Multimedia
INDIRIZZO ELETTRONICO: multimedia@mclink.it

il fisco RIVISTA
CHIAMATA GRATUITA NUOVI ABBONAMENTI
Numero Verde 167-861160

Internet. Sulla rete tutto è pubblico ma pochi lo sanno. Cosa fare per difendersi dalla «curiosità» altrui

Nelle piazze virtuali solo segreti di Pulcinella

Su Internet nulla è segreto. Neppure il numero della carta di credito che usate per fare gli acquisti nei supermarket virtuali. Per questo diventa imperativo mettere a punto dei sistemi di cifratura dei messaggi che siano facilmente utilizzabili e soprattutto inattaccabili dai malintenzionati. La tecnologia è disponibile, ma gli Stati Uniti cercano di impedirne la diffusione per paura che gruppi criminali la possano utilizzare.

ANTONIO NAVARRA

Uno dei grandi problemi di Internet, forse anzi il problema più importante, è che non si tratta del posto migliore per manipolare dati riservati, perché tutto è pubblico, trasparente e potenzialmente aperto a qualunque operatore esperto, bene o male intenzionato.

Il caso classico è quello delle carte di credito. L'operazione commerciale più semplice e fattibile sulla rete è l'acquisto di un bene in uno shopping centre virtuale. Per fare l'acquisto è necessario che un messaggio contente l'ordine e l'indicazione del mezzo di pagamento - il numero della carta di credito - venga inviato sulla rete. Il pericolo è che qualcuno intercetti il messaggio e quindi usi i numeri della carta di credito in modo fraudolento. In poche parole, spedire il numero della propria carta sulla rete è un grave rischio. Ogni messaggio elettronico va trattato come fosse pubblico.

L'unico modo per proteggersi è nascondere l'informazione, bisogna usare cioè un codice. L'umanità ha sempre usato i codici, in genere per uso bellico. Il codice più semplice consiste nel sostituire i segni dell'alfabeto con altri segni. La A si sostituisce con la N, la B con la S, e così via. Un codice così resiste cinque minuti ad un decrittatore che faccia l'analisi della frequenza delle lettere.

Nel corso degli anni sono stati sviluppati codici sempre più complicati e progressivamente assai più difficili da decodificare, ma tutti essenzialmente basati su un'alterazione dei segni usuali dell'alfabeto. La difficoltà principale con questi codici consiste nel fatto che qualche tipo di informazione in chiaro tra mittente e destinatario deve passare. Se uso un codice a permutazione, bisogna che informi il destinatario di quale tipo di permutazione ho usato. Insomma, devo trasmettergli la chiave, Nel caso della rete è chiaro che non posso mandargli un mewssaggio di posta elettronica con la chiave, perché renderebbe futile il successivo utilizzo della codifica. Il problema sulla rete e in genere in tutti i sistemi di trasmissione è dunque l'uso di cifrari che non richiedano lo scambio di chiavi di decodifica tra mittenti e destinatari.

La soluzione a questo problema è stata data dall'invenzione dei codici a doppia chiave, detti anche a chiave pubblica e chiave privata. In pratica è necessario generare una chiave scomposta in due pezzi. Uno, la chiave pubblica, viene distribuito apertamente. Lo si può mettere anche in rete. Serve a cifrare i messaggi. Chi vuole inviare un messaggio ad una persona ne utilizza la chiave pubblica per rendere il messaggio stesso incomprensibile a tutti salvo che al destinatario. Solo la chiave privata, che è in unica copia ed è in mano al ricevente, può infatti decifrare il messaggio.

Il meccanismo è un po' arcano ma efficace. In pratica, quello che succede è che il messaggio viene codificato usando un prodotto di numeri primi. Per decrittarlo bisogna scomporre in fattori questo numero, un'operazione molto semplice, ma enormemente lunga nel caso che il numero da scomporre sia molto grande. L'algoritmo più noto utilizzato per definire questi codici a doppia chiave è conosciuto con la sigla RSA, da Rivest, Shamir e Adleman, i tre scienziati che lo definirno nel 1977. Secondo quanto affermano dei ricercatori della università canadese della British Columbia, per «rompere» una chiave RSA di trecento caratteri sarebbero necessari 300 miliardi di miliardi di MIPS-anni (un MIPS-anno corrisponde ad computer che lavora per un anno ad una velocità di un milione di istruzioni al secondo).

Certo, il codice perfetto è quel codice che richiede un tempo infinito per essere penetrato, un codice buono richiede molto tempo, per esempio migliaia di ore di calcolo di un supercalcolatore. Un tempo che deve essere misurato anche in termini di costo. Alla fine il quesito al quale si deve rispondere per valutare l'affidabilità di un codice è proprio questo: quanto costa romperlo e quanto ne può ricavare l'attaccante. La capacità di calcolo dei moderni personal computer è oggi tale da riuscire a generare e gestire chiavi di lunghezza tale da scoraggiare la maggior parte degli attaccanti. Per questo oggi le informazioni sulle carte di credito e simili possono essere agevolmente trattate con l' RSA. L'ostacolo, semmai, è politico. L'algoritmo RSA è disponibile pubblicamente negli Stati Uniti ma non può essere esportato perché è soggetto alle stesse limitazioni di esportazione del materiale di armamento. Questo ostacolo, tutto sommato burocratico, potrebbe essere rimosso, ma ad esso si accompagna una preoccupazione più concreta e politica: il timore, diffuso nelle agenzie investigative degli Stati Uniti, è che i gruppi criminali globali usino l' RSA per comunicare tra loro in modo pressoché inattaccabile dall' FBI. La pressione per uscire da questa impasse è ormai enorme e la soluzione è forse vicina, con un compromesso tra esigenze della privacy individuale e necessità della sicurezza nazionale. Quando ciò avverrà assisteremo alla seconda esplosione di Internet e un vertiginoso aumento delle sue possibilità.

E c'è anche un software per cifrare le telefonate

Da oggi potete cifrare anche le vostre telefonate. Phil Zimmerman, inventore del software crittografico a doppia chiave PGP, ne ha infatti realizzata una versione per rendere inintellegibili le telefonate. E' sufficiente collegare il vostro computer alla linea telefonica tramite un modem, aggiungervi un microfono ed un paio di cuffie, e installarvi il PGPFone. Da quel momento, qualsiasi cosa diciate ad un vostro interlocutore che disponga dello stesso software sarà cifrato istantaneamente e inviato sulla linea telefonica come un insieme di segnali assolutamente inintellegibili ad un eventuale spione.
Il PGPFone è attualmente in versione Beta, signifca cioé che non é ancora definitivamente a punto. Tuttavia è già disponibile in rete, sia per Macintosh, che per Windows e potete dunque già sperimentare da voi stessi il brivido del piccolo 007.
La qualità della trasmissione varia in base alla capacità di elaborazione del vostro computer. Ma già con una macchina media la voce è molto naturale e la conversazione avviene senza difficoltà. Per avere maggiori informazioni collegatevi a http://www.primenet.com/(tilde)wprice/pgpfone.html

Phil Zimmerman, inventore del Pgp. Accanto, una cabina installata al salone MacWorld per usare il telefono su Internet
Julia Malakie/Ap

Presto possibili su Internet anche le transazioni bancarie

Verso una rete top secret

TONI DE MARCHI

Come è facile immaginare, sulla rete si trovano decine di software che vi aiutano a proteggere i vostri dati. Il più famoso ed il più facilmente ottenibile si chiama PGP, ovvero Pretty Good Privacy, che si potrebbe grosso modo tradurre "una riservatezza niente male".

Per quanto sia un software cosiddetto freeware, cioé disponibile gratuitamente in rete, ha già provocato delle gigantesche controversie negli Stati Uniti e fuori. Il suo creatore, Phil Zimmerman, soltanto lo scorso gennaio è stato definitivamente prosciolto dopo un'inchiesta federale durata due anni dov'era accusato di aver illegalemte esportato questo programma i cui algoritmi di cifratura sono così potenti da mettere in crisi persino i supercomputer della NSA, l'agenzia americana incaricata dello spionaggio elettronico.

Oggi PGG è disponibile in due versioni, una per il mercato statunitense ed una internazionale. Sono assolutamente identiche, garantisco il medesimo livello di protezione dei dati. Cambia solo la proprietà dell'algoritmo interno. Attualmente l'ultima versione internazionale è la 2.6.3i ed è disponibile da moltissimi siti, tutti raggiungibili dalla International PGP Home Page (**http://www.ifi.uio.no/staalesc/PGP/**, n.b. prima di «staalesc» e dopo la barretta va inserita una tilde, quel segno ondulato normalmente usato nello spagnolo che noi per ragioni tipografiche non possiamo riprodurre) curata da un ricercatore norvegese. PGP è disponibile in versioni per tutti i sistemi operativi, dal Macintosh allo Unix.

Chi cerca invece prodotti più rifiniti soprattutto sul piano dell'interfaccia se sta fuori degli Stati Uniti per il momento non ha scelta. Tutti i software disponibili possono essere esportati solo con versioni "deboli" della chiave di cifratura, relativamente facili da attaccare.

La statunitense Viacrypt (**http://www.viacrypt.com**) produce una versione commerciale del PGP, e proprio nei giorni scorsi è stata acquistata dalla PGP Inc. (**http://www.pgp.com**), la neocostituita società di Phil Zimmerman che ha finalmente deciso di impegnarsi direttamente sul mercato.

Di grande interesse l'estesa gamma di software criptografico della RSA Data Security (**http://www.rsa.com**), creata dai padri dell'algoritmo RSA. Qui si può trovare tutto quello che serve per proteggere anche i dati più riservati. Dal software di uso personale, l' RSA Secure di cui ci si può scaricare una copia di valutazione, fino alle specifiche di SET (Secure Electronic Transactions), lo standard ufficialmente adottato dai circuiti Mastercard e Visa per la protezione delle transazioni su Internet tramite carta di credito. L'adozione di SET come standard comune delle due più importanti organizzazioni mondiali di gestione delle carte di credito è un deciso passo avanti verso la definitiva affermazione del commercio on line. Benché SET non sia uno standard prodotto dalla RSA, tuttavia esso utilizza molte tecnologie messe a punto dalla società californiana, in particolare il sistema di cifratura a doppia chiave. L'accordo su SET isgnifica che nei prossimi mesi avremo browser capaci di gestire in modo del tutto trasparente all'utente transazioni finanziarie anche molto importanti, senza rischi. Almeno in teoria.

Ub E

#253 L'Exploratorium di San Francisco è uno dei più straordinari luoghi, forse il più straordinario, in cui la scienza si fa spettacolo. Fondato dal fratello di Roberto Oppenheimer (il signore che dirigeva il laboratorio di Los Alamos dove venne concepita la bomba atomica), è diventato il punto di riferimento per insegnanti, divulgatori e appassionati. O semplici curiosi di cose scientifiche. Il suo sito Web permette ovviamente di viaggiarvi dentro. Ma soprattutto di avere spiegazioni, disegni, proposte per esperimenti scientifici didattici continuamente nuovi.
http://www.exploratorium.edu/
#254 Un altro sito meno noto, ma divertentissimo, per divertirsi con la scienza è quello del «The Tech Museum of Innovation», di San José, California. C'è un po' di tutto, dalla robotica ai laser, passando per la vista, senso chiave dell'uomo nell'era informatica. Vi segnaliamo in particolare il percorso del colore: vi si può osservare come vedono la stessa immagini diversi animali.
http://www.thetech.org/
#255 «Reputation, reputation, reputation! Oh, I have lost my reputation! I have lost the immortal part of myself, and what remains is bestial» dice Cassio a lago nell' Otello shakespeariano. Se volete trovare questa e altre citazioni come l'amletiana «something is rotten in the State of Denmark», rimandi, note e soprattutto il testo completo delle opere del grande inglese c'è un sito che raccoglie tutto in formato ipertestuale.
http://the-tech.mit.edu/Shakespeare/works.html
#256 Tutto per i grandi mangiatori ed i raffinati viaggiatori. Epicurious è un sito che si presenta da solo, gaudente e turgido come si conviene alle cose dell'uomo. Quando ci arrivate potete scegliere quale sezione visitare. Se la vostra preferenza va al cibo la sezione culinaria è ricca e sovrabbondante, così come quella dei vini. Potete imparare come fare una straordinaria grigliata di carne o pesce o comperare dell'ottima carne per posta. Se viaggiate c'è l'altra sezione che si presenta con un «siete virtualmente lì» e poi vi spiega qual è il modo più rapido per uscire da 200 aeroporti di tutto il mondo. Serve altro?
http://www.epicurious.com/

Cd rom

Bambini surreali e metamorfosi all'italiana

Continua la fortunata serie di Stellaris, la versione su Cd Rom del gioco interattivo proposto dalla trasmissione della Rai «Solletico», un programma che forse qualche «grande» non conosce, ma che è fedelmente seguito da ogni bambino che si rispetti. E non delude nemmeno questo terzo incontro con il simpatico professor Magnus e i suoi amici perennemente in lotta contro la dottoressa Frida Friday, *Il compleanno di Medusa* (Pc, distribuzione Sacis, 59.000). Ecco la surreale trama: mentre il professor Magnus e il fedele cane Ciccio stanno esplorando il mondo di Atlantis, vengono fatti prigionieri dalla perfida Medusa. L'unico modo per addolcire la «cattiva» potrebbe essere offrirle un dono per il suo compleanno; e per trovare il giusto regalo e liberare i prigionieri, Max, Silvia e Greta K2 dovranno superare una lunga serie di ostacoli fatti di indovinelli, giochi di abilità, trabocchetti e rompicapo. Il divertimento è assicurato: belli i colori, stimolante la situazione, ricchi gli incastri, molte le possibilità di gioco proposte. L'unico difetto - ma darà fastidio soltanto ai grandi - una certa lentezza nel caricamento di scenari e immagini.

Un Cd «denso» e «ricco». Questi sono i due aggettivi che ci sembrano più appropriati per definire *The Italian Metamorphosis 1943-1968* (Pc, distribuzione Sacis, 79.000). Si tratta di un prodotto sviluppato in occasione della omonima mostra inaugurata nell'ottobre 1994 presso il Guggenheim Museum di New York (che insieme alla Prodotti Museali ha materialmente realizzato il Cd), dedicata alle grandi trasformazioni che hanno caratterizzato la cultura italiana in quei 35 anni. Come si conviene, le nuove tendenze dell'arte di quell'epoca sono lette alla luce dell'intreccio delle vicende politiche, storiche, economiche, sociali, industriali e produttive; e per tener conto di questo intreccio, ci pare che la tecnologia multimediale del Cd Rom rappresenti davvero una validissima soluzione, grazie alla possibilità di passare da un ipertesto all'altro con pochi colpi di mouse. Gli artisti, le opere, i movimenti, le principali manifestazioni, gli eventi storici sono suddivisi in otto percorsi: architettura, arte, ceramica e vetro, cinema, design, fotografia, gioiello, moda. L'imponente dotazione di fotografie, di schede ipertestuali, di spezzoni cinematografici, i brani audio, i filmati d'epoca inediti pescati dall'archivio dell'Istituto Luce, la colonna sonora originale di Luciano Berio: una montagna di materiale per un Cd davvero di grande livello.

[Roberto Giovannini]

In rete negli Usa l'elenco del telefono

Avete perso di vista lo zio americano? Non sapete come trovarlo? Facile, basta cercare su Internet, all'indirizzo http://www.switchboard.com. E' sufficiente scrivere il cognome e in un batter di ciglia avete la risposta sul vostro computer. Tutto gratis. Certo, se scrivete solo il cognome rischiate di ritrovarvi con liste interminabili perché la ricerca è fatta su tutti e 51 gli stati americani. Aggiungere il nome e magari la città aiuta a restringere la ricerca e ad avere risultati più mirati. Con lo stesso metodo potete consultare anche le pagine gialle per cercare quell'azienda di cui avete sentito parlare ma non sapete dove stia. Essenziale, se non altro per curiosità.

E c'è chi con Internet si sballa

Esiste una internet-dipendenza? Si, secondo Kimberley Young, docente di psicologia all' università di Pittsburgh, che ha riferito di un suo studio al congresso della Ameican Psychological Association. Ha studiato ben 396 casi di persone, tra i 14 ed i 70 anni, considerati psicologicamente dipendenti dai servizi on line. Queste persone passano una media di 38,5 ore alla settimana collegate ad Internet, contro le 4,9 di un gruppo di riferimento "normale". Gli Internet-dipendenti si svegliano nel cuore della notte per andare on line, pensano alla rete in ogni momento della loro giornata, anche quando sono con gli amici, si danno malati al lavoro per stare davanti al computer..

È fallita rete telematica Europe On Line

Europe On Line è stata dichiarata fallita dal Tribunale del Lussemburgo. Non è durata neppure un anno l'avventura del primo servizio in rete paneuropeo che era stato lanciato con l'ambiziosa intenzione di fare da contraltare alle statunitensi America On Line e Compuserve. Dietro Europe On Line c'erano all'inizio editori importanti come i tedeschi Burda, Springer, il francese Hachette, l'inglese Pearson. Uno dopo l'altro se ne erano tutti andati, lasciando solo Burda, Difficoltà gestionali e soprattutto una totale incertezza sulla fisionomia da far assumere a questoservizio multilingue (francese, inglese e tedesco) ne hanno decretato una fine prematura.