdulmutallab è che ha provocato terrore anche se il suo piano ha fallito. Vorrei che tutti quanti fossimo abbastanza indomiti da non farci spaventare dal prossimo attacco, anche se andasse a buon fine. Ricordate: il terrorismo non può distruggere lo stile di vita del nostro paese; solo la nostra reazione al terrorismo può farlo.

<[http://news.bbc.co.uk/2/hi/uk\\_news/england/devon/8481446.stm](http://news.bbc.co.uk/2/hi/uk_news/england/devon/8481446.stm)>

Nello stato della Carolina del Sud, tutte le organizzazioni sovversive devono registrarsi. Secondo voci di corridoio, questa legge è stata approvata l'anno scorso, ma pare risalire agli anni Cinquanta.

<[http://www.schneier.com/blog/archives/2010/02/all\\_subversive.html](http://www.schneier.com/blog/archives/2010/02/all_subversive.html)>

Dahlia Lithwick sulla "Terrorism Derangement Syndrome" (Sindrome dell'alienazione da terrorismo):

<<http://www.slate.com/id/2243429>>

Ai terroristi è vietato utilizzare iTunes:

<[http://www.schneier.com/blog/archives/2010/02/terrorists\\_proh.html](http://www.schneier.com/blog/archives/2010/02/terrorists_proh.html)>

Intervista con un truffatore online nigeriano:

<[http://www.schneier.com/blog/archives/2010/02/interview\\_with\\_16.html](http://www.schneier.com/blog/archives/2010/02/interview_with_16.html)>

Attacco Man-in-the-middle contro il sistema di pagamento delle carte chip-and-PIN:

<[http://www.schneier.com/blog/archives/2010/02/man-in-the-midd\\_1.html](http://www.schneier.com/blog/archives/2010/02/man-in-the-midd_1.html)>

Duplicatore di chiavi di auto:

<[http://www.schneier.com/blog/archives/2010/02/car-key\\_copier.html](http://www.schneier.com/blog/archives/2010/02/car-key_copier.html)>

Un articolo interessante su un aspirante spia e il suo sistema crittografico carta-e-penna.

<[http://www.wired.com/magazine/2010/01/ff\\_hideandseek/all/1](http://www.wired.com/magazine/2010/01/ff_hideandseek/all/1)>

Avventura a fumetti a tema crittografico:

<[http://www.schneier.com/blog/archives/2010/02/crypto\\_comic\\_bo.html](http://www.schneier.com/blog/archives/2010/02/crypto_comic_bo.html)>

James Fallows e la minaccia cibernetica cinese:

<<http://www.theatlantic.com/doc/201003/china-cyber-war>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

La sicurezza e lo spostamento delle funzioni (function creep)

La sicurezza è raramente statica. La tecnologia trasforma sia i sistemi di sicurezza, sia chi li attacca. Ma esiste un altro fattore che modifica il compromesso costi/benefici della sicurezza: come si utilizzano i sistemi che vengono protetti. Troppo spesso costruiamo la sicurezza intorno a un unico scopo, per poi renderci conto che il sistema viene utilizzato per uno scopo diverso -- uno scopo per il quale il sistema non era adatto sin dal principio. E a quel punto il sistema di sicurezza deve aggiornarsi e stare al passo con il cambiamento.

Prendiamo le patenti di guida, per esempio. Pensate originariamente per dimostrare una credenziale (la capacità di condurre un veicolo), assomigliavano ad altre credenziali: la licenza per esercitare la professione medica o i certificati di ispezione per gli ascensori. Erano ovviamente delle dimensioni adatte per il portafogli, ma non avevano un gran livello di sicurezza. Poi, poco a poco, le patenti di guida hanno assunto una seconda funzione: sono diventate strumenti di verifica dell'età nei bar e nelle rivendite di alcolici. Naturalmente la sicurezza non era adeguata allo scopo -- i teenager possono essere veramente ingegnosi se ci si mettono -- e col passare degli anni alle patenti di guida sono state aggiunte fototessere, funzioni anti-manomissione (una volta era facile modificare l'anno di nascita) e tecnologie anticontraffazione. Contraffare una patente di guida aveva poco valore; contraffare uno strumento di verifica dell'età ne aveva molto di più.

Oggi, le patenti di guida statunitensi stanno assumendo ancora un'altra funzione: la sicurezza contro i terroristi: Il Real ID Act (il tentativo del governo di rendere le patenti di guida ancor più sicure) non ha nulla a che vedere con il condurre un veicolo o con l'acquistare alcolici, e tutto a che vedere con il tentativo di rendere quel pezzo di plastica un sistema efficace per verificare che il possessore non si trovi sulla watch list antiterrorismo. Che si tratti di una buona idea, o che aumenti davvero il livello di sicurezza, è tutto un altro discorso.

È possibile notare questo spostamento di funzioni (detto 'function creep') un po' dappertutto. Sistemi di sicurezza Internet progettati per siti Web informativi dovrebbero improvvisamente offrire la sicurezza necessaria a siti di Internet Banking. Sistemi di sicurezza adatti a proteggere dei beni di scarso valore improvvisamente si rivelano inefficaci una volta che il prezzo di quei beni è aumentato. Ci si aspetta che i sistemi di sicurezza di un'applicazione, ideati per reti locali, continuino a funzionare bene anche quando l'applicazione viene spostata in un ambiente di cloud computing. E ci si aspetta che la sicurezza del cloud computing, pensata per le esigenze delle aziende, funzioni altrettanto bene per applicazioni governative, magari anche militari.

A volte è ovvio che sistemi di sicurezza ideati per un ambiente non funzioneranno in un altro. Non armiamo i nostri soldati allo stesso modo in cui armiamo i nostri poliziotti, e non possiamo prendere veicoli commerciali e trasformarli facilmente in veicoli appositamente modificati per l'esercito. Se all'improvviso entriamo in possesso di un sacchetto di diamanti, capiamo subito che forse è il caso di installare un antifurto domestico un po' più sofisticato. Eppure molti credono che la stessa sicurezza che protegge il computer di casa possa essere in grado di proteggere anche le macchine per il voto elettronico, e che gli stessi sistemi operativi che fanno funzionare la nostra attività siano adatti all'uso militare.

Ma queste sono tutte decisioni consapevoli, e noi professionisti di sicurezza spesso ne sappiamo di più dell'utente medio. I veri problemi sorgono quando i cambiamenti avvengono sullo sfondo, inconsciamente. Costruiamo un sistema di sicurezza perfettamente adeguato alla minaccia e (proprio come la patente di guida diventa uno strumento di verifica dell'età) la rete genera sempre più funzioni. Ma dato che è già stata dichiarata 'sicura' non sarà possibile ottenere fondi per riesaminare e migliorare la sicurezza prima che i malintenzionati ne abbiano scoperto e sfruttato le vulnerabilità.

Non mi piace giocare all'inseguimento in ambito di sicurezza, ma sembra che siamo destinati a farlo.

Questo articolo è originariamente apparso nel numero di gennaio/febbraio di IEEE Security and Privacy.

\*\* \*\*

I semifinalisti del concorso 'un nuovo logo per la TSA'

Il mese scorso ho indetto un concorso per ridisegnare il logo della TSA. Abbiamo dei finalisti. Andate a votare nei commenti al post sul mio blog. Facendo clic sulle immagini verrà visualizzata una versione ingrandita e più facile da leggere.

I contributi:

<[http://www.schneier.com/blog/archives/2010/01/tsa\\_logo\\_contes.html](http://www.schneier.com/blog/archives/2010/01/tsa_logo_contes.html)>

I finalisti:

<[http://www.schneier.com/blog/archives/2010/02/tsa\\_logo\\_contes\\_1.html](http://www.schneier.com/blog/archives/2010/02/tsa_logo_contes_1.html)>

Patrick Smith e io abbiamo promesso al vincitore delle copie dei nostri libri. Il vincitore riceverà inoltre un permesso di imbarco fasullo da usarsi con qualsiasi volo in qualsiasi giorno dell'anno, e una bottiglietta vuota da 33 cl con l'etichetta 'Soluzione salina' che si può riempire e riutilizzare più volte per passare i checkpoint di sicurezza della TSA.

\*\* \*\*

## L'attacco cinese contro Google

Il mese scorso Google ha annunciato di aver subito un attacco sofisticato da parte della Cina. Da allora si sono saputi alcuni dettagli tecnici interessanti.

La voce di corridoio per cui la Cina avrebbe utilizzato un sistema che Google aveva implementato per consentire intercettazioni legali -- voce che ho utilizzato come aggancio per un articolo su CNN.com -- non è stata confermata. A questo punto dubito che sia fondata.

La mia reazione iniziale:

<[http://www.schneier.com/blog/archives/2010/01/google\\_vs\\_china.html](http://www.schneier.com/blog/archives/2010/01/google_vs_china.html)>

Il mio articolo su CNN.com. Ancora, la congettura secondo cui l'attacco cinese si sarebbe servito di percorsi utilizzati per compiere intercettazioni legali pare non essere fondata.

<<http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html>

>

oppure <<http://tinyurl.com/y9fz5ew>>

Un altro post sull'argomento sul mio blog:

<[http://www.schneier.com/blog/archives/2010/02/more\\_details\\_on.html](http://www.schneier.com/blog/archives/2010/02/more_details_on.html)>

I dettagli tecnici:

<<http://www.wired.com/threatlevel/2010/02/apt-hacks/>>

<[http://www.darkreading.com/database\\_security/security/attacks/showArticle.jhtml?articleID=222600139](http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=222600139)>

Google e la NSA: il più grande raccoglitore di dati al mondo si allea con il più grande raccoglitore di dati al mondo. A qualcuno sembra una buona idea?

<<http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html>>

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

EPIC ha inviato una richiesta FIFA (Freedom of Information Act) di informazioni su tale accordo:

<<http://epic.org/2010/02/epic-seeks-records-on-google-n.html>>

Ho già parlato del ruolo della NSA nella protezione del cyberspazio:

<<http://www.schneier.com/essay-265.html>>

\*\* \*\*\* \*\*\*\*\* \*\*

Le news su Schneier

Sono stato intervistato allo show radiofonico New Horizons a Boise:

<<http://radio.boisestate.edu/NewHorizons.html>>

Terrò un intervento al Minneapolis College of Art and Design il 18 febbraio:

<<http://events.mcad.edu/?q=node/97>>

Interverrò anche alla RSA Conference a San Francisco il 4 marzo:  
<<http://www.rsaconference.com/2010/usa/>>

\*\* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \*\* \* \*\* \*\* \*\* \* \*\* \*\* \*\* \* \*\* \*\* \*\* \*

## Un nuovo attacco contro Threefish

Al FSE 2010 la scorsa settimana, Dmitry Khovratovich e Ivica Nikolic hanno presentato uno studio in cui eseguono l'analisi crittografica degli algoritmi ARX (algoritmi che utilizzano solamente addizioni, sottrazioni e operazioni OR-esclusive): "Rotational Cryptanalysis of ARX" [Crittanalisi rotazionale di ARX]. Nello studio gli autori dimostrano il loro attacco contro Threefish. Il loro attacco compromette 39 round su 72 di Threefish-256 con una complessità di  $2^{252,4}$ ; 42 round su 72 di Threefish-512 con una complessità di  $2^{507}$ ; e 43,5 round su 80 di Threefish-1024 con una complessità di  $2^{1014,5}$ . (Sì, oltre  $2^{1000}$ . Non ridete, si tratta di un attacco davvero valido anche se -- come gli altri qui dimostrati -- non sarà mai attuabile praticamente).

È un lavoro eccellente, e rappresenta la migliore serie di attacchi contro Threefish vista finora. (Sospetto che gli attacchi si possano estendere di qualche altro round con qualche brillante trucco crittanalitico, ma non oltre). La sicurezza dell'intero Threefish non è a rischio, naturalmente; c'è ancora un margine di sicurezza molto ampio.

Abbiamo sempre supportato la sicurezza di Threefish con qualsiasi insieme di costanti che non siano ovviamente pessime. Eppure, una banale modifica (cambiare un'unica costante nel programma delle chiavi) riduce drasticamente il numero di round attraverso cui questo attacco può penetrare. Se il NIST permette un altro giro di modifiche agli algoritmi candidati per SHA-3, ne approfitteremo sicuramente per migliorare la sicurezza di Skein; cambieremo questa costante in un valore che rimuova le simmetrie rotazionali sfruttate da questa tecnica. Se non vi sarà un altro giro di modifiche, abbiamo comunque fiducia nella sicurezza di Threefish e Skein.

Lo studio:

<<http://www.skein-hash.info/sites/default/files/axr.pdf>>

Threefish:

<<http://www.schneier.com/threefish.html>>

Gli algoritmi candidati per SHA-3:

<<http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>>

Skein:

<<http://www.skein-hash.info/>>

\*\* \*\* \*\* \* \*\* \*\* \* \*\* \*\* \*\* \* \*\* \*\* \*\* \* \*\* \*\* \*\* \* \*\* \*\* \*\* \*

Commenti dei lettori



Copyright (c) 2010 - Bruce Schneier.