

CRYPTO-GRAM
15 giugno 2009

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

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:

Il discorso di Obama sulla sicurezza cibernetica
Puzzle crittografico basato su LOST nella rivista Wired
Gli arresti antiterrorismo del mese scorso
News
Il mio intervento sugli scanner del corpo intero negli aeroporti
Le news su Schneier
Il Canile: Net1
Il cloud computing
Il Secondo Workshop Interdisciplinare sulla Sicurezza e il Comportamento Umano
Commenti dei lettori

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

Il discorso di Obama sulla sicurezza cibernetica

Sono ottimista in merito alla nuova politica di sicurezza cibernetica di Obama e alla creazione del nuovo ruolo di 'coordinatore della sicurezza cibernetica', anche se molto

dipende dai dettagli. Quel che sappiamo è che le minacce sono reali, dai furti d'identità, agli atti di hacking da parte dei cinesi, alla guerra cibernetica.

I suoi principi sono assolutamente i benvenuti: proteggere le reti governative, coordinare le risposte alle emergenze, agire al fine di proteggere l'infrastruttura nelle mani di aziende private (l'energia elettrica, le reti delle comunicazioni, e così via), anche se ritengo che egli sia un po' troppo ottimista sul fatto che non sarà necessaria una legislazione adeguata. Soprattutto, mi ha grandemente rinfanciato sentire del suo impegno per finanziare la ricerca. Molta della tecnologia che utilizziamo oggi per proteggere il cyberspazio è stata sviluppata a partire dalla ricerca universitaria, e più la finanziamo oggi, più sicuri saremo nel giro di dieci anni.

Anche l'educazione è essenziale, anche se a volte penso che i miei genitori abbiano bisogno di più educazione in materia di sicurezza cibernetica di quanto ne avranno i miei nipoti. Apprezzo inoltre l'impegno del presidente nei confronti di trasparenza e privacy, entrambe fondamentali per la sicurezza.

Ma i dettagli sono importanti. Centralizzare le responsabilità di sicurezza ha lo svantaggio di rendere la sicurezza più fragile stabilendo un unico approccio e un'uniformità di pensiero. A meno che il nuovo coordinatore non distribuisca la responsabilità, la sicurezza cibernetica non è destinata a migliorare.

Mentre l'amministrazione porta avanti il progetto, si dovrebbero applicare due principi. Uno: le decisioni di sicurezza devono essere prese il più vicino possibile al problema. Proteggere le reti dovrebbe essere compito di chi quelle reti le capisce, e le minacce devono essere affrontate da persone vicine alle minacce stesse. Ma la responsabilità distribuita porta con sé un maggior numero di rischi, per cui è fondamentale stabilire una supervisione.

Due: il coordinamento della sicurezza deve avvenire al livello più alto possibile, che si tratti di valutazione delle informazioni riguardanti minacce differenti, di risposta a un worm in Internet, di fondazione di linee guida per proteggere informazioni personali. L'intero disegno è ben più vasto di ogni singola agenzia.

Questo articolo è originariamente apparso sul sito del New York Times, insieme a molti altri di commento al discorso di Obama.

<<http://roomfordebate.blogs.nytimes.com/2009/05/29/a-plan-of-attack-in-cyberspace>>

Vale la pena leggersi anche gli altri interventi. Nello specifico voglio citare James Bamford, che tratta un concetto da me espresso più e più volte: "La storia degli 'zar' della Casa Bianca non è una delle più gloriose, come ben sa chi ha seguito l'ascesa e la caduta degli 'zar' della droga. Si fa un gran battage pubblicitario, si organizza un discorso della Casa Bianca, e poi le cose ritornano alla normalità- Il potere, la capacità di provocare cambiamenti, dipende in prima istanza da chi controlla il denaro e da chi è più vicino al presidente. Dato che il nuovo 'cyber-zar' non avrà né un libretto degli assegni, per così dire, né accesso diretto al presidente Obama, il suo ruolo sarà più simile a quello di un vigile addetto al traffico che non a quello di uno 'zar'".

Gus Hosein ha scritto un ottimo articolo sulla necessità della privacy: "Innalzare barriere intorno ai sistemi informatici è senza dubbio un buon punto di partenza. Ma quando questi sistemi vengono violati, le nostre informazioni personali rimangono

vulnerabili. Eppure i governi e le aziende stanno raccogliendo un quantitativo sempre più grande di informazioni personali. L'assunto iniziale dovrebbe essere che ogni dato raccolto è vulnerabile e soggetto ad abuso o furto. Dovremmo quindi raccogliere soltanto quelle informazioni assolutamente necessarie".

Scrissi una cosa simile a questo mio articolo nel 2002, sulla creazione del Dipartimento per la Sicurezza Nazionale: "Il corpo umano si difende mediante sistemi di sicurezza che si sovrappongono. Esso possiede un complesso sistema immunitario per combattere specificamente una malattia, ma questa battaglia contro la malattia viene distribuita attraverso i vari organi e le varie cellule. Il nostro corpo possiede ogni genere di sistemi di sicurezza, a partire dalla pelle, che tiene alla larga elementi nocivi all'organismo; al fegato, che depura il sangue da certe sostanze pericolose; fino alle difese presenti nell'apparato digerente. Tutti questi sistemi e apparati svolgono i propri compiti in maniera diversa. Inoltre questi sistemi si intrecciano l'un l'altro e, entro certi limiti, possono venirsi in aiuto nel caso uno di essi non funzioni a dovere. Potrebbe sembrare ridondante e inefficiente, ma in realtà è un sistema solido, affidabile e sicuro. È grazie a esso che siete vivi e state leggendo questo testo".

Altri link a notizie sul discorso di Obama:

<<http://www.nytimes.com/2009/05/30/us/politics/30cyber.html>>

<http://voices.washingtonpost.com/securityfix/2009/05/obama_cybersecurity_is_a_natio.html?wprss=securityfix>

oppure <<http://tinyurl.com/lrp9cm>>

<<http://www.google.com/hostednews/ap/article/ALeqM5i9mgJb3EsMIaA6aVcbSkp84g0sMwD98G2U0G0>>

oppure <<http://tinyurl.com/maz4lh>>

<<http://www.networkworld.com/news/2009/052909-obama-security-coordinator.html>>

oppure <<http://tinyurl.com/lbge8m>>

<<http://swampland.blogs.time.com/2009/05/29/obamas-cybersecurity-speech-why-bother/>>

oppure <<http://tinyurl.com/l8vhwf>>

<http://www.theregister.co.uk/2009/05/29/obama_creates_cyber_post/>

Ottimi commenti da parte di Gene Spafford:

<http://www.cerias.purdue.edu/site/blog/post/on_cyber_czars_and_60-day_reports/>

oppure <<http://tinyurl.com/nalj74>>

Ottimi commenti da parte di Bob Blakley:

<<http://notabob.blogspot.com/2009/06/cyber-security.html>>

Il mio intervento nel 2002:

<<http://www.schneier.com/crypto-gram-0212.html#3>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:

<http://www.schneier.com/blog/archives/2009/05/obamas_cybersec.html>

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

Puzzle crittografico basato su LOST nella rivista Wired

Mi è stato chiesto di realizzare un puzzle crittografico basato sulla serie televisiva LOST per il numero di Aprile 2009 della rivista Wired. Nello specifico, mi è stato dato un 'indizio' da criptare.

I dettagli si trovano nei link sottostanti. Creare una cosa di questo genere è molto difficile. L'enigma deve essere abbastanza difficile per evitare che venga risolto a prima vista, e abbastanza facile da poter essere risolto alla fine. Per complicare ancor più le cose, le persone condivideranno le proprie idee su Internet. Per cui se, per esempio (sto inventando, sia chiaro), la soluzione richiede una conoscenza della storia della civiltà Maya, della progettazione di un carburatore, di topologia algebrica e di danza popolare russa, è probabile che chi è esperto in questi rispettivi campi si incontri e ne discuta via Internet. Il puzzle deve essere difficile anche per la mente di gruppo, non solo per i singoli.

<<http://mestizorocks.blogspot.com/2009/05/spoiler-alert-lost-puzzle-solution-from.html>>

oppure <<http://tinyurl.com/oy8bok>>

<http://www.yesbutnobuty.com/archives/2009/04/lost_wired_puzz.html>

<<http://bradicali.blogspot.com/2009/04/major-major-progression-on-lost-numbers.html>>

oppure <<http://tinyurl.com/n9dfdj>>

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

Gli arresti antiterrorismo del mese scorso

Ho quattro cose da dire in merito all'arresto dei tre uomini che avevano pianificato di far saltare in aria alcune sinagoghe a New York. Uno: il rischio di un attacco terroristico vero e proprio era risibile: "Le autorità hanno affermato che i quattro uomini erano da tempo sotto indagine, e il rischio che avrebbero potuto veramente portare avanti il loro piano era proprio minimo -- ha riportato Pete Williams di NBC News".

E: "Non sono mai arrivati al punto di riuscire a combinare qualcosa", ha detto un funzionario a NBC News. "A ogni modo, è una buona cosa che gente così non possa più circolare liberamente".

Ovviamente i politici stanno usando questo incidente per diffondere ancor più paura: "Si è trattato di una minaccia molto seria che avrebbe potuto costare moltissime vite se si fosse realizzata", ha detto in un'intervista con la WPIX-TV il rappresentante Peter T. King, repubblicano da Long Island. "Sarebbe stata una tragedia orrenda e dannosa. I terroristi locali e anche gli ex-galeotti convertiti rappresentano una minaccia concreta".

Due: sono stati presi grazie all'investigazione e all'intelligence tradizionali. Non dalla sicurezza aeroportuale. Non da intercettazioni abusive senza mandato. Ma dall'investigazione e intelligence vecchio stile. Questo è ciò che funziona. Questo è ciò che ci mantiene al sicuro. Ho scritto un articolo nel 2004 che sostiene proprio questo: "L'unica maniera efficace per contrastare i terroristi è attraverso il tradizionale operato di polizia e intelligence -- scoprire i piani prima che vengano messi in atto e quindi perseguire i cospiratori".

Tre: erano degli idioti: "Il capobanda della cellula terroristica locale, composta dai quattro uomini accusati di aver progettato attentati dinamitardi alle sinagoghe del Bronx e ad aerei militari a Newburgh, ha ammesso oggi di fronte al giudice che aveva fumato marijuana prima dell'arresto avvenuto la notte precedente.

"Quando il magistrato Lisa M. Smith ha chiesto a James Cromitie se la sua capacità di discernimento fosse in qualche modo alterata o indebolita durante la sua apparizione di fronte al tribunale federale di White Plains, il 55enne ha confessato: 'No. La fumo regolarmente. Comprendo bene tutto quel che mi sta dicendo'".

Quattro: un 'informatore' ha aiutato parecchio questo gruppo: "Ad aprile, il sig. Cromitie e altri tre uomini scelsero le sinagoghe come bersaglio, secondo la dichiarazione. L'informatore li ha prontamente aiutati a procurarsi le armi, le quali, secondo le autorità, non erano in grado di essere utilizzate o detonate".

L'avvertenza che scrissi in "Ritratto del Terrorista Moderno da Idiota" è ancora attuale: "Malgrado la frenesia iniziale della stampa, assai frequentemente i dettagli veri e propri di questi casi si rivelano essere molto meno incriminanti. Troppo spesso non è chiaro se gli imputati sono davvero colpevoli, o se la polizia ha creato un crimine dal nulla".

Anzi, a ben pensarci, tutto quell'articolo del 2007 è ancora attuale. Certe cose non cambiano mai.

<<http://www.msnbc.msn.com/id/30856404/>>
<<http://www.nytimes.com/2009/05/21/nyregion/21arrests.html>>
<<http://www.schneier.com/essay-038.html>>
<<http://www.nbcnewyork.com/news/local/Accused-.html>>

Il "Ritratto del Terrorista Moderno da Idiota":
<<http://www.schneier.com/essay-174.html>>

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

News

Kylin è un sistema operativo sicuro realizzato in Cina. Pare essere una variante di Linux.

<<http://washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/>>
oppure <<http://tinyurl.com/qfwjos>>

Una fantastica minaccia da trama cinematografica: pirati nella Chesapeake Bay.

<<http://blogs.mddailyrecord.com/ontherecord/2009/05/12/pirates-on-the-bay/>>
oppure <<http://tinyurl.com/rch6xz>>

Ricordate: se non vi piace qualcosa, dichiarate che servirà ai terroristi, o che li incoraggerà o attirerà. Funziona sempre.

Penna a inchiostro invisibile:

<http://www.schneier.com/blog/archives/2009/05/invisible_ink_p.html>

Microsoft bandisce memcopy() dal suo codice base. Interessante discussione nei commenti sul fatto che sia una miglioria o soprattutto un aggiustamento cosmetico.
<http://www.schneier.com/blog/archives/2009/05/microsoft_bans.html>

La coppia di coordinate casa/lavoro possono identificarci in modo esclusivo. Questo è abbastanza preoccupante, calcolando la quantità di servizi basati sul posizionamento che stanno diffondendosi e la quantità di database che raccolgono dati sulla posizione geografica.
<http://www.schneier.com/blog/archives/2009/05/on_the_anonymit.html>

Gli IED (Improvised Explosive Device, ordigni esplosivi improvvisati) ora sono armi di distruzione di massa:
<http://www.schneier.com/blog/archives/2009/05/ieds_are_now_we.html>

Ricerca sull'insicurezza delle 'domande segrete'.
<http://www.schneier.com/blog/archives/2009/05/secret_question.html>

Difendersi dalle minacce da trama cinematografica usando i personaggi dei film:
<http://www.schneier.com/blog/archives/2009/05/defending_again.html>

Un lancio-dadi automatico fantastico, un generatore di numeri casuali per videogiochi.
<http://www.schneier.com/blog/archives/2009/05/automatic_dice.html>

Steganografia che si serve della ritrasmissione TCP. Non credo che questo genere di cose abbia applicazioni su vasta scala, ma sono ugualmente brillanti.
<<http://arxiv.org/abs/0905.0363>>

Che cosa fate se avete da effettuare troppi background check per verificare l'autorizzazione di sicurezza di una persona, e non avete sufficiente tempo per effettuarli?
<<http://www.federaltimes.com/index.php?S=4104591>>
È tutta una questione di incentivi. Gli investigatori sono stati premiati per aver completato le indagini, non per averle svolte bene.

Un uomo è stato trattenuto dai funzionari dell'immigrazione perché non aveva impronte digitali:
<<http://www.reuters.com/article/oddlyEnoughNews/idUSTRE54Q42P20090527?feedType=RSS&feedName=oddlyEnoughNews&rpc=69>>
oppure <<http://tinyurl.com/l6rbyq>>

Sempre parlando di notizie biometriche, quattro stati hanno vietato di sorridere nelle fototessere da applicare alla patente di guida.
<http://www.usatoday.com/news/nation/2009-05-25-licenses_N.htm>

Ricerca sulle minacce da trama cinematografica: "Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About?" (Minacce emergenti e pianificazione di sicurezza: come decidere di quali minacce ipotetiche preoccuparsi?)
<http://www.rand.org/pubs/occasional_papers/OP256/>
<http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf>

Cavi segreti per comunicazioni governative nascosti sottoterra nei dintorni di Washington, DC.

<http://www.schneier.com/blog/archives/2009/06/secret_govermen.html>

L'idea del mese per una trama cinematografica: armare la polizia di Boston con fucili semiautomatici:

<http://www.schneier.com/blog/archives/2009/06/boston_police_g.html>

Non so come ho fatto a perdere questa serie eccezionale di articoli su Slate apparsi a febbraio. Si tratta di otto articoli che parlano di come non vi siano stati attacchi terroristici negli Stati Uniti sulla scia dell'11 settembre (a eccezione della posta all'antrace, immagino). Leggeteli tutti.

<http://www.schneier.com/blog/archives/2009/06/why_is_terroris.html>

<<http://slate.com/id/2213025>>

Nel numero di maggio di Crypto-Gram ho scritto in merito alla polizia di Boston che ha sequestrato il computer di uno studente perché, fra le altre cose, aveva un'installazione di Linux. All'inizio del mese, la corte suprema del Massachusetts ha rigettato il mandato di perquisizione.

<http://www.schneier.com/blog/archives/2009/06/update_on_compu.html>

Questa serratura a combinazione è molto bella. Ovviamente quattro cifre è un codice d'accesso troppo breve, ma mi piace il design generale e la funzione di ricodifica automatica. È solo un prototipo, e non è nemmeno un oggetto fisico.

<<http://www.yankodesign.com/2009/05/29/twist-shout-about-forgotting-the-code/>>

oppure <<http://tinyurl.com/lcv4tj>>

Qualche tempo fa ho riportato sul mio blog di una penna per autodifesa così ben fatta da poter passare tranquillamente la sicurezza aeroportuale. Al contrario, questa penna normale in forma di pallottola probabilmente non farà altro che crearvi dei guai.

<<http://www.pencity.com/cgi-bin/SoftCart.exe/Fisher/375BulletBP.htm?L+scstore+zize0529+1244045830>>

oppure <<http://tinyurl.com/qtv8nn>>

<http://www.schneier.com/blog/archives/2009/03/self-defense_pe.html>

È di nuovo il momento per aver paura di terroristi che si servono di mappe e immagini. (Pensavo di aver scritto un buon post sull'argomento, ma questo mese Crypto-Gram è già fin troppo lunga. Leggetelo online, per favore).

<http://www.schneier.com/blog/archives/2009/06/fear_of_aerial.html>

Se pensate che ai teenager non importa la privacy, questo è un editoriale di opinione molto eloquente a opera di due studenti, sul perché le telecamere di sorveglianza siano del tutto fuori luogo nella loro scuola inglese.

<<http://www.guardian.co.uk/commentisfree/libertycentral/2009/jun/03/cctv-classroom>>

oppure <<http://tinyurl.com/pjtz2f>>

Ecco un sito che vende file MS Word corrotti. L'idea è quella di inviarli al proprio professore quando è ora di consegnare i compiti, guadagnando così qualche ora (o magari giorni) prima che il professore si accorga che è corrotto. Da un lato è un'idea brillante, ma dall'altro sono servizi come questi che costringeranno i professori a

trattare gli allegati corrotti come compiti non ancora consegnati, e danneggerà gli studenti in buona fede.

<<http://www.corrupted-files.com/Word.html>>

Ecco invece come creare un file PDF corrotto gratuitamente:

<<http://blog.didierstevens.com/2009/06/09/quickpost-make-your-own-corrupted-pdfs-for-free/>>

Insegnare ai bambini come riconoscere i terroristi: incredibile ma vero.

<http://www.schneier.com/blog/archives/2009/06/teaching_first-.html>

Differenze industriali che si evincono dai tipi di violazione della sicurezza.

<http://www.schneier.com/blog/archives/2009/06/industry_differ.html>

Un malware ruba le informazioni dei Bancomat:

<http://www.schneier.com/blog/archives/2009/06/malware_steals.html>

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

Il mio intervento sugli scanner del corpo intero negli aeroporti

Mi fa molto piacere questo riferimento al sottoscritto in una notizia di CNN.com sulla 'scansione del corpo intero' negli aeroporti:

"Bruce Schneier, un tecnologo di sicurezza rinomato a livello internazionale, ritiene che la tecnologia di scansione del corpo intero 'funziona piuttosto bene', diritti sulla privacy a parte. Egli però sostiene che l'investimento economico è stato un errore. In un mondo post-11 settembre, ha detto, sa che la sua posizione non è 'politicamente sostenibile', tuttavia egli crede che si farebbe meglio a investire denaro nella raccolta di intelligence e nelle indagini.

"È stupido investire denaro così che i terroristi possano cambiare i loro piani", ha detto Schneier al telefono dalla Polonia, dove stava intervenendo a una conferenza. "Se i terroristi vengono deviati dagli aeroporti, prenderanno di mira altri luoghi, come un hotel a Mumbai in India", ha detto".

"Faremmo meglio a perseguire i malviventi ... e a tornare ai livelli di sicurezza aeroportuale anteriori all'11 settembre", ha detto Schneier. "In politica esiste un grosso fattore, il 'pararsi le spalle', che purtroppo non ci rende più protetti".

Ho scritto in passato in merito alla sicurezza 'cover your ass' (lett. pararsi il didietro), ma fa piacere leggerlo nella stampa.

<<http://edition.cnn.com/2009/TRAVEL/05/18/airport.security.body.scans/?iref=mpstoryview>>

oppure <<http://tinyurl.com/le9skw>>

Il mio articolo sulla sicurezza CYA ('Cover Your Ass'):

<http://www.schneier.com/blog/archives/2007/02/cya_security_1.html>

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

Le news su Schneier

Marcus Ranum e io abbiamo realizzato due interventi video della nostra rubrica Face Off (Faccia a Faccia): uno sul cloud computing:

<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1355568,00.html>

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

E l'altro su chi dovrebbe essere l'incaricato per la sicurezza cibernetica:

<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1355883,00.html>

oppure <<http://tinyurl.com/p9eznn>>

Un'altra intervista con il sottoscritto in cui si parla di cloud computing:

<<http://www.vnunet.com/vnunet/video/2240924/bruce-schneier-cloud-security>>

oppure <<http://tinyurl.com/dlrv56>>

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

Il Canile: Net1

Dal sito Web: "Il brevetto FTS è stato acclamato dalle principali autorità crittografiche del mondo intero come il protocollo più sicuro e innovativo mai inventato per gestire transazioni smart card online e offline. Si veda il resoconto indipendente di Bruce Schneider [sic] nel suo libro intitolato "Applied Cryptography, seconda edizione, pubblicato alla fine degli anni Novanta".

Dopo aver postato questo sul mio blog, qualcuno -- probabilmente dell'azienda -- ha detto che si faceva riferimento al protocollo UEPS trattato a pag. 589. Comunque non mi piace il tono iperbolico e l'uso del mio nome nella citazione come approvazione implicita.

<<http://www.aplitech.co.za/Products/Security.html>>

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

Il cloud computing

Il concetto IT fortemente pubblicizzato quest'anno è il cloud computing. Detto anche 'software as a service' (SaaS), il cloud computing avviene quando si esegue software attraverso Internet e si accede a esso mediante il browser. Il software di gestione clienti di Salesforce.com è un esempio. Altro esempio è Google Docs. Se credete alla pubblicità, il cloud computing è il futuro.

Ma pubblicità e sensazionalismi a parte, il cloud computing non è nulla di nuovo. È la versione moderna del modello del timesharing che si usava negli anni Sessanta, che alla fine fu abbandonato a causa del crescente successo del personal computer. Cloud computing è quel che hanno fatto Hotmail e Gmail in questi anni, ed è quel che fanno i

siti di social networking, le aziende che offrono backup remoti, e le aziende di filtraggio della posta elettronica da remoto, come MessageLabs. Qualunque genere di outsourcing IT -- infrastruttura di rete, monitoring di sicurezza, hosting remoto -- è una forma di cloud computing.

Il vecchio modello di timesharing ebbe successo perché i computer erano costosi e difficili da mantenere. I computer e le reti di oggi sono drasticamente più economici, ma rimangono difficili da mantenere. Con l'aumentata velocità delle reti, è ancora una volta più facile far fare il lavoro sporco a qualcun altro. Il calcolo elettronico si è trasformato in un'utilità, e gli utenti sono maggiormente interessati ai risultati che non ai dettagli tecnici, per cui l'aspetto tecnico sfuma sullo sfondo.

E la sicurezza? Non è più pericoloso avere le proprie email sui server di Hotmail, i propri fogli di calcolo sui server di Google, le conversazioni personali sui server di Facebook e le previsioni di vendita della propria azienda sui server di Salesforce.com? Beh, sì e no.

La sicurezza IT ruota intorno alla fiducia. Occorre fidarsi di chi costruisce i microprocessori, dell'hardware, del sistema operativo, dei produttori di software, nonché del proprio Internet Provider. Uno qualsiasi di questi elementi può compromettere la nostra sicurezza: mandare in crash i sistemi, corrompere dati, permettere a un aggressore di ottenere accesso ai sistemi. Abbiamo speso decenni combattendo worm e rootkit che prendono di mira vulnerabilità nel software. Ci siamo preoccupati di chip infettati. Ma alla fine non abbiamo altra scelta se non quella di fidarci ciecamente della sicurezza dei fornitori IT di cui ci serviamo.

Il SaaS sposta il confine della fiducia a un livello ulteriore: adesso dobbiamo fidarci anche dei fornitori di questi servizi software, ma le cose non cambiano granché. È l'ennesima entità di cui ci si deve fidare.

Tuttavia esiste una differenza fondamentale. Quando un computer si trova all'interno della nostra rete, possiamo proteggerlo con altri sistemi di sicurezza, come firewall e IDS (sistemi anti-intrusione). È possibile costruire un sistema resistente che funziona anche nel caso in cui quei produttori di cui ci dobbiamo fidare non si rivelano così degni di fiducia. Con un modello di outsourcing, che si tratti di cloud computing o di altro, non è possibile. È necessario fidarsi totalmente del proprio outsourcer. E non solo bisogna fidarsi della sicurezza dell'outsourcer, ma anche della sua affidabilità, disponibilità, e continuità di business.

Non vogliamo che i nostri dati più importanti si trovino su qualche cloud computer che sparisce improvvisamente perché il proprietario è andato in bancarotta. Non vogliamo che l'azienda che stiamo utilizzando venga venduta al nostro diretto concorrente. Non vogliamo che l'azienda effettui dei tagli senza preavviso perché i tempi sono duri. O aumentare i suoi prezzi per poi rifiutarsi di restituire i nostri dati. Queste cose possono accadere con i produttori di software, ma i risultati non sono così drastici.

Esistono due tipi diversi di clienti del cloud computing. Il primo tipo paga solo una cifra simbolica per tali servizi, li usa gratuitamente e in cambio riceve pubblicità (esempi: Gmail, Facebook). Questo genere di clienti non hanno alcuna voce in capitolo nei confronti dell'outsourcer. Si possono perdere tutte le informazioni -- ad aziende come Google o Amazon importerà poco. Il secondo tipo di clientela paga una cifra considerevole per questi servizi: a Salesforce.com, MessageLabs, aziende di managed networking, e così via. Questa clientela ha maggior voce in capitolo, nel caso

ovviamente che tali aziende scrivano correttamente i loro contratti di servizio. In ogni caso nulla viene garantito.

La fiducia è un concetto antico quanto l'umanità, e le soluzioni sono sempre le stesse. Fare attenzione a chi diamo fiducia, fare attenzione a ciò che affidiamo a terzi, e fare attenzione a quanta fiducia si dà. Outsourcing è il futuro dell'elaborazione. Arriveremo a fare le cose per bene, ma nel frattempo cerchiamo di non cadere vittime strada facendo.

Questo articolo è originariamente apparso nel Guardian:

<<http://www.guardian.co.uk/technology/2009/jun/04/bruce-schneier-cloud-computing>>

oppure <<http://tinyurl.com/op7p7k>>

Un'altra opinione:

<http://1raindrop.typepad.com/1_raindrop/2009/06/begin-the-begin-cloud-security.html>

oppure <<http://tinyurl.com/mnc3lb>>

Un rifiuto:

<<http://www.rationalsurvivability.com/blog/?p=952>>

<<http://www.rationalsurvivability.com/blog/?p=1013>>

Il motivo per cui ultimamente parlo molto di cloud computing è che giornalisti e intervistatori continuano a farmi domande a riguardo. Mi sento un po' tirato dentro in tutta la questione.

Rimandi:

<<http://cacm.acm.org/magazines/2009/5/24642-the-rise-fall-and-resurrection-of-software-as-a-service/fulltext>>

<<http://www.infoworld.com/d/cloud-computing/what-do-if-your-cloud-provider-disappears-508>>

<<http://www.eweekeuropa.co.uk/news/cloud-computing-forerunner-facing-bankruptcy-772>>

<<http://www.techcrunch.com/2009/01/03/journalspace-drama-all-data-lost-without-backup-company-deadpooled/>>

<<http://news.zdnet.co.uk/internet/0,1000000097,39258170,00.htm>>

<<http://www.techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions/>>

<<http://www.mobileread.com/forums/showthread.php?t=44350>>

<<http://www.worldprivacyforum.org/cloudprivacy.html>>

Alla conferenza 'Computers, Freedom, and Privacy' Bob Gellman ha detto che le nove parole più importanti nel cloud computing sono "termini del servizio", "location, location, location" (cioè dove si trova il servizio) e "provider, provider, provider" -- facendo sostanzialmente un discorso analogo al mio. Occorre assicurarsi che i termini del servizio che si sottoscrivono siano accettabili. Occorre assicurarsi che la posizione geografica del provider non renda soggetti a leggi inaccettabili. E occorre assicurarsi che il provider sia qualcuno con cui si abbia voglia di lavorare. In sostanza, se dobbiamo fornire i nostri dati a qualcun altro, occorre fidarsi di lui.

<<http://www.worldprivacyforum.org/cloudprivacy.html>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:
<http://www.schneier.com/blog/archives/2009/06/cloud_computing.html>

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

Il Secondo Workshop Interdisciplinare sulla Sicurezza e il Comportamento Umano (Interdisciplinary Workshop on Security and Human Behaviour)

La scorsa settimana ho partecipato al SHB09, il Secondo Workshop Interdisciplinare sulla Sicurezza e il Comportamento Umano, che si è tenuto al MIT. È stato un incontro di due giorni, organizzato da Ross Anderson, Alessandro Acquisti e il sottoscritto, in cui sono convenuti ricercatori di sicurezza informatica, psicologi, economisti comportamentali, sociologi, filosofi e altre personalità -- tutti studiosi del lato umano della sicurezza. Mi sono occupato di fare un liveblogging del workshop; quanto segue sono i riassunti dei vari interventi. (Gli studiosi sono stati invitati ad aggiungere un link al proprio sito e link ai loro lavori in relazione con l'argomento trattato. Questi link si trovano alla fine di ogni riassunto).

Il tema della prima sessione, moderata da David Clark, era l'inganno.

Frank Stajano, Cambridge University, ha presentato una ricerca svolta insieme a Paul Wilson, che riprende truffe vere e proprie per la trasmissione "The Real Hustle". La sua tesi è che costruiamo sistemi di sicurezza basati sulla nostra 'logica', ma che gli utenti non seguono sempre la nostra logica. Sono i truffatori che comprendono veramente le azioni della gente, per cui dobbiamo capire quel che capiscono i truffatori. Elementi come la distrazione, l'avidità, i complici ignoti e l'acquiescenza sociale sono importanti.

<<http://www.cl.cam.ac.uk/~fms27/>>

Usability of Security Management: Defining the Permissions of Guests

<<http://www.cl.cam.ac.uk/~fms27/papers/2006-JohnsonSta-guests.pdf>>

David Livingstone Smith, University of New England, è un filosofo di formazione, e torna ai fondamentali: "Di cosa stiamo parlando?" Una definizione teorica -- "ciò che qualcosa deve avere per essere indicato da un termine" -- dell'inganno è difficile da tracciare. "Instillare una falsa credenza o convinzione", dall'Oxford English Dictionary, è una definizione inadeguata. "Ingannare significa operare intenzionalmente in modo che qualcuno abbia una falsa credenza o convinzione" -- neanche questa funziona. "Agire deliberatamente affinché qualcuno abbia una falsa credenza o convinzione che l'attore sa essere falsa" -- ancora, non è sufficientemente precisa. Il problema fondamentale è che tutte queste sono definizioni antropocentriche. L'inganno non è esclusivo degli uomini; offre agli organismi un margine evolutivo. L'orchidea specchio inganna la vespa inducendola a posarsi imitando e discernendo sostanze chimiche tipiche della vespa femmina. Questo esempio dimostra che abbiamo bisogno di una definizione di "scopo" più ampia. La sua definizione formale: "Per i sistemi A e B, A inganna B se A possiede un qualche attributo C con una funzione propria F, e B possiede un meccanismo C* con la funzione propria F* di produrre rappresentazioni, in modo che la funzione propria di C è quella di fare in modo che C* non riesca a eseguire F* inducendo C* a formare false rappresentazioni, e C può farlo eseguendo F*; e la falsa rappresentazione di B permette a qualche caratteristica di A di eseguire la sua propria funzione".

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

Less than human: self-deception in the imagining of others

<http://realhumannature.com/?page_id=61>

Un intervento sulla menzogna alla Ciudad de Las Ideas

<<http://www.laciudaddeideas.com/ciudad2/play.php?vid=106>>

Una discussione che è seguita:

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

Why War? - Perché la guerra

<http://realhumannature.com/?page_id=26>

Poi sono intervenuto io, sulla psicologia di Conficker, su come la mente umana si lasci ingannare in materia di sicurezza, e perché non si dovrebbero assumere scrittori di fantascienza per riflettere sui rischi del terrorismo (articolo che sarà pubblicato su Wired.com).

<<http://www.schneier.com/blog/archives/2009/04/conficker.html>>

<<http://www.schneier.com/essay-232.html>>

Dominic Johnson, University of Edinburgh, ha parlato del suo capitolo del volume Natural Security: A Darwinian Approach to a Dangerous World [Sicurezza naturale: un approccio darwiniano a un mondo pericoloso]. La vita ha un'esperienza di 3,5 miliardi di anni in materia di innovazione di sicurezza; consideriamo l'approccio della biologia alla sicurezza. Biomimica, ecologia, paleontologia, comportamento animale, psicologia evolutiva, immunologia, epidemiologia, selezione e adattamento sono tutti campi rilevanti. La ridondanza è uno strumento di sopravvivenza assai importante nelle specie. Ecco un esempio di adattamento: la minaccia dell'11 settembre era reale, e ne eravamo a conoscenza, ma non abbiamo fatto nulla in proposito. La tesi di Johnson: l'adattamento a minacce di sicurezza inusitate tende ad avvenire a seguito di grandi sciagure. Vi sono molti esempi storici a proposito, come Pearl Harbor. Fra le cause: bias sensoriali, psicologici, di leadership, organizzativi e politici -- tutte forze che ci spingono verso il mantenimento dello status quo. Quindi per noi è naturale adattarci malamente alle minacce di sicurezza del mondo moderno. Una persona fra il pubblico ha domandato se la teoria del controllo fosse in qualche modo rilevante in questo modello.

<<http://dominicdpjohnson.com/>>

Paradigm Shifts in Security Strategy

<<http://www.cl.cam.ac.uk/~rja14/shb09/johnsond1.pdf>>

Perceptions of victory and defeat

<<http://dominicdpjohnson.com/publications/books.html>>

Jeff Hancock, Cornell University, studia l'inganno interpersonale: come il modo in cui mentiamo fra noi si interseca con le tecnologie di comunicazione; e come le tecnologie modificano il nostro modo di mentire. Si può utilizzare la tecnologia per rilevare una menzogna? Malgrado le nuove tecnologie, le persone mentono per motivi tradizionali. Per esempio, sui siti di incontri, gli uomini tendono a mentire sulla propria altezza e le donne sul proprio peso. Anche la registrabilità di Internet cambia il nostro modo di mentire. Più una persona mente, più l'uso della prima persona singolare tende a diminuire. Hancock lo ha verificato in svariati contesti: come le persone si descrivono nelle chat room, e le dichiarazioni vere e false rilasciate dall'amministrazione Bush sull'11 settembre e sull'Iraq. L'effetto era maggiormente pronunciato quando i funzionari dell'amministrazione stavano rispondendo a domande dirette che non quando stavano leggendo affermazioni preparate.

<http://www.comm.cornell.edu/staff/employee/jeffrey_t_hancock.html>

On Lying and Being Lied To: A Linguistic Analysis of Deception in Computer-Mediated Communication

<<http://www.cl.cam.ac.uk/~rja14/shb09/hancock1.pdf>>

Separating Fact From Fiction: An Examination of Deceptive Self-Presentation in Online Dating Profiles

<<http://www.cl.cam.ac.uk/~rja14/shb09/hancock2.pdf>>

Il tema della seconda sessione era la frode. (I temi delle sessioni sono da considerarsi in senso generale. Si è cercato di raggruppare gli studiosi che trattavano temi correlati, ma di tanto in tanto occorre gestire l'eccezione e i limiti della programmazione dell'evento).

Julie Downs, Carnegie Mellon University, è una psicologa che studia il modo in cui le persone prendono decisioni, e ha parlato del phishing. Per determinare come le persone rispondono ai tentativi di phishing -- quali messaggi email aprono e quando fanno clic sui link -- ha osservato come i soggetti interagivano con la propria posta elettronica. La Downs ha scoperto che le strategie messe in atto dalla maggioranza dei soggetti per contrastare gli attacchi di phishing potevano funzionare 5-10 anni fa, ma non sono più sufficienti ora che i phisher si sono adattati. Ha anche scoperto che educare le persone sul phishing non le rendeva più efficienti nel rilevare tentativi di phishing, ma più soggette ad aver paura di svolgere qualsiasi attività online. Downs ha riscontrato questo tipo di reazione eccessiva fra vittime recenti di attacchi phishing, ma anche in questo caso i soggetti non erano migliori di altri nel distinguere messaggi email genuini da tentativi di phishing. Ciò che fa la differenza è la comprensione contestuale: come analizzare un URL, come e perché avvengono le truffe, che cosa fa SSL e cosa non fa.

<<http://sds.hss.cmu.edu/src/faculty/downs.php>>

Behavioral Response to Phishing Risk

<<http://www.cl.cam.ac.uk/~rja14/shb09/downs1.pdf>>

Parents' vaccination comprehension and decisions

<<http://www.cl.cam.ac.uk/~rja14/shb09/downs2.pdf>>

The Psychology of Food Consumption

<<http://www.cl.cam.ac.uk/~rja14/shb09/downs3.pdf>>

Jean Camp, Indiana University, studia le persone che corrono rischi online. Quattro punti principali: 1) "le persone creano modelli mentali da narrazioni interiori sul rischio", 2) "si agisce per attenuare un rischio solo se il rischio viene percepito come importante", 3) "la contestualizzazione del rischio può mostrare l'importanza di certi rischi", e 4) "la narrazione può far aumentare il desiderio e la capacità di utilizzare strumenti di sicurezza". Le storie sono importanti: "la gente è disposta a lavare le scatolette di cibo per gatti e di raccogliere i fiori di liquidambar per comportarsi da buoni vicini, ma lasciano che i propri computer si uniscano a reti di zombie" -- questo perché nel primo caso esiste una buona storia esemplare dietro, ma non è così nel secondo caso. Camp ha presentato due esperimenti per dimostrarlo. Uno era un esperimento video in cui dei responsabili commerciali venivano osservati mentre cercavano di installare PGP. Nessuno vi riuscì: non c'era narrativa, e la metafora mista di una 'chiave' fisica e crittografica confondeva i soggetti.

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

Experimental Evaluation of Expert and Non-expert Computer Users' Mental Models of Security Risks

<<http://www.cl.cam.ac.uk/~rja14/shb08/camp.pdf>>

Matt Blaze, University of Pennsylvania, ha parlato delle macchine per il voto elettronico e la frode. Ha narrato l'aneddoto sulla frode elettorale vera e propria accaduta nel Kentucky con una di queste macchine (vedere il secondo link). Durante la sessione di domanda e risposta, Blaze ha meditato sulla difficoltà di avere un modello di sicurezza

che avesse potuto individuare il problema, e come sapere se quel modello poteva essere sufficientemente completo.

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

Electronic vote rigging in Kentucky

<http://www.crypto.com/blog/vote_fraud_in_kentucky/>

Jeffrey Friedberg, Microsoft, ha discusso la ricerca che Microsoft sta compiendo intorno a TUX (Trust User Experience). Ha parlato della difficoltà di verificare i certificati SSL, e poi di come Microsoft ha aggiunto una 'barra verde' per indicare siti fidati, e di come i soggetti che hanno imparato a fidarsi della barra verde si siano fatti ingannare da attacchi 'picture in picture' in cui un sito Web ha incorporato nella sua pagina una finestra del browser con barra verde. Molte persone non si rendono conto che le informazioni all'interno della finestra del browser sono arbitrarie, ma che tutti gli elementi intorno a essa non lo sono. L'interfaccia utente, l'esperienza utente, i modelli mentali hanno tutti molta importanza. Progettare e valutare la TUX è difficile. Dalla sessione di domanda e risposta: l'addestramento non serve a molto, perché di fronte a una storia plausibile, le persone si comporteranno in maniera diversa rispetto a quanto appreso durante il training.

<<http://www.mccullagh.org/image/10d-14/jeffrey-friedberg-microsoft.html>>

Internet Fraud Battlefield

<<http://www.cl.cam.ac.uk/~rja14/shb09/friedberg.pdf>>

End to End Trust and the Trust User Experience

<http://www.microsoft.com/mscorp/twc/endtoendtrust/blogPosting.aspx?blogSource=20090423_friedberg.xml>

Testimony on "spyware"

<<http://www.microsoft.com/presspass/exec/friedberg/04-29spyware.mspx>>

Stuart Schechter, Microsoft, ha presentato una ricerca sulle domande segrete. In pratica, le domande segrete non funzionano. Si possono facilmente indovinare basandosi sulle risposte più comuni; parenti e amici possono facilmente prevedere risposte specifiche; e molte persone si dimenticano le domande. Ancora peggio, più memorabili sono le domande/risposte, più sono facili da indovinare. Fare in modo che le persone scrivano le proprie domande non è un metodo migliore: "Qual è il mio gruppo sanguigno?", "Quanto sono alto?".

<<http://www.eecs.harvard.edu/~stuart/>>

It's no secret

<<http://research.microsoft.com/pubs/79594/oakland09.pdf>>

The Emperor's New Security Indicators

<<http://usablesecurity.org/emperor/emperor.pdf>>

Tyler Moore, Harvard University, ha discusso i suoi studi empirici sul crimine online e le relative difese. I frodatori sono bravi a ingannare gli utenti, ma sono anche molto efficaci nello sfruttare i punti deboli dei professionisti IT per perpetuare l'infrastruttura necessaria a effettuare tali exploit su larga scala (mantenere pagine Web fasulle, inviare spam, riciclare i profitti attraverso i cosiddetti 'money mule', e via dicendo). Vi è un rifiuto molto diffuso fra i difensori a cooperare fra loro, e gli aggressori sfruttano questi limiti. Siamo più bravi a eliminare siti di phishing che a difenderci dai 'money mule' (ossia 'muli portasoldi', persone che vengono convinte a prestarsi per riciclare denaro). I difensori tendono a sistemare i problemi immediati, non i problemi sottostanti.

<<http://people.seas.harvard.edu/~tmoore/>>

The Consequences of Non-Cooperation in the Fight Against Phishing

<<http://people.seas.harvard.edu/~tmoore/ecrime08.pdf>>
Information Security Economics -- and Beyond
<http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf>

Nella fase di dibattito si è parlato molto delle relazioni fra i siti Web, come le banche, e gli utenti -- e di come questo vada a incidere sulla sicurezza, nel bene e nel male. Jean Camp non vuole avere una relazione con la sua banca, perché ciò la coinvolgerebbe eccessivamente nei confronti della banca (qualcuno fra il pubblico ha fatto notare che, in quanto contribuente, lei è già eccessivamente coinvolta). Angela Sasse ha detto che la metafora più corretta è "regole di ingaggio", piuttosto che relazioni.

La terza sessione si intitolava "Usabilità".

Andrew Patrick (NRC Canada fino al suo licenziamento di pochi giorni fa) ha parlato dei sistemi biometrici e del comportamento umano. I dati biometrici vengono utilizzati dappertutto: per le iscrizioni in palestra, a Disneyworld, alle frontiere internazionali. Il governo canadese sta valutando l'utilizzo della scansione dell'iride a distanza per eventi come le Olimpiadi del 2010. Esistono due problematiche di usabilità diverse: rispetto all'utente finale e rispetto al chi autentica. L'accettazione dei dati biometrici da parte delle persone dipende grandemente dal contesto. E naturalmente le informazioni biometriche non sono segrete. Patrick ha suggerito che per difenderci da questa proliferazione dell'utilizzo dei dati biometrici per l'autenticazione, ognuno dovrebbe pubblicarli. La spiegazione logica è che li stiamo pubblicando comunque; tanto vale farlo consciamente.

<<http://andrewpatrick.ca>>

Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems

<<http://www.andrewpatrick.ca/essays/fingerprint-concerns-performance-usability-and-acceptance-of-fingerprint-biometric-systems>>

Luke Church, Cambridge University, ha parlato di quel che lui chiama 'design incentrato sull'utente'. Esiste un'economia dell'usabilità: "Per semplificare alcune cose, dobbiamo renderne altre più complesse" -- pertanto ha senso rendere più facili le cose che vengono fatte più comunemente, a scapito di quelle fatte più raramente. Vi sono molti paralleli con la sicurezza. Il risultato è la cosiddetta 'appliancisation' (un premio a chi inventa un termine migliore): il culmine di comportamenti di sicurezza e di ciò che possono svolgere i sistemi, il tutto inserito in una serie di scelte dell'utente. In pratica si dà agli utenti un controllo significativo sulla propria sicurezza. Luke ha discusso i molti benefici e problemi di questo approccio.

<<http://www.lukechurch.net>>

SHB Position Paper

<<http://www.lukechurch.net/Professional/Publications/SHB-2009-06-TheUserExperienceOfComputerSecurity.pdf>>

Usability and the Common Criteria

<<http://www.lukechurch.net/Professional/Publications/WISA-2008-09-IntroducingUsabilityToTheCommonCriteria.pdf>>

Diana Smetters, Palo Alto Research Center, ha cominciato il suo intervento con queste premesse: si può insegnare agli utenti, ma non più di tanto, per cui è preferibile progettare attentamente i sistemi in modo da 1) ridurre al minimo quel che gli utenti devono imparare, 2) facilitare l'apprendimento di tali nozioni e 3) massimizzare i vantaggi che derivano da ciò che imparano. Troppo spesso la sicurezza si trova in

contrasto con il processo che permette di realizzare un lavoro. "Finché gli errori di configurazione (falsi allarmi) saranno comuni, ogni tecnologia che richiede agli utenti di osservare indicatori di sicurezza e di reagire a ciò che gli indicatori comunicano sarà destinata a fallire perché gli attacchi possono semplicemente mascherarsi da errori, e gli utenti li ignoreranno razionalmente". Smetters consiglia di venire incontro all'utente a metà del percorso costruendo nuovi modelli di sicurezza che soddisfino davvero le esigenze dell'utente. (Per esempio: il phishing è un problema di discrepanza fra ciò che l'utente ha in testa e la reale direzione dell'URL. SSL non funziona, ma come dovrebbero autenticarsi i siti Web di fronte agli utenti? La soluzione di Smetters sono i link protetti: un insieme di bookmark sicuri in browser protetti. Ha poi descritto un prototipo e i test effettuati con un gruppo di soggetti.

<<http://www.parc.com/about/people/176/diana-smetters.html>>

Breaking out of the browser to defend against phishing attacks

<<http://www.parc.com/publication/2068/breaking-out-of-the-browser-to-defend-against-phishing-attacks.html>>

Building secure mashups

<<http://www.parc.com/publication/2054/building-secure-mashups.html>>

Ad-hoc guesting: when exceptions are the rule

<http://www.usenix.org/event/upsec08/tech/full_papers/dalal/dalal.pdf>

Jon Callas, PGP Corporation, ha usato la metafora della "rupe della sicurezza": bisogna continuare a scalarla fino ad arrivare in cima, ed è arduo, per cui è più semplice rimanere sul fondo. Lui preferirebbe una "rampa della sicurezza", così che le persone possano fermarsi almeno a metà strada. La sua idea è quella di stabilire alcune policy - - criptatura delle email, regole per le chiavette USB -- e farle rispettare. Questo funziona molto bene nelle organizzazioni, dove il dipartimento IT ha un controllo dittatoriale sulla configurazione utente. Se non possiamo insegnare granché agli utenti, allora è il caso di imporre loro certe policy.

<<http://www.pgp.com/company/management.html>>

Improving Message Security With a Self-Assembling PKI

<<http://middleware.internet2.edu/pki03/presentations/03.pdf>>

Rob Reeder, Microsoft, ha presentato una possibile soluzione al problema delle domande segrete: l'autenticazione sociale. Il concetto di base è quello di utilizzare persone conosciute (fiduciari) che confermino la nostra identità e che attestino che abbiamo perduto la password. Poi ha descritto come funziona il protocollo, e ha illustrato alcuni esempi di attacchi e difese potenziali, nonché esperimenti di collaudo del protocollo. Nella sessione di domanda e risposta ha parlato di persone che si sono offerte come fiduciari, e del fatto che non sia un grosso problema implementare questa soluzione.

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

Expanding Grids for Visualizing and Authoring Computer Security Policies

<<http://www.robreeder.com/pubs/xGridsCHI2008.pdf>>

Lorrie Cranor, Carnegie Mellon University, ha parlato degli avvisi di sicurezza. La scelta migliore è quella di sistemare il pericolo; la seconda in ordine di importanza è quella di prevenirlo -- ma troppo spesso ci limitiamo a mettere in guardia le persone. Però, dato che solitamente i pericoli non sono così seri, la maggioranza degli utenti li ignora. "Spesso il software chiede conferma all'utente e fornisce informazioni scarse o nulle che aiutino l'utente a prendere una decisione". È preferibile utilizzare una qualche specie di analisi automatizzata che assista l'utente nel rispondere agli avvisi. Per i siti Web, per esempio, il sistema dovrebbe bloccare quei siti con una probabilità di rischio molto alta,

senza infastidire gli utenti se la probabilità di un pericolo è bassa; e aiutare gli utenti a prendere delle decisioni in tutte le situazioni a tinte grigie, per così dire. Cranor ha poi descritto un prototipo e ha presentato studi sugli utenti effettuati con il prototipo; il suo studio verrà presentato a USENIX Security ad agosto.

<<http://lorrie.cranor.org/>>

A Framework for Reasoning About the Human in the Loop

<<http://www.cylab.cmu.edu/default.aspx?id=2396>>

Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators

<<http://www.guanotronic.com/~serge/papers/chi09a.pdf>>

School of Phish: A Real-World Evaluation of Anti-Phishing Training

<http://www.cylab.cmu.edu/research/techreports/tr_cylab09002.html>

You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings

<<http://www.guanotronic.com/~serge/papers/warned.pdf>>

Gran parte della discussione si è incentrata sulla reale gravità del problema, e su quanta sicurezza è necessaria per essere sufficiente. Il gruppo ha anche parlato degli incentivi economici che le aziende hanno per sistemare oppure ignorare le problematiche di sicurezza, e se gli approcci di mercato (o, come lo ha chiamato Jean Camp, "the happy Libertarian market pony") siano sufficienti. Alcune aziende sono incentivate a convincere gli utenti ad agire in modo errato, o al limite a non fare nulla. Per esempio, i siti di social networking hanno maggior valore se gli utenti condividono ampiamente le proprie informazioni.

In un successivo dibattito si è parlato del whitelisting, e se funzionava o meno. Esiste il problema dei malviventi che riescano a entrare nelle white list (liste bianche), e il rischio che organizzazioni come la RIAA sfruttino la lista bianca per far rispettare il copyright, o che le grandi banche sfruttino la lista bianca come strumento per fermare banche più piccole e appena fondate. Un altro problema è che l'utente potrebbe non capire che cosa significhi una lista bianca.

Dave Clark, dal pubblico: "Non è difficile mettersi una cintura di sicurezza, e se serve una lezione si prenda un aereo". Si è trattato di una sessione un po' monotematica: dobbiamo assolutamente invitare più psicologi la prossima volta.

David Livingstone Smith ha moderato la quarta sessione, nella quale si è parlato grosso modo di metodologia.

Angela Sasse, University College London, ha lavorato sulla sicurezza usabile per più di dieci anni. Come parte di un progetto chiamato 'Trust Economics', ha osservato se le persone si conformano alle policy di sicurezza e perché lo fanno o non lo fanno. Ha scoperto che esiste un limite allo sforzo che si è disposti a fare per conformarsi -- si tratta più di costo percepito che di costo effettivo. Policy rigorose e semplici verranno rispettate molto più di policy permissive ma complesse. Il processo di verifica della conformità, e l'eventuale premio o sanzione, sono altri elementi che influiscono sulla volontà di conformarsi. Le persone giustificano la non conformità con "scuse frequentemente addotte".

<<http://www.cs.ucl.ac.uk/staff/a.sasse/>>

The Compliance Budget: Managing Security Behaviour in Organisations

<http://hornbeam.cs.ucl.ac.uk/hcs/publications/Beautement+Sasse+Wonham_The%20Compliance%20Budget_Managing%20Security%20Behaviour%20in%20Organisations_NSPW2008.pdf>

Human Vulnerabilities in Security Systems

<<http://www.ktn.ginetiq-tim.net/files/Public/whitepapers/HFWG%20White%20Paperfinal.pdf>>

Bashar Nuseibeh, Open University, ha parlato della sicurezza sui cellulari; nello specifico, della sicurezza di Facebook sui cellulari e dispositivi mobili. Ha fatto una cosa brillante nei suoi esperimenti. Dato che non poteva intervistare le persone nel momento in cui stavano facendo qualcosa (stava interagendo con utenti 'mobili'), ha chiesto loro di fornire una 'frase mnemonica' che gli permettesse di condurre efficacemente le interviste in un secondo momento. Il sistema ha funzionato molto bene, e ha prodotto tutta una serie di informazioni sul perché le persone avevano preso delle decisioni di privacy precedentemente.

A Multi-Pronged Empirical Approach to Mobile Privacy Investigation

<<http://mcs.open.ac.uk/ban25/>>

Security Requirements Engineering: A Framework for Representation and Analysis

<http://mcs.open.ac.uk/ban25/papers/Haley-TSE-04359475-for_web.pdf>

James Pita, University of Southern California, studia il personale di sicurezza che deve sorvegliare un determinato luogo. Nella sua analisi vi sono risorse limitate -- guardie, telecamere, ecc. -- e un insieme di luoghi che devono essere custoditi. Un esempio potrebbe essere l'aeroporto di Los Angeles, dove un numero finito di unità K-9 deve sorvegliare otto terminal. Il suo modello utilizza un gioco di Stackelberg per ridurre al minimo la prevedibilità (altrimenti l'avversario potrebbe apprendere i punti deboli del sistema e sfruttarli a proprio vantaggio) e massimizzando la sicurezza al tempo stesso. Esistono delle complicazioni -- incertezza osservativa e razionalità limitata degli aggressori -- che ha cercato di includere nel proprio modello.

<<http://teamcore.usc.edu/pita/>>

<<http://mcs.open.ac.uk/ban25/papers/chi2008-Mancini-et-al.pdf>>

Deployed ARMOR Protection: The Application of a Game Theoretic Model for Security at the Los Angeles International Airport

<<http://teamcore.usc.edu/pita/publications/2008/AAMASind2008Final.pdf>>

Markus Jakobsson, Palo Alto Research Center, ha fatto notare che gli assicuratori auto chiedono alle persone se fumano per avere un'idea se tendono a mettere in atto comportamenti ad alto rischio. Nel suo esperimento, ha selezionato cento persone che sono state vittima di frodi online e cento persone che non lo sono state. Ha poi chiesto loro di completare un questionario riguardante vari rischi per la persona, come l'alpinismo o il buttarsi con un paracadute; rischi finanziari, come l'acquisto di azioni e di beni immobili; e rischi legati a Internet, come visitare siti porno e utilizzare reti Wi-Fi pubbliche. Jakobsson ha riscontrato una correlazione significativa fra rischi diversi, ma non ho notato emergere un pattern generale. Durante il dibattito, molte persone avevano domande sui dati raccolti. È necessaria un'ulteriore analisi, e probabilmente una maggior quantità di dati. A essere onesti, bisogna dire che Jakobsson non ha ancora ultimato la sua analisi.

<<http://www.informatics.indiana.edu/markus/>>

Male, late with your credit card payment, and like to speed? You will be phished!

<<http://www.cl.cam.ac.uk/~rja14/shb09/jakobsson-shb09.pdf>>

Social Phishing

<<http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf>>

Love and Authentication

<<http://www.ravenwhite.com/files/chi08JSWY.pdf>>

Quantifying the Security of Preference-Based Authentication

<<http://www.ravenwhite.com/files/quantifying.pdf>>

Rachel Greenstadt, Drexel University, ha discusso le modalità con cui uomini e macchine possono collaborare nel prendere decisioni di sicurezza. Tali decisioni sono difficili per svariate ragioni: perché dipendono dal contesto, richiedono conoscenze specifiche, sono dinamiche, e richiedono una complessa analisi dei rischi. E uomini e macchine sono molto abili nello svolgere compiti diversi. Modo di autenticare di una macchina: La persona accanto a me conosce la chiave privata di Jake, per cui deve essere Jake. Modo di autenticare di un essere umano: La persona accanto a me assomiglia a Jake e ha la stessa voce di Jake, per cui deve essere Jake. Il punto è progettare sistemi che prendano la parte migliore di questi due sistemi di autenticazione, e non la peggiore. Greenstadt ha poi descritto due esperimenti che prendevano in esame due decisioni: "dovrei effettuare il login in questo sito?" (il problema del phishing) e "dovrei pubblicare questo articolo in forma anonima o il mio stile linguistico mi tradirà?".

<<http://www.cs.drexel.edu/~greenie>>

Practical Attacks Against Authorship Recognition Techniques (pre-print)

<http://www.cs.drexel.edu/~greenie/brennan_paper.pdf>

Reinterpreting the Disclosure Debate for Web Infections

<<http://weis2008.econinfosec.org/papers/Greenstadt.pdf>>

Mike Roe, Microsoft, ha parlato del crimine nei giochi online, specialmente in Second Life e Metaplace. Nei giochi online esistono quattro classi di persone: explorers (gli esploratori), socializers (i socializzatori), achievers (persone di successo, che puntano al successo) e griefer (persone che causano problemi e portano scompiglio). I 'griefer' cercano di infastidire i 'socializer' in mondi sociali come Second Life, o cercano di infastidire gli 'achiever' in mondi competitivi come World of Warcraft. Il crimine non è necessariamente di natura economica; criminali che cercano di rubare denaro in questi giochi sono un problema minore rispetto a chi cerca unicamente di interferire. Durante la sessione di domanda e risposta, Dave Clark ha detto che i 'griefer' sono una costante, ma la frode economica cresce nel tempo. Io ho risposto che i due tipi di aggressori sono persone diverse, con profili di personalità diversi. Ho anche fatto notare che esiste un altro genere di aggressore: gli 'achiever' che si servono di meccanismi illegali per avvantaggiarsi.

<<http://research.microsoft.com/users/mroe/>>

Durante la discussione, Peter Neumann ha fatto presente come la sicurezza (intesa come incolumità) sia una proprietà emergente, e che richiede sicurezza, affidabilità, e sopravvivenibilità. Altri erano incerti a riguardo.

La prima sessione del secondo giorno si intitolava "Fondamenta", sorta di tema jolly per riunire una serie di interventi che esulavano da altre sessioni. La moderatrice è stata Rachel Greenstadt.

Terence Taylor, International Council for the Live Sciences, ha parlato delle lezioni che insegna l'evoluzione per quanto riguarda il vivere in stretto rapporto con il rischio. Le varie specie che sono sopravvissute non sono riuscite nell'intento attraverso l'eliminazione dei rischi nel loro ambiente: sono sopravvissute grazie all'adattamento. Non sempre l'adattamento è quel che pensiamo. Per esempio, si potrebbe vedere la caduta dell'Unione Sovietica come incapacità di adattamento, ma si può anche considerarla un'ottima forma di adattamento. Il rischio è importante e necessario per la sopravvivenza di una società, perché coloro che sono disposti a rischiare sono le

persone che guidano il cambiamento. Durante il dibattito, John Mueller ha evidenziato una differenza essenziale fra i sistemi umani e biologici: gli esseri umani tendono a rispondere in maniera drammatica di fronte a eventi anomali (gli attacchi all'antrace), mentre i sistemi biologici rispondono a fronte di un cambiamento sostenuto. E David Livingstone Smith ha fatto una domanda sulla differenza fra l'adattamento biologico che influenza il buon esito riproduttivo dei geni di un organismo, anche a scapito dell'organismo stesso, e l'adattamento di sicurezza. (Consiglio il libro che ha curato: Natural Security: A Darwinian Approach to a Dangerous World).

<<http://www.icscharter.org/people.html>>

Darwinian Security

<<http://www.darwiniansecurity.org>>

Natural Security

<<http://www.youtube.com/watch?v=job2avPAbgU>>

Andrew Odlyzko, University of Minnesota, ha discusso lo spazio umano e il cyberspazio. Non possiamo costruire sistemi sicuri -- è risaputo -- ma non possiamo nemmeno tollerarli. Abbiamo bisogno di una certa flessibilità nei nostri sistemi. E infine, non abbiamo bisogno di sistemi sicuri. Riusciamo a sopravvivere malgrado l'enorme insicurezza che ci circonda. Il problema del cyberspazio è che è stato originariamente concepito come una realtà separata dal mondo fisico, e che avrebbe potuto correggere le inadeguatezze del mondo fisico. In realtà i due mondi sono intrecciati e spesso è lo spazio umano a correggere le inadeguatezze del cyberspazio. Lezioni: costruire sistemi caotici, non ordinati; creare una rete di collegamenti verso altri sistemi; creare archivi permanenti.

<<http://www.dtc.umn.edu/~odlyzko/>>

Network Neutrality, Search Neutrality, and the Never-Ending Conflict Between Efficiency and Fairness in Markets

<<http://www.cl.cam.ac.uk/~rja14/shb09/odlyzko.pdf>>

Economics, psychology, and sociology of security

<<http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf>>

Danah Boyd, Microsoft Research, svolge studi etnografici sui teenager nel cyberspazio. I ragazzi tendono a non mentire ai loro amici nel cyberspazio, ma mentono al sistema. Sin da piccoli è stato loro insegnato a mentire online per proteggersi. I teenager condividono regolarmente le proprie password: con i loro genitori se costretti, o con il proprio migliore amico o partner. È un modo per dimostrare fiducia. È parte del protocollo sociale di questa generazione. In generale, i teenager non utilizzano i media sociali allo stesso modo degli adulti. E quando cresceranno non utilizzeranno i media sociali come li stanno utilizzando gli adulti di oggi. I ragazzi vedono la privacy in termini di controllo, e basano la loro visione della privacy prendendo a modello le celebrità e come loro si servono dei media sociali. Il loro senso della privacy è molto più complicato e ricco di sfumature. Durante il dibattito, Danah non era sicura se la generazione più giovane sia più o meno predisposta a lasciarsi ingannare dalle frodi in Internet rispetto a noi -- questi ragazzi sono molto meno esperti tecnicamente di quanto possiamo pensare. "L'unica cosa che salva i teenager è la paura dei loro genitori"; cercano quindi di chiuderli fuori, e così facendo chiudono fuori anche altre persone. Lo status socio-economico ha grande importanza, in modalità che Danah sta ancora cercando di analizzare. Esistono tre diversi tipi di reti sociali: reti personali, reti articolate e reti comportamentali, molto diversi l'una dall'altra.

<<http://www.danah.org>>

Taken Out of Context -- American Teen Sociality in Networked Publics

<<http://www.danah.org/papers/TakenOutOfContext.pdf>>

Mark Levine, Lancaster University, ha raccolto dati dalle telecamere CCTV di sorveglianza del Regno Unito. Egli ricerca comportamenti aggressivi e studia quando e in che modo gli astanti contribuiscano ad aggravare o a 'raffreddare' le situazioni. I risultati: con l'estendersi dei gruppi non vi è aumento di atti antisociali, se mai un aumento significativo di atti pro-sociali. Levine è in possesso di molti altri dati e ha effettuato tutta una serie di analisi che è troppo complicato riassumere qui. Una scoperta importante: quando una terza parte interviene in un'interazione aggressiva, è assai più probabile che la situazione scenda di intensità. In sostanza, i gruppi possono agire contro la violenza. "Quando si tratta di violenza (e sicurezza), i processi di gruppo sono parte della soluzione -- non parte del problema".

<<http://www.psych.lancs.ac.uk/people/MarkLevine.html>>

The Kindness of Crowds

<http://www.economist.com/science/displaystory.cfm?story_id=13176759>

Intra-group Regulation of Violence: Bystanders and the (De)-escalation of Violence

<<http://www.cl.cam.ac.uk/~rja14/shb09/levine1.pdf>>

Jeff MacKie-Mason, University of Michigan, è un economista: "I problemi di sicurezza sono problemi di incentivi". Ha parlato della motivazione, e di come realizzare sistemi che ne tengano conto. Gli esseri umani sono dispositivi intelligenti; non possono essere programmati, ma possono venire influenzati mediante le scienze del comportamento motivazionale: microeconomia, teoria del gioco, psicologia sociale, psicodinamica, e psicologia della personalità. Ha fatto un paio di esempi generali di come queste teorie possano guidare il progetto di sistemi di sicurezza.

<<http://jeff-mason.com>>

Humans are smart devices, but not programmable

<<http://www.cl.cam.ac.uk/~rja14/shb09/mackie-mason.pdf>>

Security when people matter

<<http://hdl.handle.net/2027.42/55773>>

A Social Mechanism for Supporting Home Computer Security

<<http://hdl.handle.net/2027.42/63006>>

Joe Bonneau, Cambridge University, ha parlato di reti sociali, come Facebook, e di privacy. Le persone fraintendono il perché la privacy e la sicurezza siano importanti in siti di social networking come Facebook. E sottovalutano ciò che Facebook è in realtà, ovvero una reimplementazione dell'intera Internet. "Ogni cosa su Internet sta diventando sociale", e questo fa cambiare la sicurezza. Il phishing è cambiato, le truffe stile 419 sono cambiate. Il contesto sociale facilita la messa in atto di alcune truffe; le reti sociali sono divertenti, rumorose e imprevedibili. "Le persone utilizzano i sistemi di social networking con il cervello spento". Ma il contesto sociale può servire anche a individuare frodi e anomalie, e può essere utilizzato per stabilire fiducia.

<<http://www.cl.cam.ac.uk/~jcb82/>>

Sesta sessione, "Il terrore", moderata da Stuart Schechter.

Bill Burns, Decision Research, studia la reazione sociale al rischio. Ha discusso il suo modello teorico di come le persone reagiscono a eventi di terrore, e ha discusso i dati degli attacchi dell'11 settembre, degli attentati dinamitardi del 7 luglio nel Regno Unito, e del collasso finanziario del 2008. In sostanza, non possiamo rimanere in uno stato di timore. A prescindere da quel che avviene, il terrore ha il suo picco massimo immediatamente dopo l'evento, e sfuma all'incirca 45 giorni dopo. Secondo Burns,

l'errore più grave che abbiamo commesso dopo l'11 settembre è stato quello di etichettare l'evento come atto terroristico invece che atto criminoso internazionale.

<<http://www.decisionresearch.org/people/burns/>>

The Diffusion of Fear: Modeling Community Response to a Terrorist Strike

<<http://www.cl.cam.ac.uk/~rja14/shb08/burns.pdf>>

Chris Cocking, London Metropolitan University, esamina il comportamento di gruppo di persone che reagiscono a situazioni di emergenza. Tradizionalmente, gran parte della pianificazione di emergenze si basa sul modello del panico: le persone che compongono una folla sono soggette a comportamenti irrazionali e si fanno prendere dal panico. Esiste anche un modello di legame sociale che prevede che le norme sociali non vengono violate in gruppi di persone. Cocking preferisce un approccio di auto-categorizzazione: le sciagure creano un'identità comune, che genera un comportamento disciplinato e altruistico fra estranei. Più grande la minaccia, più grande sarà questa identità comune, ed è possibile che si crei una resistenza spontanea all'evento. Ha mostrato una fotografia di 'panico' a New York l'11 settembre 2001 e ha fatto notare come non fosse affatto panico. Il panico sembra essere più un mito che una realtà. Ciò presenta delle conseguenze a livello di linee di condotta durante un evento di emergenza: se si passano informazioni alle persone, queste tenderanno a non reagire in maniera eccessiva e incontrollata; se vi è una reazione esagerata è perché le persone stanno agendo come individui e non come gruppi, pertanto chi si trova in una posizione di autorità dovrebbe incoraggiare un senso di identità collettiva. "Le folle possono essere parte della soluzione, non del problema".

<<http://news.bbc.co.uk/1/hi/uk/4702659.stm>>

Effects of social identity on responses to emergency mass evacuation

<<http://www.sussex.ac.uk/affiliates/panic/>>

Richard John, University of Southern California, ha parlato del processo di amplificazione sociale del rischio (in ambito di terrorismo). Gli eventi di per sé causano un numero di vittime relativamente basso; sono i cambiamenti a livello comportamentale successivi a un evento che fanno aumentare il numero di vittime. Esiste una dinamica della percezione del rischio, e dipende moltissimo dal contesto. John si serve di illustrazioni per studiare come la percezione del rischio cambia nel tempo, e ha discusso alcuni degli studi che sta conducendo, e idee per studi futuri.

<<http://www.usc.edu/schools/college/psyc/people/faculty1003386.html>>

Decision Analysis by Proxy for the Rational Terrorist

<<http://www.cl.cam.ac.uk/~rja14/shb09/john1.pdf>>

Mark Stewart, University of Newcastle, Australia, prende in esame la sicurezza dell'infrastruttura e se i costi superano i benefici. Ha parlato di compromessi costi/benefici e di come applicare la valutazione probabilistica del rischio terrorismo; poi ha cercato di applicare questo modello allo U.S. Federal Air Marshal Service. Il suo risultato: il servizio non vale il costo. Si può cavillare sui suoi dati, ma il valore reale è un processo trasparente. Durante il dibattito ho detto che è importante rendersi conto che i rischi non si possono considerare in isolamento gli uni dagli altri, che chiunque scenda a un compromesso di sicurezza sta soppesando svariati rischi: rischi di terrorismo, rischi politici, i rischi personali inerenti alla propria carriera, ecc.

<<http://www.newcastle.edu.au/research-centre/cipar/>>

A risk and cost-benefit assessment of United States aviation security measures

<<http://polisci.osu.edu/faculty/jmueller/STEWJTS.PDF>>

Risk and Cost-Benefit Assessment of Counter-Terrorism Protective Measures to Infrastructure

<<http://nova.newcastle.edu.au/vital/access/manager/Repository/uon:3125>>

John Adams, University College London, applica al terrorismo il suo modello di termostato di rischio. Ha presentato una serie di fotografie divertenti che illustravano reazioni esagerate al rischio, la maggior parte delle quali non si riferivano tanto all'avversione per il rischio, quanto all'avversione per la responsabilità. Ha parlato della paranoia burocratica, nonché degli incoraggiamenti burocratici alla paranoia, e di come tutto questo stia cominciando ad avere un effetto contrario a quanto sperato. Le persone trattano i rischi in modi diversi, a seconda che siano volontari, impersonali o imposti e a seconda del livello di controllo (totale, ridotto, nullo) che hanno sui rischi.

<<http://john-adams.co.uk/about/>>

Deus e Brasileiro?

<<http://john-adams.co.uk/2008/12/31/deus-e-brasileiro/>>

Can Science Beat Terrorism?

<<http://john-adams.co.uk/2009/03/06/the-world-under-assault-can-science-beat-terrorism/>>

Bicycle bombs: a further inquiry

<<http://john-adams.co.uk/2009/01/16/bicycle-bombs-a-further-enquiry-and-a-new-theory/>>

Dan Gardner, Ottawa Citizen, ha parlato di come i mass media trattano i rischi, le minacce, gli attacchi, e così via. Ha parlato dei vari modi con cui i media sbagliano, tutti ben noti ai presenti. Secondo la sua tesi, non è che i media presentino le cose in maniera erronea o alterata per aumentare l'audience e quindi i profitti, ma che i media si comportano così perché i reporter sono esseri umani. La propensione alle cattive notizie non è il risultato dell'ingigantire quelle notizie da parte dei media, ma della naturale tendenza umana a ricordare eventi negativi più degli eventi positivi. Le news serali si incentrano sulle storie perché la gente, reporter compresi, reagisce alle storie, e le vicende con elementi di novità, emozione e dramma sono storie migliori.

<<http://www.amazon.com/Science-Fear-Shouldnt-Ourselves-Greater/dp/0525950621>>

Parte del dibattito ha riguardato la natura del panico: se esiste e dove, e qual è il suo volto. Qualcuno del pubblico ha domandato se il panico potesse essere in rapporto con la vicinanza all'evento; qualcun altro ha fatto notare come persone molto vicine ai luoghi delle bombe del 7 luglio scattavano fotografie e facevano telefonate -- e che non vi era alcun segnale di panico. Inoltre l'11 settembre la quasi totalità delle persone che si trovavano al di sotto del punto in cui avvenne l'impatto fra gli aerei e le Torri Gemelle uscirono dall'edificio sane e salve; e chi si trovava al di sopra non poté uscire e morì. Angela Sasse ha rilevato che il precedente attacco contro il World Trade Center e i conseguenti cambiamenti effettuati nelle procedure di evacuazione hanno contribuito alla mancanza di panico l'11 settembre. Bill Burns ha detto che il ritratto della più pura forma di panico è una persona che sta annegando. Jean Camp ha chiesto se i recenti attentati contro centri di salute per la donna debbano essere classificati come atti terroristici, o se è meglio trattarli come reati. Si è parlato anche degli sky marshal e della loro efficacia. Io sono intervenuto dicendo che non sono gli sky marshal a essere il deterrente, ma l'idea degli sky marshal. Terence Taylor ha detto che aumentare l'incertezza fra i terroristi è di per sé una misura di sicurezza. Si è anche dibattuto su quanto i terroristi siano avversi al rischio: pare che vogliano credere di avere una probabilità di successo dell'80-90% prima di sferrare un attacco.

La penultima sessione della conferenza aveva come tema la privacy, ed è stata moderata da Tyler Moore.

Alessandro Acquisti, Carnegie Mellon University, ha presentato una ricerca su come le persone valutano la propria privacy. Ha iniziato elencando una varietà di bias cognitivi che influenzano le decisioni di privacy: illusione di controllo, eccessiva sicurezza di sé, bias ottimistico, effetto di dotazione, e così via. Ha poi discusso due esperimenti. Il primo dimostrava un 'effetto gregario': se un soggetto crede che altri stiano manifestando un comportamento sensibile, sarà più propenso a manifestare a sua volta un simile comportamento. Il secondo prendeva in esame l'effetto rana: le intrusioni nella privacy rendono le persone più guardinghe o le desensibilizzano per quanto riguarda il rivelare informazioni personali? Quel che ha scoperto è che le persone tendono a impostare il proprio livello di privacy all'inizio di un sondaggio, e non reagiscono favorevolmente se interpellate con domande semplici all'inizio e domande più personali alla fine. Nel dibattito, Joe Bonneau ha chiesto ad Acquisti se le protezioni della privacy messe in atto dalle persone tendono ad aumentare con il tempo; Acquisti non aveva prove conclusive, ma ha fornito diverse possibili spiegazioni del fenomeno.

<<http://www.heinz.cmu.edu/~acquisti/>>

What Can Behavioral Economics Teach Us About Privacy?

<<http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf>>

Privacy in Electronic Commerce and the Economics of Immediate Gratification

<<http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf>>

Anche Adam Joinson, University of Bath, studia come le persone valutano la propria privacy. Ha parlato di privacy espressiva, ossia privacy che permette alle persone di esprimersi e di formare relazioni interpersonali. La sua ricerca ha mostrato come le differenze nell'uso di Facebook in paesi diversi dipendono da quanto la gente si fidi di Facebook come azienda, e non dal livello di fiducia verso altri utenti di Facebook. Un altro studio ha preso in esame entrate di Secret Tweet e Twitter. Joinson ha rilevato 16 marcatori che gli hanno permesso di determinare automaticamente quali tweet contenevano informazioni personali sensibili e quali no, con un alto livello di probabilità. Poi ha tentato di determinare se le persone con un largo seguito in Twitter pubblicassero meno segreti rispetto a chi avesse solo pochi seguaci. Non ha rilevato alcuna differenza.

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

Privacy, Trust and Self-Disclosure Online

<http://people.bath.ac.uk/aj266/pubs_pdf/joinson_et_al_HCI_final.pdf>

Privacy concerns and privacy actions

<http://people.bath.ac.uk/aj266/pubs_pdf/ijhcs.pdf>

Peter Neumann, SRI, ha parlato della mancanza di privacy sanitaria (troppe persone hanno accesso alle nostre informazioni sanitarie), del voto (il problema della privacy rende ancora più arduo il problema del voto, e il problema sicurezza del voto / privacy, da cima a fondo, va ben al di là della semplice protezione delle macchine per il voto), e della privacy in Cina (il governo richiede che tutti i computer venduti in Cina contengano un software che permetta di spiare gli utenti). Qualsiasi possibile soluzione deve poter riflettere l'ubiquità della minaccia. Quando progettiamo dei sistemi, dobbiamo anticipare quali saranno i problemi relativi alla privacy. I problemi di privacy sono dappertutto, e la gente comune non ha idea della profondità della questione.

<<http://www.csl.sri.com/users/neumann/>>

Holistic systems

<<http://www.csl.sri.com/neumann/holistic.pdf>>

Risks

<<http://www.csl.sri.com/users/neumann/#3>>

Identity and Trust in Context

<<http://www.csl.sri.com/neumann/idtrust09+x4.pdf>>

Eric Johnson, Dartmouth College, studia il problema dell'accesso alle informazioni da un punto di vista aziendale. Ha svolto studi sul campo in aziende come banche commerciali e banche d'investimenti, e ha rilevato che il controllo accessi basato sul ruolo non funziona, poiché le compagnie non riescono a determinare chi è in possesso di quel ruolo. A peggiorare le cose, i ruoli cambiano rapidamente, specialmente in organizzazioni vaste e complesse. Per esempio, un gruppo commerciale di 3.000 persone sperimenta 1.000 cambi di ruolo nel giro di tre mesi. Il risultato è che le aziende effettuano un controllo accessi mediocre, sia aumentando che restringendo eccessivamente il raggio d'azione dei dipendenti. Ma dato che terminare il lavoro è la cosa più importante, le aziende tendono a concedere troppi permessi, ovvero dare ai dipendenti un accesso maggiore del necessario. Il suo compito attuale è ricavare il giusto insieme di incentivi e controlli per impostare gli accessi in maniera più adeguata. La sfida è riuscire nell'intento senza che le persone diventino avverse ai rischi. Nel dibattito, ha riconosciuto l'impossibilità di creare un sistema di controllo accessi perfetto, e che probabilmente le aziende dovrebbero permettere eventuali violazioni del controllo degli accessi, analogamente all'imporre un limite di velocità di 55 miglia orarie, senza però multare chi supera questo limite ma sta sotto le 70 miglia orarie.

<<http://mba.tuck.dartmouth.edu/pages/faculty/eric.johnson/>>

Access Flexibility with Escalation and Audit

<http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/wise_v1.pdf>

Security through Information Risk Management

<http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/JohnsonRiskManagement_Finald.pdf>

Christine Jolls, Yale Law School, ha osservato come le persone condividono regolarmente le loro informazioni più private con i propri amici più intimi, pertanto la privacy non è questione di segretezza, ma riguarda più che altro il controllo. Vi sono momenti in cui le persone prendono decisioni di privacy molto importanti. Per esempio, concedono ai propri datori di lavoro il diritto di controllare le loro email o di effettuare test delle urine senza preavviso. In generale, i tribunali stabiliscono che il concedere diritti di privacy in forma generica e indefinita -- "dò il permesso di prendere un campione della mia urina un giorno qualsiasi in futuro" -- non è valido, ma lo è la concessione di diritti di privacy per circostanze immediate -- "dò il permesso di prendere un campione della mia urina oggi". Jolls ritiene che questo sia ragionevole per vari motivi, come il bias ottimistico e una maggiore concentrazione sul presente a scapito del futuro. Senza rendersene conto, i tribunali hanno implementato un sistema che l'economia comportamentale riterrebbe ottimale. Durante il dibattito, Jolls ha parlato del ruolo che la coercizione ha in tutto questo: il sistema legale degli Stati Uniti tende a non preoccuparsene.

<<http://www.law.yale.edu/faculty/CJolls.htm>>

Rationality and Consent in Privacy Law

<<http://www.cl.cam.ac.uk/~rja14/shb09/jolls1.pdf>>

Employee Privacy

<<http://www.cl.cam.ac.uk/~rja14/shb09/jolls2.pdf>>

Anche Andrew Adams, University of Reading, osserva il ruolo della privacy nei servizi di social networking. I suoi risultati sono preliminari e si basano su interviste con studenti universitari in Canada, Giappone e Regno Unito, e concordano notevolmente con quanto sostenuto da Danah Boyd e Joe Bonneau. Nel Regno Unito: le persone entrano

nei siti di social networking per aumentare il proprio livello di interazione con persone che già conoscono nella vita reale. Rivelare informazioni personali va bene, ma rivelare troppo no. Ancor più interessante, non va bene rivelare di altre persone più di quanto esse non rivelino di sé. In Giappone: le persone sono molto più aperte a creare amicizie online. C'è più anonimato. Non va bene rivelare informazioni di altre persone, ma "l'errore è anche della persona della quale si sono rivelate certe informazioni, perché non ha scelto i propri amici in maniera giudiziosa". Questa responsabilità della vittima è un tema comune ad altri elementi di privacy e sicurezza in Giappone. I dati del Canada sono ancora in fase di elaborazione.

<<http://www.personal.rdg.ac.uk/~sis00aaa/>>

Regulating CCTV

<<http://deposit.depot.edina.ac.uk/119/>>

Un'ottima espressione: la 'regione del bucato' ('laundry belt'): abbastanza vicino da permettere agli studenti di tornare a casa ogni finesettimana con la biancheria da lavare, ma abbastanza lontano da non farli sentire oppressi dai genitori -- in genere un paio d'ore di distanza usando i mezzi pubblici (nel Regno Unito).

L'ottava e ultima sessione dello SHB09 era intitolata ottimisticamente "Come sistemiamo il mondo?". Io moderavo, per cui il mio liveblogging ne ha risentito, specie nella fase di dibattito.

David Mandel, Defense Research and Development Canada, fa parte del Thinking, Risk, and Intelligence Group al DRDC di Toronto. La sua prima osservazione: "Fate attenzione ai presunti salvatori del mondo". La sua seconda osservazione: quando si afferma che qualcosa non funziona, è importante specificare gli aspetti per i quali non funziona e come sarebbe la situazione se quel qualcosa funzionasse. La sua terza osservazione: è anche importante analizzare le conseguenze di ogni potenziale soluzione. Un'analisi di come stanno le cose è basata sulla percezione, ma un'analisi di come le cose dovrebbero funzionare dovrebbe essere basata sul valore. Mandel ha anche presentato dei dati che mostrano come le previsioni effettuate da analisti di intelligence (almeno in un'organizzazione canadese) siano state molto valide.

<<http://mandel.socialpsychology.org/>>

Applied Behavioral Science in Support of Intelligence Analysis

<<http://www.cl.cam.ac.uk/~rja14/shb09/mandel.pdf>>

Radicalization: What does it mean?

<<http://individual.utoronto.ca/mandel/Mandel-radicalization.pdf>>

The Role of Instigators in Radicalization to Violent Extremism

<http://individual.utoronto.ca/mandel/NATO_HFM140_Instigators_Mandel.pdf>

Ross Anderson, Cambridge University, ha domandato "Dove si trova l'equilibrio?". Sia la privacy che la sicurezza sono bersagli mobili, ma Anderson si aspetta che presto verrà raggiunto un equilibrio societario. Aumentano gli incentivi a effettuare una discriminazione dei prezzi, e diminuiscono i costi per agire in quel senso. Ha presentato una serie di esempi di sistemi database che hanno raggiunto punti di equilibrio molto diversi fra loro, a seconda di fattori come il lobbying aziendale, le realtà politiche, indignazione pubblica, ecc. Anderson crede che la privacy verrà regolamentata, ma quando e come? "Dove finirà la linea di confine della privacy, e perché? Come possiamo spingerla da una parte o dall'altra?"

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

Database State

<<http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf>>

book chapters on psychology and terror

<<http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf>>

<<http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c24.pdf>>

Alma Whitten, Google, ha presentato un insieme di ideali sulla privacy (molto in stile europeo) e alcune delle sfide ingegneristiche che presentano. "Sfida ingegneristica n.1: Come supportare l'accesso e il controllo a informazioni personali non autenticate? Sfida ingegneristica n.2: Come informare gli utenti sia in merito a informazioni autenticate che in merito a informazioni non autenticate? Sfida ingegneristica n.3: Come bilanciare da una parte la concessione agli utenti del controllo sulla raccolta dei dati e dall'altra il rilevamento e il blocco degli abusi? Sfida ingegneristica n.4: Come fornire agli utenti un controllo a grana fine sulle loro informazioni senza sommergerli di opzioni? Sfida ingegneristica n.5: Come collegare azioni sequenziali al tempo stesso impedendo che possano essere collegabili a una certa persona? Sfida ingegneristica n.6: Come rendere evidenti agli utenti i benefici dell'analisi dei dati aggregati? Sfida ingegneristica n.7: Come evitare o rilevare la registrazione accidentale di dati che possono essere collegati a un certo individuo?" (Si noti che Alma ha richiesto di non essere registrata).

John Mueller, Ohio State University, ha parlato di terrorismo e del Dipartimento per la Sicurezza Nazionale. Il terrorismo non è una minaccia; è un problema e una causa di preoccupazione, certo, ma la parola 'minaccia' è ancora troppo estrema. Al Qaeda non è una minaccia, e rappresenta il potenziale aggressore più pericoloso per gli Stati Uniti e l'Europa occidentale. E i terroristi sono immensamente stupidi. Nel frattempo la questione del terrorismo "è diventata un cono gelato che si lecca da solo". In altre parole, è ora una burocrazia governativa che si perpetua all'infinito. Il numero dei potenziali bersagli terroristici è pressoché infinito; le probabilità che uno qualsiasi di tali bersagli verrà attaccato sono essenzialmente nulle; i terroristi scelgono i bersagli per la maggior parte in modo casuale; se si protegge un bersaglio in maniera specifica, si rendono meno sicuri altri bersagli; moltissimi bersagli sono vulnerabili in quanto non è difficile danneggiarli fisicamente, ma invulnerabili in quanto possono essere ricostruiti con relativa rapidità e con spese sostenibili (anche un bersaglio come il Pentagono); è praticamente impossibile rendere invulnerabile una vasta serie di potenziali obiettivi terroristici; se si sceglie di proteggere certi bersagli, occorre determinare se dovrebbero essere veramente protetti o meno. (Consiglio caldamente il suo libro, "Overblown").

<<http://psweb.sbs.ohio-state.edu/faculty/jmueller/>>

Reacting to Terrorism: Probabilities, Consequences, and the Persistence of Fear

<<http://psweb.sbs.ohio-state.edu/faculty/jmueller/ISA2007T.PDF>>

Evaluating Measures to Protect the Homeland from Terrorism

<<http://psweb.sbs.ohio-state.edu/faculty/jmueller/ISA9.PDF>>

Terrorphobia: Our False Sense of Insecurity

<<http://www.the-american-interest.com/ai2/article.cfm?Id=418&MIId=19>>

Adam Shostack, Microsoft, ha evidenziato il fatto che è difficile anche comprendere quale parte del problema affrontare per prima. Una delle problematiche è la vergogna. Non abbiamo voglia di parlare di quel che non va, per cui non possiamo utilizzare quelle informazioni per determinare la direzione da intraprendere. Creiamo delle scuse -- i clienti se ne andranno, la gente sposterà denuncia, le azioni crolleranno -- anche se sappiamo benissimo che è stata dimostrata la falsità di tali scuse.

<<http://www.homeport.org/~adam/>>

<<http://newschoolsecurity.com/>>

Durante il dibattito si è molto discusso sull'alternativa fra informare gli utenti o bombardarli di informazioni che non possono comprendere. E molto altro che non sono riuscito a trascrivere.

Ecco tutto. SHB09 è stato un workshop fantastico, ricco di persone e dibattiti interessanti. Ci vediamo l'anno prossimo, nell'altra Cambridge.

Anche Ross Anderson e Adam Shostack hanno scritto dei riassunti della conferenza. E Matt Blaze ha effettuato registrazioni audio:

<<http://www.lightbluetouchpaper.org/2009/06/11/security-and-human-behaviour-2009/>>

<<http://newschoolsecurity.com/2009/06/shb-session-1-deception/>>

<<http://www.crypto.com/blog/shb09/>>

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

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) 2009 - Bruce Schneier.