

Il WEIS iniziò l'anno successivo, alla University of California a Berkeley, ed è andato crescendo. È l'unico workshop in cui i tecnologi si riuniscono con economisti e giuristi per cercare di comprendere le problematiche della sicurezza informatica.

E l'economia ha molto da insegnare alla sicurezza informatica. Generalmente si considera quest'ultima come un problema di tecnologia, ma spesso i sistemi falliscono a causa di incentivi economici malposti: le persone che potrebbero proteggere un sistema non sono quelle che subiscono i costi degli errori e dei fallimenti.

Se si comincia a prestare attenzione, le considerazioni economiche si trovano dappertutto nel campo della sicurezza informatica. Negli ospedali, i sistemi di registrazione delle cartelle cliniche prevedono estese funzioni di gestione della fatturazione per gli amministratori che le specificano, ma non sono altrettanto efficienti nella protezione della privacy dei pazienti. Gli sportelli bancomat sono stati bersaglio di frodi in paesi come il Regno Unito e i Paesi Bassi, dove una legislazione insufficiente non ha offerto alle banche adeguati incentivi per mettere al sicuro i propri sistemi, e ha permesso che scaricassero i costi delle frodi sui propri clienti. E uno dei motivi per cui Internet non è sicura è che la responsabilità degli attacchi è troppo indefinita.

In tutti questi esempi le considerazioni economiche della sicurezza sono molto più importanti di quelle tecniche.

Più in generale, molti dei quesiti fondamentali sulla sicurezza sono di ordine economico tanto quanto lo sono di ordine tecnico, se non di più. Spendiamo abbastanza per tenere lontani gli hacker dai nostri sistemi? O stiamo spendendo troppo? E stiamo investendo cifre adeguate in forze di polizia e in servizi militari? E stiamo spendendo i nostri budget di sicurezza per le iniziative giuste? Alla luce di quanto accaduto l'11 settembre 2001, domande come queste diventano di primaria importanza.

L'economia, in effetti, può spiegare molte delle sconcertanti realtà della sicurezza in Internet. I firewall sono assai diffusi, la crittografia della posta elettronica è rara: questo non a causa della relativa efficacia delle rispettive tecnologie, ma per le pressioni economiche che spingono le aziende a installarle. Le grandi imprese divulgano raramente informazioni sulle intrusioni: ciò a causa degli incentivi economici che invitano a non farlo. E un sistema operativo non sicuro è lo standard internazionale, in parte, perché i suoi effetti economici sono in larga parte sostenuti non dalla compagnia che produce tale sistema operativo, ma dai consumatori e clienti che lo acquistano.

Alcune delle problematiche di cyber-condotta più controverse si collocano direttamente fra l'Information Security e l'economia. Per esempio, la questione della gestione dei diritti digitali: la legge sul copyright è troppo restrittiva, o non è abbastanza restrittiva, per elevare la produzione creativa della società? E se è necessario che sia più restrittiva, le tecnologie DRM finiranno con il beneficiare l'industria musicale o i produttori di tecnologia? L'iniziativa di Microsoft per il Trusted Computing è una buona idea, o è soltanto un altro sistema per costringere i clienti a rimanere con Windows, Media Player e Office? Ogni tentativo di rispondere a queste domande finisce con l'impigliarsi sia in problematiche di Information Security sia di ordine economico.

Il WEIS incoraggia studi e articoli su queste e altre problematiche di economia e di sicurezza informatica. Abbiamo assistito a presentazioni di studi sull'economia dell'investigazione digitale dei telefoni cellulari (se possedete un telefono poco comune, la polizia probabilmente non avrà gli strumenti per condurre un'analisi forense), e

Come reagire:

<http://www.schneier.com/crypto-gram-0307.html#1>

I falsi allarmi:

<http://www.schneier.com/crypto-gram-0307.html#8>

Sistemi di controllo incorporati e Sicurezza

<http://www.schneier.com/crypto-gram-0207.html#1>

La nuova generazione dell'hacking telefonico:

<http://www.schneier.com/crypto-gram-0107.html#1>

Il monitoraggio innanzitutto:

<http://www.schneier.com/crypto-gram-0107.html#5>

L'esposizione totale e la CIA:

<http://www.schneier.com/crypto-gram-0007.html#1>

Unicode e i rischi legati alla sicurezza:

<http://www.schneier.com/crypto-gram-0007.html#9>

Il futuro del "Crypto-Hacking":

<http://www.schneier.com/crypto-gram-9907.html#hacking>

I pasticci e le approssimazioni di SSL:

<http://www.schneier.com/crypto-gram-9907.html#doghouse>

La declassificazione di Skipjack:

<http://www.schneier.com/crypto-gram-9807.html#skip>

** **

Una piccola lezione di sicurezza dagli attentati dinamitardi di Mumbai

Due citazioni: "Le Autorità hanno inoltre drasticamente limitato la rete telefonica cellulare temendo che potesse essere utilizzata per attuare altri attacchi". E "Alcuni dei feriti sono stati visti comporre convulsamente numeri di telefono sui loro cellulari. L'intera rete mobile ha collassato, aumentando il senso di panico fra le persone".

I telefoni cellulari sono molto utili per i terroristi, ma lo sono di più per tutti noi.

<http://www.stuff.co.nz/stuff/0,2106,3729278a12,00.html>

Nota: La storia è stata cambiata online, e la seconda citazione è stata soppressa.

** **

Google e la "frode del clic"

Il business pubblicitario di Google, che frutta alla società 6 miliardi di dollari l'anno, è a rischio perché non vi è la certezza che la gente stia davvero guardando gli annunci. Il problema viene chiamato "click fraud", ovvero "frode del clic"; ve ne sono due tipologie di base.

Per quanto riguarda la frode del clic in rete, voi mantenete GoogleAds

sul vostro sito web. Google vi paga ogni volta che qualcuno fa clic su uno degli annunci nel vostro sito. È frode se vi sedete al computer e fate continuamente clic sull'annuncio o, ancora meglio, scrivete un programma che lo faccia al vostro posto. Google non ha difficoltà a rilevare questo tipo di frode, pertanto gli scaltri frodatori del clic nella rete simulano differenti indirizzi IP o installano cavalli di Troia su computer di altre persone per generare i finti clic.

L'altro tipo di frode del clic è competitivo. Notate che un vostro concorrente in affari ha comprato un annuncio da Google, pagando Google per ogni clic. Voi quindi sfruttate le tecniche descritte sopra per effettuare ripetuti clic sui suoi annunci, costringendolo a spendere denaro (a volte molto denaro) per nulla. (Click Monkeys è un sito-imbroglio che si offre di commettere la frode del clic per vostro conto.)

La frode del clic è diventata un classico "braccio di ferro" della sicurezza. Google migliora i propri strumenti di rilevazione delle frodi, per cui i frodatori si fanno sempre più scaltri... e si perpetua il ciclo. Nel frattempo Google sta affrontando svariate cause intentate da coloro che sostengono che la compagnia non stia facendo abbastanza per risolvere il problema. A mio avviso tutti hanno ragione: è nell'interesse di Google sia risolvere la questione, sia minimizzare l'importanza del problema.

Ma il problema più generale è davvero importante e difficile da risolvere: come si fa a sapere se vi è realmente una persona seduta al computer? Come si può sapere se quella persona sta prestando attenzione, se non sta utilizzando qualche espediente per automatizzare le risposte, se non è assistita dagli amici? I sistemi di autenticazione sono una faccenda complessa, che siano basati su qualcosa che si conosce (password), qualcosa che si possiede (token), o su chi siamo (biometria). Però nessuno di questi sistemi può proteggervi da qualcuno che se ne va e lascia a un'altra persona il suo posto davanti al computer, o da un computer infettato da un Trojan.

Il problema si presenta anche in altri contesti.

Per anni, le compagnie produttrici di videogiochi di rete hanno combattuto contro giocatori che utilizzano dei programmi che li aiutano a giocare meglio: programmi che permettono di sparare perfettamente o di vedere informazioni di norma invisibili o non accessibili.

Giocare è meno divertente se tutti vengono assistiti da un computer, ma a meno di non esservi un premio in denaro, la posta è piuttosto bassa. Non è così nel caso dei siti di poker online, dove giocatori assistiti dal computer, o anche computer che giocano da soli, possono potenzialmente eliminare dal gioco tutti i giocatori in carne e ossa.

Basta guardarsi intorno in Internet per vedere questo problema emergere in continuazione. Il principio che sta alla base dei captcha (un test fatto di una o più domande e risposte per determinare se l'utente sia un umano o un computer, ndr) è quello di assicurarsi che chi sta visitando il sito web sia davvero una persona, e non solo un bot su un computer. Gli esami online non funzionano perché l'esaminatore non può essere certo che lo studente non abbia il libro aperto davanti a sé o un amico alle spalle pronto ad aiutarlo. In entrambi i casi la soluzione è ovviamente un proctor, ovvero un "sorvegliante", ma non è sempre il modo più pratico ed evita i vantaggi degli esami a distanza.

Questo problema è emerso perfino in sede processuale. In un caso, l'accusa dimostrò che il computer dell'imputato aveva commesso un qualche reato di hacking, ma la difesa sostenne che non era stato

l'imputato a commettere tale crimine: qualcun altro stava controllando il suo computer. E in un altro caso, un imputato accusato di un reato di pedopornografia ha riconosciuto di avere del materiale illegale nel suo computer, ma ha dichiarato che il computer si trovava in una stanza comune di casa sua e che era solito tenere molte feste, e che non era stato lui a scaricare il materiale pornografico.

Anni fa, parlando di sicurezza, mi lamentavo a riguardo del collegamento fra computer e sedia. La parte facile è proteggere informazioni digitali: nel computer da scrivania, in transito fra computer e computer, o in enormi server. La parte difficile è proteggere le informazioni nel tratto fra computer e persona. Analogamente, è molto più semplice autenticare un computer che non una persona seduta davanti a esso. E verificare l'integrità di dati è molto più semplice del verificare l'integrità (in tutti i sensi) della persona che li sta guardando.

Ed è un problema che andrà peggiorando a mano a mano che i computer diventeranno sempre più capaci di imitare le persone.

Google sta testando un nuovo modello pubblicitario per affrontare la frode del clic: il costo per azione. Gli inserzionisti non pagano finché il cliente non esegue una certa azione: compra un prodotto, compila un questionario, cose del genere. È un modello difficile da far funzionare (Google diventerebbe più un partner nella vendita finale invece di essere un semplice visualizzatore neutrale di pubblicità), ma è la risposta di sicurezza corretta contro la frode del clic: cambiare le regole del gioco, in modo che la frode del clic perda di significato.

Ecco come si risolve un problema di sicurezza.

Cause legali contro Google:

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/03/09/BUGRMHKQTR1.DTL>>

oppure <<http://tinyurl.com/z6gju>>

<http://www.marketwire.com/mw/release_html_b1?release_id=103417>

Il sito-imbroglio:

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

I captcha:

<<http://en.wikipedia.org/wiki/Captchas>>

L'esperimento costo-per-azione di Google:

<http://www.betanews.com/article/Google_Tests_CostPerAction_Ads/1151005169>

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

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

News

Storia surreale di una persona in arrivo negli Stati Uniti dall'Iraq che viene trattenuta alla frontiera perché era solita vendere immagini protette da copyright su T-shirt.

<<http://www.latimes.com/news/opinion/commentary/la-oe-lemoine13jun13,0,1507648.story>> oppure <<http://tinyurl.com/ourlr>>

Patrick Smith cura la rubrica "Ask the Pilot" su Salon. Ha scritto due ottimi post sulla sicurezza aerea, uno su come il sistema israeliano non potrà funzionare negli Stati Uniti, e l'altro sul profiling:

<http://www.salon.com/tech/col/smith/2006/06/09/askthepilot189/>
<http://www.salon.com/tech/col/smith/2006/06/16/askthepilot190/>

Vi sono svariate tecnologie di crittografia che permettono di analizzare dati senza conoscere alcun dettaglio sui dati stessi. Lo si consideri una specie di data mining con privacy abilitata.

<http://www.wired.com/news/wireservice/0,71184-0.html>

"How to build a low-cost, extended-range RFID skimmer" [Come costruire un economico lettore RFID a lungo raggio], di Ilan Kirschenbaum e Avishai Wool. Sarà presentato al 15° USENIX Security Symposium a Vancouver, Canada, che si terrà il prossimo agosto.

<http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html>

Studio affascinante sulla sicurezza della Xbox. La conclusione: "Il sistema di sicurezza della Xbox si è rivelato un totale fallimento".
http://www.xbox-linux.org/wiki/17_Mistakes_Microsoft_Made_in_the_Xbox_Security_System oppure <http://tinyurl.com/blbke>

Sembra quasi una premessa fantascientifica: androidi che controllano la popolazione e rilevano eventuali reati.

<http://www.wired.com/news/wireservice/0,71198-0.html>

Generatori casuale di identità:

<http://dev.allredtech.com/fakename/>

Non ho idea di quanto bene funzionino.

Ulteriori informazioni sullo scandalo dell'intercettazione avvenuta in Grecia:

http://www.schneier.com/blog/archives/2006/06/greek_wiretappi_1.html

http://www.schneier.com/blog/archives/2006/07/greek_wiretappi.html

Ne ho parlato in precedenza:

http://www.schneier.com/blog/archives/2006/02/phone_tapping_i.html

AT&T riformula la sua politica sulla privacy:

<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2006/06/21/BUG9VJHB9C1.DTL&type=business>

oppure <http://tinyurl.com/on53q>

<http://ars.userfriendly.org/cartoons/?id=20060625>

Conosco il problema legato alla data in Unix da molto tempo, ma questa è la prima volta che sento di un bug vero e proprio dovuto al "millennium bug" dei sistemi Unix legato all'anno 2038.

<http://thedailywtf.com/forums/thread/78254.aspx>

MySpace sta intensificando la sicurezza.

<http://www.cnn.com/2006/TECH/internet/06/20/myspace.safety.ap.ap/index.html>

oppure <http://tinyurl.com/rplw8>

Onestamente, sembrano più misure di sicurezza per proteggere la propria posizione che sicurezza reale: MySpace sta proteggendosi da eventuali cause legali. "Esperti di sicurezza" sembrano essere d'accordo sul fatto che non migliorerà di molto la sicurezza.

<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/25/AR2006062500426.html> oppure <http://tinyurl.com/r4vkn>

Gli errori nell'effettuare redazioni digitali stanno diventando talmente comuni da non fare più notizia:

http://www.mercurynews.com/mld/mercurynews/sports/special_packages/doping_scandal/14882936.htm oppure <http://tinyurl.com/kbyjm>

Si sarebbe portati a credere che una zecca nazionale abbia buone misure di sicurezza contro gli stessi dipendenti. Invece no, un impiegato della

zecca nazionale australiana ha rubato 600 dollari al giorno nell'arco di dieci mesi.

<<http://www.smh.com.au/news/national/mint-security-lapse-amazes-judge/2006/06/21/1150845228544.html>> oppure <<http://tinyurl.com/hox2e>>

Interessante ricerca su come sconfiggere il firewall nazionale cinese:
<<http://www.lightbluetouchpaper.org/2006/06/27/ignoring-the-great-firewall-of-china/>>

oppure <<http://tinyurl.com/zzbt5>>

Il Congresso apprende quanta poca privacy ci è rimasta:

<<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/25/AR2006062500426.html>>

Eccellente analisi sull'applicazione del CALEA al VoIP: "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP" [Implicazioni di sicurezza dell'applicazione del Communications Assistance to Law Enforcement Act al protocollo Voice over IP], di Steve Bellovin, Matt Blaze, Ernie Brickell, Clint Brooks, Vint Cerf, Whit Diffie, Susan Landau, Jon Peterson, e John Treichler. Si legga almeno il riassunto esecutivo.

<<http://www.itaa.org/news/docs/CALEAVOIPreport.pdf>>

Forse non avrei dovuto fare queste dichiarazioni: " 'Ho una rete Wi-Fi totalmente aperta', ha detto Schneier a ZDNet UK. 'Prima di tutto, non mi importa se i miei vicini di casa stanno utilizzando la mia rete. In secondo luogo, i miei computer sono protetti. Terzo, è una cosa educata. I miei ospiti possono farne uso' ". Per la cronaca, possiedo una rete wireless ultra-sicura che trasmette automaticamente qualsiasi tentativo di intrusione a degli energumani con cani feroci.

<http://news.com.com/2100-1029_3-6088741.html>

Più veritiero che divertente, purtroppo. Un modello per notizie di cronaca sulla raccolta dati:

<http://www.concurringopinions.com/archives/2006/06/template_for_ne.html>

Non posso credere che mi sia dimenticato di scrivere nel mio blog di questo ottimo articolo sulla Fiera dell'Intercettazione di Washington, DC:

<http://www.wired.com/news/technology/0,71022-0.html?tw=wn_story_page_prev2>

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

Fresche di brevetto: pallottole protette da password:

<http://www.newscientisttech.com/article.ns?id=dn9412&feedId=online-news_rss20>

oppure <<http://tinyurl.com/pyn4s>>

Microsoft ha la capacità di disabilitare Windows da remoto? Forse.

<<http://blogs.zdnet.com/Bott/?p=84&tag=nl.e622>>

Caricare controlli ActiveX in Vista senza privilegi di amministratore.

<http://www.schneier.com/blog/archives/2006/07/load_activex_co.html>

Si discute molto se questa sia una buona idea o meno. Tanto per cominciare, io credo che ActiveX stesso sia una pessima idea.

Una canzone: Facial Recognition Technology Blues [Il Blues della tecnologia di riconoscimento facciale]

<<http://www.eddiebandthegspots.com/Facial%20Recognition%20Technology%20Blues.mp3>> oppure <<http://tinyurl.com/hgnbm>>

Questo telefono cellulare possiede un Breathalyzer incorporato. Vi

avvisa nel caso siate troppo ubriachi per guidare, e vi permette di bloccare alcuni numeri di telefono, in modo che non possiate chiamarli in stato di ebbrezza (numeri di ex-amanti o magari del vostro capo, per esempio).

<http://abcnews.go.com/Technology/story?id=2125709>

Rapporto annuale dal Privacy Commissioner (Commissario sulla Privacy) del Canada.

http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.asp

Questo è il rapporto relativo al 2001-2002:

http://www.privcom.gc.ca/information/ar/02_04_10_e.asp

Una lettura eccellente.

In questo attacco è possibile ottenere il controllo di un computer altrui utilizzando la sua interfaccia wireless, anche se non è collegato a una rete. Non vi sono ancora i dettagli: i ricercatori presenteranno i loro risultati al BlackHat il 2 agosto.

http://www.infoworld.com/article/06/06/21/79536_HNwifibreach_1.html

<http://www.blackhat.com/html/bh-usa-06/bh-usa-06-index.html>

Questo è un nuovo brevetto concesso alla Marina Militare degli Stati Uniti. Pare che abbiano brevettato il firewall.

<http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetacgi%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220050022023%22.PGNR.&OS=DN/20050022023&RS=DN/20050022023> oppure

<http://tinyurl.com/khex6>

Ecco una cronologia delle fughe di dati a partire dal furto ai danni di ChoicePoint del febbraio 2005. Identità rubate in totale: 88.794.619.

Anche se, quasi certamente, molti nomi ricorrono più volte in quell'elenco.

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Ho già spiegato perché i sistemi di data mining che seguono lo stile di sorveglianza all'ingrosso della NSA sono inutili per rintracciare terroristi. Ecco una spiegazione più formale:

<http://www.lewrockwell.com/orig7/rudmin1.html>

Il mio articolo:

http://www.schneier.com/blog/archives/2006/03/data_mining_for.html

Una risposta alla responsabilità sul software è quella di programmare deliberatamente in modo da offuscare le responsabilità. Questa entrata di blog sulla "programmazione inaffidabile" è satirica, ma estremamente acuta.

<http://pestilenz.org/cgi-bin/bloxsom.cgi/2005/11/11>

Una notizia sul fallimento dell'autenticazione a due fattori. I phisher stanno passando ad attacchi di tipo man-in-the-middle, che aggirano le misure di sicurezza.

http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoof_s_2factor_1.html oppure <http://tinyurl.com/rbmr2>

L'avevo previsto lo scorso anno.

<http://www.schneier.com/crypto-gram-0503.html#2>

Il New York Times sta diffondendo voci allarmistiche sul possibile collegamento tra furto di identità e chi fa uso di metamfetamine. Pare che costoro siano idealmente adatti a essere anche hacker informatici. Non so se ciò sia vero o meno, ma mi preoccupano gli eventuali interventi governativi nel caso l'hacking venga connesso alla guerra alla droga.

<http://www.nytimes.com/2006/07/11/us/11meth.html>

I codici del satellite Galileo sono stati craccati. In realtà i codici

craccati sono di un satellite prototipo; i codici definitivi di Galileo saranno diversi.

<http://www.newswise.com/articles/view/521790/>

Gingilli da spia che è possibile acquistare. Per me non è interessante ciò che è disponibile sul mercato oggi, quanto ciò che si può immaginare sia a disposizione delle vere spie.

http://darkcreek.com/detective_equipment/notebook.htm

Ottimo articolo su come la complessità riduca in larga misura l'efficacia delle indagini antiterrorismo. Le storie di risorse sprecate provengono tutte dal Regno Unito, ma le morali sono universali.

http://www.theregister.com/2006/07/06/90_days_terror_law_analysis/

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

Ottenere un codice di sblocco personale per il cellulare O2

O2 è un operatore di telefonia cellulare del Regno Unito. La compagnia offre la possibilità di impostare un codice PIN sul vostro telefono. L'idea è che, in caso il telefono vi venga rubato, il ladro non può effettuare chiamate. Se digita il codice PIN errato per tre volte, il telefono viene bloccato. Se i legittimi proprietari sbagliano a inserire il PIN o se lo dimenticano, possono contattare O2 e ottenere un codice PUK (Personal Unlock Code, ossia codice di sblocco personale). Presumibilmente l'operatore procederà a verificare che il chiamante sia davvero il legittimo proprietario del telefono.

Fin qui tutto bene.

O2, però, ha deciso di automatizzare il processo di ottenimento del PUK. Ora chiunque può visitare il sito web di O2, inserire un numero di cellulare valido, e ottenere un codice PUK valido per resettare il PIN di quel telefono. Senza alcun tipo di autenticazione.

Sembra una pessima idea, ma dopo averne parlato nel mio blog, un rappresentante di O2 mi ha inviato quanto segue:

"Sì, pare che vi sia un rischio di sicurezza nel servizio offerto da O2, ma crediamo che tale rischio sia minimo. Il rischio è quando il telefono di un cliente viene smarrito o rubato. In tal caso, due possono essere gli scenari:

"Scenario 1 - Il telefono è spento. Accendendolo, viene richiesto un codice PIN. Anche se il codice PUK può permettere il reset del PIN a tutti gli effetti, occorre conoscere il numero di telefono della SIM per ottenerlo. Non vi è alcun modo per risalire al numero di telefono esaminando la SIM o il cellulare stesso. Nel caso il numero di telefono sia noto, il rischio è lo stesso dello Scenario 2.

"Scenario 2 - Il telefono è acceso. In questo caso, il ladro può utilizzare comunque il telefono senza dover acquisire un codice PUK.

"In entrambi gli scenari abbiamo considerato che la misura di sicurezza primaria sia dare la possibilità al cliente di informarci sulla perdita/furto del cellulare il più rapidamente possibile, in modo che possiamo disattivare da remoto sia la SIM sia il cellulare stesso (così da non poter essere utilizzato con nessun'altra SIM)".

Il sito web di O2:

<http://www.o2.co.uk/puk/landing/0,,555,00.html>

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

La League of Women Voters appoggia i tracciati cartacei verificabili dal votante

Per molto tempo, la League of Women Voters (LWV) ha sostenuto la parte sbagliata della discussione sulle problematiche legate alle macchine per il voto elettronico. Essa era a favore delle macchine, e non vedeva la necessità di tracciati cartacei verificabili dal votante. (Sul sito web della LWV era presente un Q&A [Domanda e Risposta] terrificante e fuorviante sulla questione, ma ora è stato eliminato. Barbara Simons ha pubblicato una confutazione che comprende il Q&A originale).

La politica della LWV è bizantina: sostanzialmente vi sono unioni locali sotto unioni statali, che a loro volta stanno sotto l'unione nazionale (LWVUS). Viene indetta un'assemblea ad anni alterni, e ogni genere di risoluzioni vengono approvate dai membri. Ma l'ufficio nazionale ha un potere decisionale maggiore di quello dell'insieme dei membri e delle unioni statali. La politica delle macchine per il voto ne è un esempio.

All'assemblea del 2004, l'insieme dei membri della LWV approvò una risoluzione sul voto elettronico chiamata "SARA", che stava per "Secure, Accurate, Recountable, Accessible" [Sicuro, Preciso, Conteggiabile nuovamente, e Accessibile]. Coloro a favore della risoluzione credevano che "Recountable", cioè conteggiabile nuovamente, significasse anche tracciabile, ovvero tracciati cartacei verificabili dal votante. Ma l'ufficio nazionale della LWV decise di interpretare SARA in modo da sostenere che "conteggiabile nuovamente" non implica tracciati cartacei. Mentre non era più possibile opporsi del tutto alla carta, l'ufficio si rifiutò di sostenere che la carta fosse un'opzione desiderabile. Per esempio, l'ufficio nazionale prendeva a modello il sistema della Georgia, e in Georgia si utilizzano macchine Diebold DRE senza carta. Viene quasi da pensare che la leadership della LWVUS sia nelle tasche di qualcuno.

E quindi all'assemblea del 2006, l'insieme dei membri della LWV ha approvato UN'ALTRA risoluzione. Questa è stata scritta molto più chiaramente, pensata per evitare che l'ufficio nazionale sostenga che la LWV non sia a favore dei tracciati cartacei verificabili dall'utente.

Purtroppo la League of Women Voters non ha pubblicato un comunicato stampa su questa risoluzione (vi è un comunicato stampa di VerifiedVoting.org sull'argomento). Sono certo che l'ufficio nazionale molto semplicemente si rifiuta di riconoscere la posizione dei membri su tale problematica, e che desidera che la cosa sparisca in tutta quiete. È un peccato: la risoluzione è davvero ottima e merita di essere pubblicizzata.

Ecco il testo della risoluzione:

"Risoluzione riguardante il Programma che richiede un Scheda Cartacea Verificabile dal Votante o Registrazione Cartacea per le Macchine per il Voto Elettronico

"Mozione per l'adozione della seguente risoluzione riguardante il programma che richiede un scheda cartacea verificabile dal votante o registrazione cartacea per i sistemi di voto elettronico.

"Premesso che: Alcune LWV hanno avuto difficoltà nell'applicare la

Risoluzione SARA (Secure, Accurate, Recountable, Accessible) approvata alla scorsa Assemblea, e

“Premesso che: I sistemi di voto elettronico sprovvisti di tracciati cartacei non sono intrinsecamente più sicuri, possono non funzionare correttamente, e non prevedono un tracciato di verifica conteggiabile nuovamente,

“Di conseguenza sia stabilito che:

“La posizione sul Diritto di Voto del Cittadino sia interpretata così da affermare che la LWVUS sostenga solo sistemi di voto progettati in modo che:

1. impieghino una scheda cartacea verificabile dal votante o altro tipo di registrazione cartacea, essendo tale scheda cartacea la registrazione ufficiale della volontà del votante; e che
2. il votante possa verificare con i propri occhi, o con l'aiuto di appositi dispositivi per chi abbia disabilità visive, che la scheda cartacea/registrazione rifletta precisamente la sua volontà; e che
3. tale verifica possa avvenire durante il procedimento di voto; e che
4. la scheda cartacea/registrazione sia utilizzata per verifiche e nuovi conteggi; e che
5. i totali dei voti possano essere verificati da un conteggio manuale indipendente delle schede cartacee/registrazioni; e che
6. verifiche di routine delle schede cartacee/registrazioni in seggi elettorali selezionati casualmente possano essere condotte per qualsiasi elezione, e i risultati pubblicati dalla giurisdizione”.

Fra l'altro, l'insieme dei membri dell'assemblea LWV del 2006 ha anche votato una risoluzione a favore della neutralità della rete (l'unione del Connecticut ha pubblicato un comunicato stampa, dato che è stata a capo dell'iniziativa), e una contro la pena di morte. L'ufficio nazionale della LWV non ha emanato alcun comunicato stampa nemmeno per queste due risoluzioni.

Il comunicato stampa di Verified Voting:

<http://www.verifiedvotingfoundation.org/article.php?id=6363>

Il comunicato stampa della LWV del Connecticut sulla neutralità della rete:

<http://www.lwvct.org/issues/action/061506-release-net%20neutrality.htm>

Q&A con la confutazione di Barbara Simons:

<http://www.schneier.com/lwv-qa.pdf>

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

Il rapporto del Brennan Center sul voto elettronico

Ho collaborato con la Task Force per la Sicurezza del Voto del Brennan Center. Agli inizi di questo mese abbiamo rilasciato un rapporto sul voto elettronico.

Dal riassunto esecutivo:

“Nel 2005, il Brennan Center ha riunito una Task Force composta da scienziati governativi, accademici e del settore privato riconosciuti a livello internazionale, esperti di macchine per il voto elettronico, e professionisti della sicurezza per condurre la prima analisi sistematica nazionale delle vulnerabilità di sicurezza nei tre sistemi di voto

elettronico più comunemente adottati. La Task Force ha impiegato più di un anno a condurre la sua analisi e a stilare il presente rapporto. Durante questo periodo la metodologia, l'analisi e il testo sono stati estensivamente sottoposti a peer review da parte del NIST (National Institute of Standards and Technology)."

Inoltre:

"La Task Force ha esaminato le minacce di sicurezza per le tecnologie utilizzate nei sistemi Direct Recording Electronic ("DRE"), nei sistemi DRE muniti di tracciato cartaceo verificabile dal votante ("DREs w/ VVPT") e nei sistemi Precinct Count Optical Scan ("PCOS"). L'analisi parte dal presupposto che una adeguata sicurezza fisica e le varie procedure di contabilità siano già predisposte e attivate".

Inoltre:

"Dall'analisi della minaccia emergono tre punti fondamentali nel Rapporto sulla Sicurezza:

1. Tutti e tre i sistemi di voto presentano significative vulnerabilità legate alla sicurezza e all'affidabilità, che costituiscono un reale pericolo per l'integrità delle elezioni nazionali, statali e locali.
2. Le vulnerabilità più preoccupanti di ognuno dei sistemi considerati possono essere sostanzialmente corrette se si implementano adeguate contromisure a livello statale e locale.
3. Poche giurisdizioni hanno implementato alcune delle contromisure essenziali per rendere i più semplici attacchi contro i sistemi per il voto elettronico molto più difficili da eseguire con successo".

Inoltre:

"Vi è una serie di passi che le varie giurisdizioni potrebbero intraprendere per affrontare le vulnerabilità individuate dal Rapporto sulla Sicurezza e, così facendo, rendere molto più sicuri i propri sistemi di voto. Consigliamo l'adozione delle seguenti misure di sicurezza:

1. Condurre verifiche automatiche di routine che confrontino le registrazioni cartacee controllate dal votante con le registrazioni elettroniche che seguono ogni elezione. Un tracciato cartaceo verificato dall'utente, accompagnato da una robusta verifica automatica di routine di tali tracciati può fare molto per contrastare gli attacchi più semplici.
2. Effettuare un "test parallelo" (selezione casuale di macchine per il voto e collaudo il più possibile realistico durante la giornata elettorale). Per le macchine DRE senza carta, in particolar modo, il test parallelo aiuterà le varie giurisdizioni a rilevare attacchi software e bug software più insidiosi che potrebbero non essere scoperti durante l'ispezione e altre verifiche.
3. Vietare l'utilizzo di macchine per il voto dotate di componenti wireless. Tutti e tre i sistemi di voto sono molto più vulnerabili agli attacchi se dotati di componenti wireless.
4. Utilizzare un procedimento trasparente e di selezione casuale per tutte le procedure di auditing. Perché qualsiasi auditing sia efficace (e per assicurarsi che il pubblico confidi in tali procedure), le giurisdizioni devono sviluppare e implementare procedure trasparenti e di selezione casuale.
5. Garantire una programmazione e un'amministrazione dei sistemi di voto decentralizzate. Quando una singola entità, come un rivenditore o un consulente statale o nazionale, esegue compiti chiave per molte giurisdizioni, gli attacchi contro le elezioni a livello statale diventano più semplici da condurre.

6. Istituire procedure chiare ed efficaci per gestire evidenze di frode o errori. Sia le verifiche automatiche di routine, sia il test parallelo, possiedono un valore di sicurezza discutibile in assenza di procedure efficaci di azione in caso vengano scoperte prove di malfunzionamenti e/o di frodi. Il rilevamento di una frode senza una risposta adeguata non potrà impedire che gli attacchi vadano a buon fine".

Il rapporto è lungo, ma ritengo che valga la pena leggerlo. Se non avete molto tempo, comunque, leggete almeno il Riassunto Esecutivo.

Il rapporto ha suscitato reazioni da parte della stampa. Purtroppo gli articoli in circolazione riciclano alcune delle ridicole argomentazioni che Diebold continua a sostenere malgrado questo tipo di analisi. Dall'articolo del Washington Post:

"I produttori di macchine per il voto hanno liquidato molte delle preoccupazioni in proposito come puramente teoriche e che non riflettono l'esperienza reale delle elezioni, per esempio come le macchine siano tenute in un ambiente sicuro.

" 'Non si tratta semplicemente dell'attrezzatura, della singola macchina', ha dichiarato David Bear, un portavoce di Diebold Election Systems, uno dei principali produttori del paese. 'Sono tutti gli elementi dell'ambiente elettorale che contribuiscono a rendere sicura un'elezione".

" 'Questo rapporto è basato più su una speculazione che non su un'analisi dei fatti. A tutt'oggi, i sistemi di voto non sono mai stati attaccati con successo durante un'elezione dal vivo', ha dichiarato Bob Cohen, un portavoce dell'Election Technology Council, un cartello di produttori di macchine per il voto. 'Le presunte vulnerabilità presentate in questo studio, pur interessanti a livello teorico, sarebbero estremamente difficili da sfruttare' ".

Vorrei che il Washington Post trovasse qualcuno che facesse presente che in questi anni vi sono state molte, moltissime irregolarità con le macchine per il voto elettronico, e la mancanza di prove convincenti di avvenuta frode è esattamente il problema dei loro sistemi non-verificabili. O che l'argomentazione "è tutto a livello teorico" è la stessa che i produttori di software erano soliti utilizzare per screditare le vulnerabilità di sicurezza prima che il movimento per l'esposizione totale li costringesse ad ammettere i molti problemi dei loro software.

Il rapporto:

<http://www.brennancenter.org/presscenter/releases_2006/pressrelease_2006_0627.html> oppure <<http://tinyurl.com/mwzy8>>
<<http://www.brennancenter.org/programs/downloads/Full%20Report.pdf>>
<<http://www.brennancenter.org/programs/downloads/Executive%20Summary.pdf>>
>

Le notizie:

<http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006-06-27T130232Z_01_N26181575_RTRUKOC_0_US-VOTINGMACHINES.xml>
oppure
<<http://tinyurl.com/kca69>>
<<http://business.bostonherald.com/technologyNews/view.bg?articleid=145981>>
oppure <<http://tinyurl.com/gdx71>>
<http://www.usatoday.com/news/washington/2006-06-26-e-voting_x.htm>
<<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/27/AR20060>>

62701451_pf.html>
oppure <http://tinyurl.com/oudom>

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

Commenti dei lettori

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

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

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

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:

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

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

La versione italiana è curata da Communication Valley SpA

<http://www.communicationvalley.it/>.

Per iscriversi o cancellarsi andare all'indirizzo

<http://www.cryptogram.it/>.

I numeri arretrati sono disponibili all'indirizzo

<http://www.cryptogram.it/>.

Per informazioni crypto-gram@communicationvalley.it.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare 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 Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <http://www.schneier.com>.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di Counterpane Internet Security, Inc.

Copyright (c) 2006 by Bruce Schneier.