

Ma personalmente trovo il tutto un po' improbabile. In primo luogo, per insicuri che siano questi sistemi, non è facile penetrarvi e fare danni estremi. Credo sia facile penetrarvi e fare qualche tentativo qua e là finché qualcosa non si rompe, ma nulla di spettacolare. Una volta tanto l'oscurità gioca a nostro favore; il semplice fatto che i comandi sono arcani e astrusi, che i singoli cambiamenti non sono per nulla ovvi, e che non esistono manuali a portata di mano, rende tutto il sistema più sicuro.

Secondariamente, il terrorismo "tecnologicamente primitivo" è molto più affidabile ed efficace di quello tecnologicamente avanzato. Anche se i pericoli visti sopra sono reali, li ritengo di minore entità rispetto ad esplosivi o a dei pazzi dotati di armi automatiche. Certo, aprire gli scarichi fognari ed inquinare un fiume farà sicuramente notizia, ma far saltare una delle tre principali tubazioni sotto Manhattan porta danni più ingenti.

La vera minaccia è rappresentata da chi attacca a distanza. Credo che uno scenario possibile sia questo: un sedicente terrorista (non un vero terrorista, ma uno che legge di terrorismo sui giornali e simpatizza) da un paese qualsiasi proverà ad attaccare le infrastrutture in questo modo. Vi penetrerà e farà qualche danno. Niente di spettacolare, ma sarà un tentativo riuscito.

La soluzione è duplice. Primo, evitare che sistemi come DCS e SCADA finiscano su Internet. Secondo, modificare i protocolli in modo da incrementare la sicurezza. E terzo, niente panico: il rischio non è poi così alto.

Argomentazione: siamo in pericolo

<<http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html>>

<http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_2070000/2070706.stm>

<<http://www.cnn.com/2002/US/06/27/alqaeda.cyber.threat/index.html>>

Contro-argomentazione: non lo siamo

<<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/06/30/MN152350.DTL>>

Un vero attacco:

<<http://www.theregister.co.uk/content/4/22579.html>>

** **

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo quinto anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare tutti a questo indirizzo: <<http://www.counterpane.com/crypto-gram.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

La nuova generazione dell'hacking telefonico:

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

Il monitoraggio innanzitutto:

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

L'esposizione totale e la CIA:

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

Unicode e i rischi legati alla sicurezza:

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

Il futuro del "Crypto-Hacking":

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

I pasticci e le approssimazioni di SSL:

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

La declassificazione di Skipjack:

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

** **

Il Canile: Cryptico

Mi basta citare dal comunicato stampa: "Dalla combinazione di matematica del caos e di computer science, la compagnia danese Cryptico ha sviluppato un nuovo incredibile algoritmo di cifratura, superiore a qualsiasi altra soluzione attualmente sul mercato. Il prodotto, chiamato CryptiCore (tm), è in grado di cifrare alla velocità di 1 Gigabit al secondo, cioè da cinque a dieci volte più velocemente degli altri algoritmi. La compagnia ha ordinato dettagliate richieste di brevetto su questa tecnologia".

E, tra le altre cose, "Questa tecnologia è avvalorata da parecchi esperti riconosciuti a livello internazionale". Ovviamente non vengono fatti nomi.

Mi sorprende sempre nel constatare quanta gente crede a questa roba.

<<http://www.2minvest.com/news.asp?id=216>>

** **

News

La grande notizia riguarda il nuovo sistema Palladium di Microsoft. So di doverci ritornare più dettagliatamente, ma questo mese non ne ho avuto il tempo: sarà per la prossima volta. Per intanto vi lascio con i miei tre dubbi principali. Primo: sicurezza per chi? Sembra proprio che questo sistema significhi sicurezza più per Microsoft e Disney che per chi possiede il computer. Secondo: ma Microsoft si rende conto che qualche fantasioso aggeggio hardware per la crittografia non risolve i bug del software? In Microsoft si ricordano dei bug che hanno afflitto il loro ultimo tentativo di code signing, ActiveX? Terzo: quali sono le problematiche antitrust legate al fatto di prendere protocolli standard e sostituirli con protocolli proprietari Microsoft? Ad ogni modo, vi sono anche molte buone idee in Palladium, ma bisogna assicurarsi che vengano sfruttate in maniera corretta.

Gli USA costruiscono e lanciano costosissimi aerei-spia, e poi condividono i risultati con chiunque voglia controllarli.

<<http://www.cnn.com/2002/TECH/science/06/13/nato.spyplane/index.html>>

<<http://www.newscientist.com/news/news.jsp?id=ns99992405>>

<http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=738&e=3&u=/nm/20020613/tc_nm/nato_surveillance_dc_7>

Considerazioni sul terrorismo:

<<http://www.infowarrior.org/articles/2002-07.html>>

Interessanti problematiche di sicurezza legate a Kazaa. Sapete l'ultima? Molte persone non installano correttamente Kazaa e si ritrovano inavvertitamente a condividere parecchi file personali.

<<http://zdnet.com.com/2100-1105-933836.html>>

<<http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf>>

"Tecnologie per rendere sicuri gli edifici Federali", un lungo e interessante resoconto del GAO.

<<http://www.gao.gov/new.items/d02687t.pdf>>

Degli hacker sono penetrati all'interno della rete governativa della California e hanno avuto libero accesso per un mese intero alle informazioni personali di 265.000 impiegati statali. La dichiarazione più irritante proviene dall'ufficio governativo californiano: "Le nostre difese non sono poi così male, e poi cose del genere accadono in continuazione". Ma santo cielo, gente, assumetevi le responsabilità per il vostro network.

<<http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2002/05/25/MN179392.DTL>>

I siti Web dell'esercito americano non sono messi tanto meglio, pare.
<http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_2049000/2049780.stm>

La cyber-sicurezza è al terzo posto nell'elenco delle priorità per l'FBI, dopo il terrorismo e lo spionaggio.
<<http://zdnet.com.com/2100-1105-927933.html>>
<http://www.gcn.com/vol1_no1/daily-updates/18800-1.html>
<<http://www.wired.com/news/politics/0,1283,52853,00.html>>
<<http://www.computerworld.com/securitytopics/security/story/0,10801,71533,00.html>>

Un articolo che spiega i motivi del fallimento delle PKI:
<<http://www2.cio.com/research/security/edit/a05232002.html>>

I rischi legati alla sicurezza nella trasmissione di numeri di carta di credito attraverso le reti wireless.
<<http://www.newsfactor.com/perl/story/18134.html>>

Il terrorismo potrebbe diventare lo stimolo per una migliore e più pervasiva cyber-assicurazione.
<<http://www.washingtonpost.com/ac2/wp-dyn/A27682-2002Jun10>>

Eccellente confutazione dell'articolo della Alexis de Tocqueville Institution sulla presunta scarsa sicurezza del software open source, di cui abbiamo discusso il mese scorso.
<<http://www.theregus.com/content/4/25196.html>>
Microsoft, dal canto suo, ammette di finanziare l'AdTI.
<<http://www.wired.com/news/business/0,1367,52973,00.html>>
<<http://online.securityfocus.com/columnists/89>>
Nessuna dichiarazione per chiarire se Microsoft abbia o meno finanziato quello scritto, ma lo scorso anno la stessa organizzazione aveva pubblicato un articolo che esaltava i benefici dei programmi di certificazione Microsoft.

Un altro comunicato-burla:
<<http://news.com.com/2100-1023-935188.html>>
<<http://www.usatoday.com/life/cyber/invest/2002/06/12/phony-release.htm>>

Un buon articolo sul perché il software è così malfatto, e alcune possibili soluzioni:
<<http://www.technologyreview.com/articles/mann0702.asp?p=0>>

I bagarini modificano il sistema di prenotazioni del Campionato Mondiale:
<<http://www.ds-osac.org/edb/cyber/news/story.cfm?KEY=8341>>

Difetti dei procedimenti dell'FBI nel gestire le vulnerabilità informatiche:
<<http://www.cnn.com/2002/TECH/industry/06/18/computer.security.ap/index.html>>
<<http://news.zdnet.co.uk/story/0,,t269-s2111994,00.html>>

Ancora sulla responsabilità connessa al software:
<<http://zdnet.com.com/2100-1104-936945.html>>
<<http://www.usatoday.com/life/cyber/tech/2002/06/17/microsoft-security.htm>>
<<http://www.cio.com/archive/061502/safer.html>>

Attacchi dall'interno: impiegati sabotatori.
<http://www.cio.com/archive/060102/doom_content.html>

Gruppi di hacker pro-Islamici: realtà o invenzione della stampa?
<<http://www.mi2g.com/cgi/mi2g/press/180602.pdf>>

Uno studente afferma di aver rivoluzionato la crittografia dopo aver visto un cartone animato. (Come mai non si incontrano mai degli articoli su persone che hanno rivoluzionato, che so, la neurochirurgia?). Almeno la stampa più importante ha ignorato questa storia.
<<http://chronicle.com/free/2002/07/2002070301t.htm>>

La MPAA (Motion Picture Association) sta cercando di convincere il Congresso a imporre un "Broadcast Flag", una sorta di contrassegno sulla diffusione audio/video che i computer e hardware simili, una volta riconosciuto, si rifiuterebbero di copiarlo. Leggetevi prima le FAQ della MPAA sul contrassegno, e poi la confutazione delle stesse FAQ da parte dell'Electronic Frontier Foundation (EFF):
<<http://bpdg.blogs.eff.org/archives/000148.html>>

Tassonomia dell'attacco DoS distribuito:
<http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf>

Signal Intelligence (SIGINT), il data mining e l'analisi di traffico nella guerra alla droga:
<<http://www.business2.com/articles/mag/print/0,1643,41206,FF.html>>

Una campagna tedesca contro il trattenimento dei dati:
<<http://www.stop1984.com/index2.php?text=letter.txt>>

** ** ** ** **

Le news di Counterpane

Il secondo trimestre 2002 è stato il migliore in assoluto. Sempre più compagnie (e molti grossi nomi) ci richiedono di monitorare le loro reti. E sempre più distributori stanno offrendo i servizi di Counterpane. Siamo ormai la più grande azienda di monitoraggio della sicurezza a livello mondiale, e continuiamo a crescere.

I nuovi rivenditori di Counterpane:
<<http://www.counterpane.com/pr-resellers2.html>>

** ** ** ** **

Il virus Perrun

Il 13 giugno, McAfee ha pubblicato un comunicato stampa che descrive un nuovo virus che colpisce i file JPEG, come per esempio le fotografie digitali. Nei classici termini allarmistici, il comunicato cerca, spaventando un po' tutti, di indurci ad acquistare o ad aggiornare il software antivirus.

Questa storia fa emergere tre punti importanti. Il primo riguarda una cosa che ho già detto: non c'è separazione tra file di dati e di programmi. Abbiamo visto dei virus che colpiscono i file di dati di Microsoft Office, e virus che colpiscono file Postscript. Un virus che mira ai file JPEG non è niente di eccezionale, come non lo sarebbe un virus che infettasse i formati XML, PDF, ecc. Basta aspettarselo. Se non accadrà con la presente incarnazione di un tale formato, avverrà con una successiva.

Il secondo punto è che questo presunto virus non ha niente a che vedere con il fenomeno appena descritto. Non esiste alcun virus eseguibile all'interno dello JPEG. Con ottima approssimazione posso affermare che Perrun non è nemmeno un virus: è un programma, un eseguibile EXE, che inserisce del codice nei file JPEG. Senza il file EXE non accade nulla. Può funzionare soltanto se si è già infettati, con un programma che estrae il codice dalle immagini. Ma tutto questo non solo è debole, è proprio stupido. Sono esterrefatto che un qualsiasi competente ricercatore di virus abbia degnato questa storia della pur minima attenzione.

Terzo e ultimo punto: si noti come McAfee sfrutti questa storia per seminare panico. Questo non è un virus che sta effettivamente colpendo dei computer. Non è un virus che viene dal nulla. Non è nemmeno una minaccia nell'immediato. Secondo la stampa "i ricercatori di McAfee hanno ricevuto il virus direttamente dal suo creatore".

Ho sempre sospettato una certa intimità fra gli autori di virus e le compagnie produttrici di software antivirus. Le seconde hanno di certo bisogno dei primi, con lo scopo comune di far parlare dei virus e di ottenere una costante ondata di guadagni dai vari aggiornamenti. Ed ecco un esempio di scambio di informazioni.

Da: Chel van Gennip <chel@vangennip.nl>
Oggetto: Rimediare agli insuccessi dell'Intelligence

Ritengo che lei non abbia sviluppato un punto della questione. La sicurezza non è altro che il controllo dei danni a un costo ragionevole. Per quanto concerne il terrorismo, questo controllo è limitato: i costi per una sicurezza al 100% sarebbero troppo elevati. Lei ha parlato delle conseguenze sulle libertà civili e sul denaro speso. Con una sicurezza al 100%, questa sicurezza sarebbe l'unica cosa che avremmo.

Uno dei problemi risiede nel fatto che il nemico non ha una base centrale, un quartier generale, e questo limita di molto un approccio tradizionale. Un altro problema è la totale inosservanza, da parte del nemico, di molti valori fondamentali, in primis della propria vita. Questi due fattori rendono estremamente difficile combattere contro una tale minaccia. Ritengo che un approccio strategico contro questo nemico debba tenere conto dei due problemi seguenti: dare all'avversario qualcosa da perdere, per renderlo vulnerabile, e cercare di riportarlo verso una maggiore osservanza della sua ideologia sostenendo alcuni aspetti di quell'ideologia oppure creando divergenze.

Un approccio, per così dire, simile a quello degli antichi Romani: panem et circenses.

Da: Mike <John.Michael.Williams@Computer.org>
Oggetto: Rimediare agli insuccessi dell'Intelligence

Le sue osservazioni mi ricordano ciò che ho sempre sostenuto per anni con quelli della mia cerchia che avevano motivo di darmi retta: la deficienza fondamentale dell'Intelligence statunitense sta interamente nell'eredità di J. Edgar, che ha consolidato tutto il controspionaggio e il controterrorismo in una struttura "di polizia" e di forza dell'ordine, in parte come gioco di potere, ma soprattutto come patriota (a nessun altro importava, in quei giorni). Altri potevano avere voce in capitolo (come Angleton), ma l'FBI aveva poteri di polizia: erano armati, pericolosi, ed estremamente inquisitivi; uno scalpo in più sulla cintura significava moltissimo, più per la carriera che per la sicurezza, però, specialmente dove occorrevo strategie sul lungo termine.

Mi meraviglia il fatto che nessuno finora, in tutta la stampa accessibile, abbia paragonato la STRUTTURA dell'intelligence americana a quella, più efficace, di altri paesi, compresi il Regno Unito e Israele, a cui lei fa riferimento.

Gli israeliani hanno la Mossad, il loro "istituto" di intelligence internazionale di alto profilo, prendendosi l'opposizione mentre moltissime altre entità, come quelli che mandano avanti Pollard possono al più essere definiti dei bricconi. Gli israeliani hanno poi lo Shin Bet per la sicurezza interna, un'organizzazione apparentemente ed efficacemente separata, e di solito ben coordinata. E con ogni probabilità hanno anche un equivalente dello Special Branch, data la loro eredità britannica.

Gli inglesi hanno un'organizzazione tripartita: il SIS (il Secret Intelligence Service, detto anche MI6, istituito per il solo spionaggio internazionale); il Security Service (detto anche MI5, istituito per l'interno, forse per rimediare all'inefficienza di quello del Commonwealth, non so.); e il reparto speciale di Scotland Yard, lo Special Branch, la "polizia nazionale". Le forze dello Special Branch, debitamente indottrinate e addestrate, possono immischiarsi in casi di sicurezza nazionale o estera, nel caso si debba procedere a prosezioni e arresti.

Né l'MI5 né l'MI6 hanno poteri di polizia. Le intercettazioni che vengono fatte da parte di "personale per la sicurezza del governo britannico" senza alcun mandato - me lo conferma un alto burocrate inglese - non possono essere usate in tribunale. E credo vi siano altre analoghe restrizioni significative sulla presentazione di prove raccolte dall'MI5.

Dove sono gli accademici, i teorici, i professionisti, gli operatori? Abbiamo bisogno del loro apporto e della loro opera di confronto comparativo nei confronti di questi attuali pasticci, prima che la Sicurezza Nazionale segua le orme del vecchio J. Edgar.

Da: Mike Robinson <miker@sundialservices.com>
Oggetto: Rimediare agli insuccessi dell'Intelligence

Nessuno ha parlato del sondaggio d'opinione come problematica per la sicurezza, e dubito che se ne parlerà... ma la storia (e anche le politiche aziendali) ci dice con chiarezza che alcune delle peggiori decisioni intraprese sono arrivate come pronta reazione da parte di un politico o di un funzionario che non si è preventivamente circondato delle più esaustive e obiettive fonti di informazione disponibili... in barba agli esperti di indagini-campione. In tempi di guerre e crisi, a maggior ragione, l'aspetto decisionale deve necessariamente precedere l'opinione pubblica. Le decisioni più coraggiose e importanti non sono mai state molto popolari ai tempi in cui furono intraprese.

Da: Abdul Rehman Gani <abdulg@eastcoast.co.za>
Oggetto: Rimediare agli insuccessi dell'Intelligence

Mi rattrista vedere come la discussione si sia spostata a come migliorare le attività dell'intelligence e l'analisi per prevenire futuri attacchi terroristici, quasi come se fossero inevitabili. Questo, unito alle gravi incursioni entro le libertà civili in una delle nazioni più libere del mondo, lascia il singolo individuo di fronte a un triste futuro. Abbiamo forse inseguito una chimera, qui in Sudafrica, quando sognavamo un futuro di democrazia che garantisse i diritti umani? La pace e la prosperità sono ottenibili solamente con la limitazione delle libertà civili, della libertà di espressione, attraverso provvedimenti razzisti e una maggiore intrusione nelle nostre vite? Non è forse qualcosa che abbiamo messo da parte quando Nelson Mandela divenne presidente nel 1994?

Per fortuna non è di questo che abbiamo bisogno. Le cose sembrano prendere questa piega perché gli Stati Uniti stanno reagendo con piani di trattamento dei sintomi e non dei problemi. Quanti altri tiranni e dittatori riceveranno fondi, armi e supporti dal vostro governo prima che gli americani si rendano conto che tutto questo digrignare i denti, tutti questi allarmi antiterrorismo, e tutti i miliardi di dollari spesi nel tentativo di monitorare ogni cosa non è un modo efficace di procedere? Quanti altri interessi particolari dovranno ancora influenzare le politiche di mercato e quindi distruggere le economie più giovani in nome del libero mercato?

Perché non spendere miliardi (se occorre spendere tali cifre) nell'esportazione di democrazia, nell'implementare un commercio reale ed equo, e premiare i progressi concreti di quei paesi in via di sviluppo? L'America non deve necessariamente possedere tutto.

C'è un punto di vista assai comune e condiviso fuori dagli USA secondo cui, vista l'influenza della politica americana nelle nostre vite, dovremmo avere anche noi voce in capitolo nella scelta del presidente degli Stati Uniti. Ciò ovviamente è assai improbabile che accada. Tutto ciò che possiamo fare è sperare che voi cittadini americani teniate gli occhi aperti e non vi facciate distrarre dal vostro governo in merito a quelli che sono i veri problemi, come la politica estera degli USA.

Ciò significa spingere il vostro governo a una maggiore correttezza, così che possiate raccogliere i frutti della pace. Così che possiate affermare che il vostro non è soltanto un paese potente, ma che è anche grande.

Dopo l'11 settembre l'America dovrebbe impegnarsi a ridurre il numero di persone che vorrebbero agire contro di essa, invece che continuare a mietere odio e poi stare sulla difensiva. Ma questo pare impossibile, e in un simile scenario un altro attacco è purtroppo inevitabile.

Da: "Lucky Green" <shamrock@cypherpunks.to>
Oggetto: Ordigni nucleari

Installare un ordigno nucleare in una cavità del sottosuolo o in un tunnel della metropolitana non è granché come effetto moltiplicatore. Si tratta solo di una variante di quella che sarebbe una deflagrazione a livello del terreno. Come dovrebbe sapere un qualsiasi apprendista terrorista nucleare, il sistema tradizionale per aumentare sul lungo termine l'impatto di un'arma nucleare è quello di avvolgerla nel cobalto.

Parentesi di natura fisica: il normale cobalto 59 assorbirà volentieri l'enorme quantità di neutroni generata dall'ordigno. Una volta che un neutrone viene catturato, il cobalto 59, di facile reperibilità, diviene cobalto 60, una sostanza altamente radioattiva comunemente utilizzata per fornire energia a dispositivi di irradiazione di uso medico. Il cobalto 60 decade con un periodo di dimezzamento di alcuni anni rispetto al nickel 60, che a sua volta rilascerà immediatamente l'energia in eccesso sotto forma di due particelle gamma ad alto coefficiente energetico prima di trasformarsi in normale nickel. Come risultato della suddetta radiazione gamma, l'area coperta dalle radiazioni rimarrebbe inabitabile per svariati decenni.

La prima volta che ho letto di questa modalità di "inquinare" un'arma nucleare è stato in un fumetto di Superman quando avevo all'incirca sei anni. Quest'anno ne compirò 40.

Direi che il punto è su come estendere l'impatto di un ordigno nucleare a periodi di tempo prolungati. Non c'è alcun motivo razionale, da parte di un giornalista oggi, per non pubblicare questi concetti. A meno che l'America non intenda mettere all'indice le biblioteche, i libri di testo di fisica nucleare elementare, e anche i fumetti di trent'anni fa.

Fra l'altro, se lei è interessato ad approfondire i concetti relativi alle armi nucleari, consiglio la lettura del libro di John McPhee "The Curve of Binding Energy". È un testo molto accessibile, e si legge d'un fiato. Non è necessaria alcuna cultura specifica. Il libro tratta inoltre della possibilità di abbattere le Torri Gemelle con un ordigno nucleare fatto in casa. Naturalmente ora sappiamo che non è stato nemmeno necessario ricorrere a un'arma del genere.

Da: <microlenz@earthlink.net>

Oggetto: Ingannare la polizia con impronte digitali falsificate...

Dia un'occhiata al racconto "L'avventura del Costruttore di Norwood" di Sir Arthur Conan Doyle, dove si dice: "[...] Quando quei pacchetti furono sigillati, Jonas Oldacre fece in modo che McFarlane chiudesse uno dei sigilli apponendo il proprio pollice sulla cera fresca. [...] Fu poi estremamente semplice prendere un calco dell'impronta dal sigillo, bagnarlo con tutto il sangue che si poteva ottenere pungendosi con uno spillo, per poi trasferire l'impronta sul muro durante la notte..."

È chiaro che le impronte di gelatina di cui si è parlato sono più sofisticate, ma sono anche passati cent'anni!

Da: <bryk@SOFTWARE.ORG>

Oggetto: Numeri di carta di credito "usa e getta".

I "veri rischi" a cui lei allude sono quelli dei commercianti (e possibilmente di Citibank), non miei.

Ho dato un'occhiata, tempo fa, ai numeri virtuali di carte di credito di Citibank e non ho trovato molti incentivi nel farne uso. Certo, lo schema è interessante. Ma aiuta a proteggere Citibank e i commercianti, non me. Se la mia carta di credito viene rubata e utilizzata per acquisti illeciti, chi è da ritenersi responsabile? In molti casi, non certo io. Come afferma il loro annuncio pubblicitario, "Come sempre, zero dollari di responsabilità per addebiti non autorizzati sul vostro conto... Se non avete comprato, non pagate. Garantito". E questo non è affatto diverso dalle normali carte di credito.

Da: "Benjamin J. Tilly" <ben_tilly@operamail.com>

Oggetto: La sicurezza e il protocollo SOAP

Gunnar Peterson [l'autore dell'email pubblicata nel numero scorso] evidenzia correttamente i benefici per lo sviluppo facendo uso del protocollo SOAP. SOAP rende più semplice sviluppare. Un buon modello semantico facilita l'integrazione dello scopo attraverso la progettazione del sistema, cosa che a sua volta facilita la progettazione di sistemi che si rivelano sicuri se i livelli sottostanti funzionano tutti come previsto (e non è detto: si veda la sua nota su Unicode).

Tuttavia questo fraintende completamente la natura della minaccia di cui è preoccupato.

La sicurezza non è primariamente un problema che nasce dall'incapacità di un singolo progetto di essere debitamente designato e implementato. Le minacce legate alla sicurezza nascono perché, fra tutti i progetti in cui investire fiducia, alcuni o molti di essi finiranno con l'avere delle debolezze che attireranno potenziali malintenzionati. Ci si deve anche guardare, fra le altre cose, da un certo tipo di monitoraggio automatizzato che è in gran parte indipendente dal codice dell'applicazione (codice, in un certo qual modo, poco attendibile).

Detto questo, si considerino le seguenti osservazioni:

- Le applicazioni realizzate con SOAP saranno progettate nello stesso modo in cui oggi il software viene progettato. Il che significa scarsa comprensione e consapevolezza delle problematiche di sicurezza, e molte opportunità di commettere errori basilari e ben noti da parte di persone relativamente inesperte.

