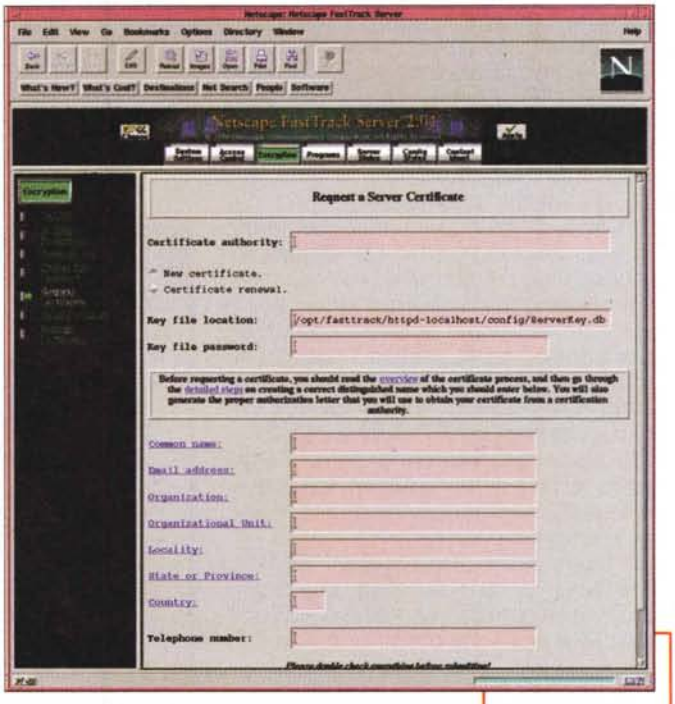
A cura di Corrado Giustozzi

Secure Socket Layer

Linux può essere un'ottima piattaforma per sviluppare applicazioni di commercio elettronico ad un costo contenuto, purché si sia pienamente coscienti delle problematiche relative alla sicurezza e si adottino le opportune precauzioni.

di Giuseppe Zanetti



Dati richiesti per l'ottenimento del certificato SSL.

Facendomi un giretto su www.amazon.com, una delle più grandi librerie su Internet, mi sono imbattuto in un commento di un lettore entusiasta che ringraziava l'autore di un libro su come costruire un negozio elettronico su WWW mediante pochi script CGI. Nelle pubblicità americane i commenti dei clienti soddisfatti si sprecano e spesso sono utilizzati in modo strumentale per vendere il prodotto, tuttavia una cosa risaltava particolarmente in questo caso, ovvero la presunta possibilità di ottenere, con un programma autocostruito e venduto in libreria a soli 30$, lo stesso risultato che si sarebbe ottenuto con un programma dal costo di cento o mille volte superiore. Sarà vero?

Molti di coloro che producono servizi Internet si sono già imbattuti nel problema del commercio elettronico e lo hanno affrontato in modi diversi, a seconda delle specifiche richieste, delle capacità e dell'esperienza di ciascuno.

Se, almeno per la parte di realizzazione della vetrina del negozio, la questione può essere affrontata in modo abbastanza semplice e per soli 30$, lo stesso non si può certamente dire per quanto riguarda le problematiche relative alla sicurezza della transazione commerciale vera e propria.

Il problema

Una delle complicazioni fondamentali del commercio elettronico consiste nel fatto che, utilizzando un comune server WWW, i dati che il browser invia al server possono essere letti in chiaro da chiunque disponga di una macchina connessa ad una delle reti attraverso cui essi transitano. Occorrono, è vero, anche gli opportuni privilegi di accesso alle interfacce di rete, che in Linux/UNIX si ottengono collegandosi come root, tuttavia in altri sistemi operativi meno evoluti essi sono disponibili a tutti gli utenti.

In Linux per ottenere un dump su file di tutti i pacchetti che transitano per la nostra rete è sufficiente eseguire, come root, il comando:

```
tcpdump -i eth0 -w filename
```

Il file così ottenuto può essere ripulito e visionato comodamente, così come è possibile, mediante opportuni parametri di tcpdump, oppure mediante un programmino scritto ad hoc, filtrare, nel modo che al pirata è più comodo, i diversi pacchetti, allo scopo di tenere solamente quelli diretti alla porta TCP del server WWW.

I dati contenuti nel file, una volta ripuliti dalle informazioni relative all'header dei pacchetti TCP/IP, possono essere letti in chiaro, in quanto il protocollo HTTP non esegue una codifica degli stessi, se non quella, banale, necessaria per inviare correttamente i caratteri ad 8 bit.

La spedizione dei dati relativi alle carte di credito e ai dati personali sensibili deve perciò essere effettuata prevedendo particolari misure di protezione, atte ad evitare che essi possano essere intercettati e ne possa essere fatto un utilizzo fraudolento o non conforme al motivo per cui i dati stessi sono stati forniti (come prescritto dalla legge n. 675 del 31/12/96 sulla Privacy).

La confidenzialità dei dati inviati: Secure Socket Layer

La soluzione consiste nello spedire i dati importanti in forma cifrata, utilizzando un algoritmo crittografico a chiave pubblica, in modo che essi possano essere letti solamente dall'effettivo destinatario. L'utilizzo dello strumento crittografico permette inoltre di garantire, oltre alla confidenzialità, anche l'autenticazione dei due soggetti e l'integrità dei dati trasmessi (vedere il riquadro).

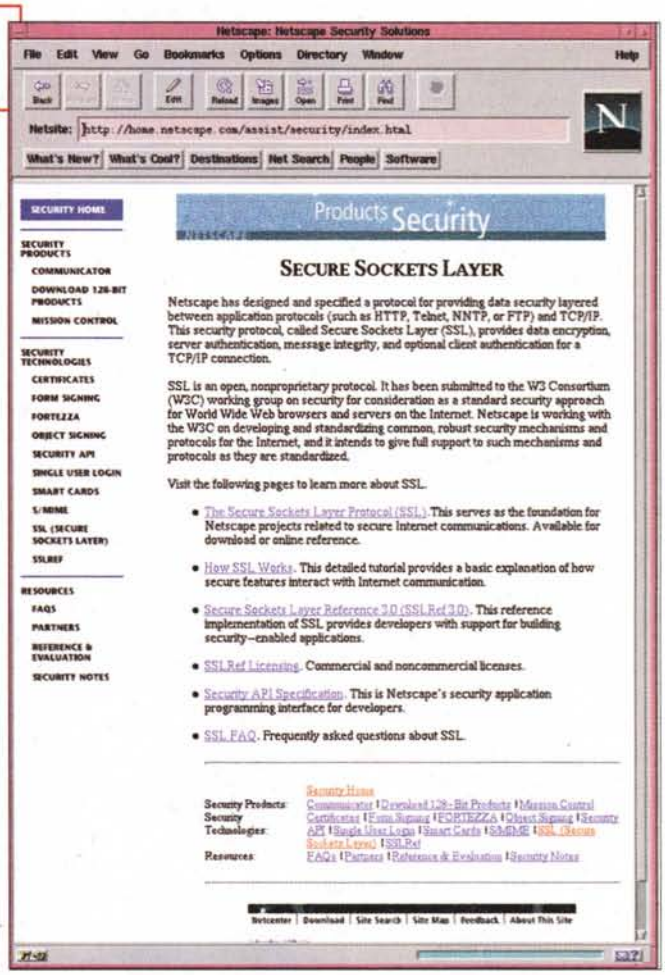
La scelta di quale algoritmo utilizzare, generalmente il migliore fra quelli supportati sia dal client che dal server coinvolti nella comunicazione, e lo scambio delle chiavi pubbliche necessarie alla codifica vengono eseguiti nel WWW mediante il protocollo SSL (Secure Socket Layer), introdotto da Netscape nei propri prodotti Netscape Secure Server e Netscape Navigator, ed ora adottato come standard da quasi tutti i produttori.

L'utilizzo di SSL come protocollo di trasporto sicuro dei dati viene evidenziato dal browser Netscape grazie all'icona a forma di chiave posta in basso a sinistra dello schermo, che appare intera invece che spezzata.

In realtà nel campo dove compare l'URL si nota che il protocollo usato non è più il classico HTTP, bensì la sua versione sicura HTTPS (anche la porta TCP da 80 è divenuta la 443).

L'utilizzo di SSL per il trasporto dei dati ci tutela inoltre contro il rischio che un merchant server si faccia passare per qualcun altro e che noi, ingenuamente, facciamo acquisti nel suo negozio.

La pagina del sito di Netscape che descrive il funzionamento del sistema SSL.



Bookmark

La versione attuale della libreria SSLeay è disponibile su:
ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL/SSLeay-x.x.x.tar.gz

Le applicazioni "sicure" si trovano su:
ftp://ftp.psy.uq.oz.au/pub/Crypto/SSLapps/

La FAQ di SSLeay:
http://www.psy.uq.oz.au/~ftp/Crypto

Stronghold
http://stronghold.c2.net

Thawte Consulting
http://www.thawte.com/

Sioux
http://www.thawte.com/products/sioux

Roxen
http://www.roxen.com

La garanzia reciproca fra venditore e acquirente

La cifratura dei dati, pur garantendo la confidenzialità dei dati contro eventuali occhi indiscreti, non mette tuttavia al sicuro da un utilizzo irregolare degli stessi da parte del negoziante beneficiario della transazione, il quale potrebbe ad esempio addebitarci della merce senza poi spedircela, oppure potrebbe vendercela ad un prezzo diverso da quanto concordato.

La soluzione, semplice nell'idea quanto complessa nella sua implementazione, consiste nell'affidarsi ad un terzo che garantisca sia noi che il negoziante sull'altrui identità ed onestà. Per quanto riguarda la parte relativa allo scambio di denaro, tali garanti esistono già: essi sono le banche e gli enti gestori delle carte di credito, che, se da una parte garantiscono che il cliente abbia un conto in banca adeguato a coprire le spese effettuate, dall'altro garantiscono anche la serietà dell'esercizio commerciale.

I mezzi disponibili per effettuare pagamenti elettronici in modo sicuro sono spiegati nel riquadro a parte.

Il ruolo delle Certification Authority

La soluzione chiave della sicurezza consiste nell'affidarsi ad un terzo di fi-

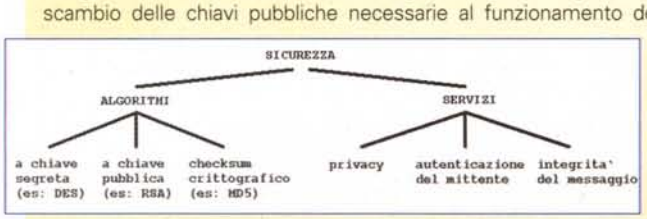
ducia, la Certification Authority (CA), che garantisca, mediante un apposito certificato che il client deve verificare prima di eseguire una transazione sicura, sulle chiavi pubbliche e sull'identità di ambo i soggetti.

La cifratura a chiave pubblica

La crittografia è quella parte della matematica che concerne la cifratura dei dati in modo che essi non possano essere letti da altri, se non dal destinatario. Il processo si avvale di una o più chiavi e può essere di tipo simmetrico (la stessa chiave permette sia la codifica che la decodifica dei dati) che asimmetrico (o a "chiave pubblica").
Nel secondo caso si utilizza una coppia di chiavi, la "chiave pubblica", che può (deve) essere divulgata, e quella "privata", che invece deve essere mantenuta segreta. Il funzionamento del sistema è semplice e sfrutta il fatto che, nonostante con una chiave si possano decodificare i messaggi generati dall'altra, non è possibile (o conveniente) partendo da una trovare la seconda.
Il messaggio da inviare viene codificato utilizzando la chiave pubblica del destinatario, che lo decodificherà mediante la propria chiave privata. Essendo questa in possesso del solo destinatario e non essendoci la necessità di farla passare per la rete, la sicurezza è garantita.
Se invece si utilizza la propria chiave privata per codificare un messaggio, esso può essere letto da qualunque persona a conoscenza della nostra chiave pubblica. Ciò non aggiunge nulla alla sicurezza del messaggio, in quanto rimane leggibile a tutti (dato che la nostra chiave pubblica, per definizione, è in possesso a molti), tuttavia permette di essere sicuri sull'identità del mittente.
L'algoritmo di tipo simmetrico più utilizzato per la codifica di dati è il DES (Data Encryption Standard), mentre quello a chiave pubblica più famoso è RSA (dal nome dei suoi autori: Rivest, Shamir e Adleman).
Attualmente in Internet viene utilizzato anche un altro tipo di codifica, detta di hash, il cui più famoso esponente è MD5, che consiste nel mappare il messaggio in uno molto più breve, in modo tale che il risultato possa essere utilizzato come "firma" per garantire riguardo all'integrità dello stesso (si usa il procedimento crittografico per ottenere una funzione simile al checksum o al calcolo del CRC).

Nella codifica a chiave pubblica, contrariamente a quanto accade usando quella a singola chiave segreta, non è necessario che la nostra chiave privata sia in possesso anche del nostro interlocutore.

Gli algoritmi di crittografia come DES, RSA e MD5 sono solamente i mattoni che permettono di costruire un sistema sicuro. Il problema centrale e più critico in tutti i discorsi sulla sicurezza consiste infatti nella distribuzione delle chiavi da utilizzare per lo scambio cifrato dei dati. Per un file server, ad esempio, è necessaria la sicurezza assoluta sull'identità del client prima di offrirgli accesso in lettura o scrittura ad un disco.
Per risolvere il problema sono state scelte strade diverse, a seconda delle necessità. Ad esempio per lo scambio di chiavi fra client e server TCP/IP, oltre a SSL, può essere utilizzato il protocollo Kerberos sviluppato dal MIT, basato su un authentication server che svolge il ruolo di terzo di fiducia fra gli host che dialogano. Un metodo diffuso per lo scambio delle chiavi pubbliche necessarie al funzionamento del PGP, che permette lo scambio sicuro di e-mail, è invece quello dello scambio delle stesse di persona durante appositi PGP party, organizzati in occasione di raduni di gruppi di utenti o di importanti manifestazioni di informatica.



Tassonomia della sicurezza in rete,

Essa inoltre certifica che noi siamo chi diciamo di essere (denominazione, domicilio, dati anagrafici, diritto d'uso del nome e del dominio, ...). Il certificato infatti viene concesso solamente dopo la verifica, da parte della CA, dei documenti spediti dall'azienda, che, per quanto riguarda l'ottenimento di un certificato SSL, consistono in una visura camerale e nella verifica che l'azienda risulti intestataria dei domini su cui risiede il server.

Come avviene per la registrazione di un dominio, la richiesta di un certificato è soggetta a rinnovo ed al pagamento dei relativi costi di gestione, che generalmente ammontano a poche centinaia di dollari all'anno.

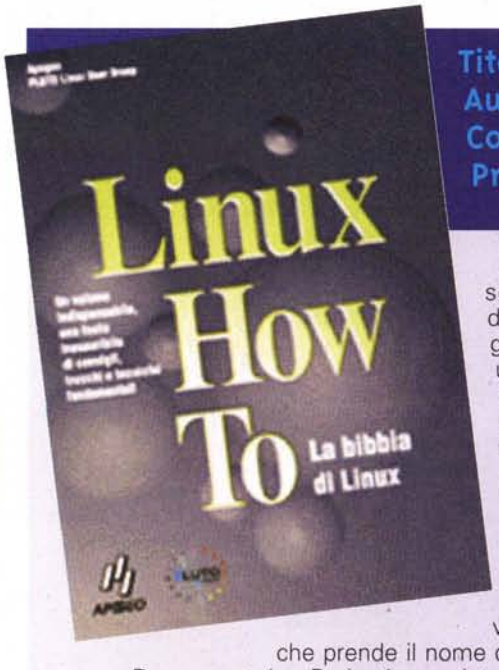
E` necessario porre una certa cura nella scelta della CA, in quanto non tutte (o per meglio dire, quasi nessuna) forniscono certificati al di fuori degli Stati Uniti o per tutti i modelli di server.

Mentre il browser di Netscape permette all'utente di accreditare nel proprio browser certificati emessi da ulteriori CA oltre a quelle già conosciute, la stessa operazione è assai complessa con le versioni 3 di Internet Explorer, costringendo a ricorrere ad una delle CA scelte da Microsoft. Volendo che il nostro sito sia visibile facilmente agli utenti di entrambi questi browser, la scelta si restringe a non più di un paio di CA: VeriSign (http://www.verisign.com), che è la più famosa fra le CA ma offre certificati solamente per pochi server (fra cui purtroppo non l'Apache-SSL per Linux), e la sudafricana Thawte Consulting (http://www.thawte.com), che, oltre ad essere meno restrittiva, ha persino un ufficio a Milano.

Nel caso ve ne fosse la necessità, è possibile acquisire certificazioni ancora più accurate, relative ad esempio alla nostra capacità di mantenere gli impegni finanziari assunti o all'attività che svolgiamo (vendita di computer all'ingrosso piuttosto che di prodotti ittici al dettaglio).

La sicurezza del server innanzitutto

Purtroppo c'è una cosa che nessuna CA è in grado di verificare (almeno non al basso costo che viene richiesto per un certificato SSL), ovvero la sicurezza della macchina che funge da server contro attacchi provenienti dall'esterno. Essa è competenza dei gestori del-



Titolo: Linux How To - La bibbia di Linux
Autori: Vari - Traduzione a cura del PLUTO Users Group
Codice: 317. **Pagine:** 1024. **Formato:** 17 x 24 cm.
Prezzo: L. 65.000. **ISBN:** 88-7303-317-2

Quelli di noi che seguono l'attività del più grande gruppo italiano di utenti Linux sanno che fin dalla sua fondazione uno degli scopi principali è stato quello di produrre documentazione in italiano sul nostro sistema operativo. Il progetto, che prende il nome di ILDP (Italian Linux Documentation Project), consiste nella traduzione (e nel tenere aggiornato il materiale prodotto) di ciò che è reperibile gratuitamente nei diversi siti Internet. I primi documenti ad essere terminati sono stati gli How To, ovvero quelle raccolte di informazioni su aspetti specifici del sistema, dalle istruzioni su come configurare un collegamento ad Internet a tutti i parametri delle diverse schede di rete. Nonostante la tipologia di informazioni contenuta negli How To sia molto variegata, l'utilità di questi documenti è notevole, in quanto spesso contengono delle ricette belle e pronte che permettono di risolvere in pochissimi minuti i problemi più disparati.

I documenti originali sono scritti su base volontaristica e vengono distribuiti secondo la stessa licenza GPL di Linux. La traduzione dei documenti è stata curata da diversi membri del gruppo nel tempo libero ma nonostante ciò è quasi sempre di ottimo livello qualitativo, e così doveva essere considerato il fatto che ogni traduttore, oltre ad essere esperto o comunque utente di Linux, è iscritto ad una apposita mailing list in cui, parallelamente al lavoro di traduzione vero e proprio, si discute su come rendere in italiano i diversi termini incontrati o sullo stile da utilizzare nella traduzione stessa. E' interessante notare come, fra le persone più attive nella lista e più attente alla fedeltà della traduzione ed al rispetto della lingua, vi siano i membri italiani del PLUTO attualmente residenti all'estero.

I documenti tradotti sono disponibili anche gratuitamente in formato elettronico nel sito del gruppo, anche se all'editore va il merito di aver provveduto ad una attenta opera di rilettura e correzione degli stessi ed alla traduzione dei pochi documenti ancora mancanti all'appello.

Oltre ai documenti tradotti, nel libro ne è compreso uno già originariamente in italiano, l'Italian HOWTO di Marco "gaio" Gaiarin, che copre i diversi aspetti di Linux in Italia, a partire dalla corretta configurazione della tastiera e del fuso orario per arrivare alla lista dei negozi e delle librerie italiane dove reperire i CD-ROM ed i testi su Linux.

Nonostante essi siano disponibili gratuitamente in formato elettronico, la possibilità di poter disporre degli How To già stampati e raccolti in modo organico ed ordinato vale senz'altro il prezzo di copertina richiesto, senz'altro inferiore a quanto si spenderebbe stampandosi uno per uno in casa i singoli documenti.

Ovviamente la documentazione disponibile gratuitamente per Linux non si esaurisce con gli How To, ma comprende anche i manuali di sistema, alcuni dei quali già tradotti, così come i libri del Linux Documentation Project (manuale per l'utente, manuale per l'amministratore di sistema, manuale sul networking,...) e la documentazione relativa ad alcuni programmi importanti, ad esempio Gnome.

Se volete collaborare al progetto e fare qualcosa di concreto per Linux, il PLUTO è sempre alla ricerca di nuovi traduttori. Le informazioni sui documenti mancanti e le regole per la traduzione si trovano nel sito del gruppo. Il consiglio è quello di visitarlo anche se non conoscete l'inglese, in quanto, oltre a quello relativo alla documentazione, troverete comunque altri progetti utili a cui poter dare il vostro contributo.

Per ulteriori informazioni:
Libro del PLUTO:
http://www.apogeonline.com/catalogo/317.html
Sito del PLUTO (ILDP):
http://www.pluto.linux.it/ Linux Documentation Project:
http://sunsite.unc.edu/mdw

la macchina e della rete che la ospita e deve essere perseguita tenendo in considerazione che i possibili punti di attacco ad un server sono molti e che, quando si tratta di soldi, sono in molti i pirati disposti a metterci sopra le mani. Avere la possibilità di eseguire uno scambio sicuro di dati non serve a nulla quando gli stessi possono essere ottenuti in modo più semplice direttamente dalla macchina in cui vengono conservati (oppure entrando in possesso di un nastro di backup).

Oltre alle classiche precauzioni di evitare di creare utenti nella macchina e di attivare i soli servizi di rete indispensabili, evitando quelli notoriamente fonte di problemi di sicurezza, come tftp o finger, è bene prevedere anche una politica inflessibile di restrizione degli accessi al server alle sole persone/macchine autorizzate. Essa può essere implementata usando opportunamente il TCP wrapper interno a Linux (tcpd, configurabile mediante i file /etc/hosts.allow e /etc/hosts.deny) e, a livello di rete, mediante un firewall, che può essere realizzato, ad esempio mediante un'altra macchina Linux, usando le apposite funzioni del kernel. L'uso di un firewall permette anche di migliorare la sicurezza contro problemi di eventuali macchine "deboli" della rete, che altrimenti potrebbero essere utilizzate come ponte per accedere più facilmente al server (nel caso ad

esempio l'accesso ad esso fosse permesso da una di queste macchine).

Bisogna infine tenere presente che, analogamente a quanto accade nel caso dell'HTTP, anche gli altri protocolli comunemente utilizzati in Internet (telnet, POP3, FTP,...) si passano le password in chiaro e che è abbastanza banale, anche per un pirata alle prime armi, scrivere un programma che in poche ore è in grado di fare collezione di tutte le password che viaggiano nello spezzone di rete a cui è connesso.

Essendo SSL uno strato (Layer) di software adattabile a qualunque connessione TCP/IP, esistono versioni di client e server in grado di rendere sicura la maggior parte dei servizi di solito utilizzati: telnet, FTP, POP3,...

E` buona norma che essi siano sempre utilizzati al posto degli originali non cifrati per compiere tutte le comunicazioni da e verso il server. Altri programmi basati sulla crittografia, che possono essere usati allo scopo, sono SSH (Secure Shell), CIPE (tunnelling TCP/IP sicuro),...

Scelta del WWW server "sicuro"

Affinché il meccanismo funzioni correttamente, è necessario possedere sia un browser in grado di parlare il protocollo SSL, che un server in grado di capirlo. Mentre come browser si useranno quasi certamente i vari Netscape Navigator e Internet Explorer, possibilmente in ambiente multipiattaforma, per il server bisogna decidere se orientarsi verso un prodotto commerciale o piuttosto verso quanto offre il software libero.

Il ricorso ad un prodotto commerciale è certamente un'ottima scelta, anche perché non si tratta di software particolarmente costoso, in quanto permette di fare le cose in modo veloce e senza possibilità di commettere errori ed evita problemi con le CA che spesso non forniscono supporto per prodotti "fai da te".

Allo scopo un ottimo prodotto disponibile per Linux è il Netscape FastTrack server che abbiamo già incontrato durante la recensione dell'Openlinux di Caldera. Altri WWW server commerciali con supporto di SSL sono: Stronghold, Sioux, Roxen,...

La configurazione del sistema è semplice ma deve essere condotta con una certa cura: essa consiste innanzitutto nella generazione delle chiavi, pubblica e privata, necessarie per il funzionamento degli algoritmi a chiave pubblica. Il livello di sicurezza ottenibile dipende direttamente dalla lunghezza delle chiavi utilizzate, oltre che dal tipo di algoritmo scelto per la codifica. Entrambi questi valori possono essere influenzati da fattori che prescindono quelli tecnici, ad esempio da brevetti o dalla norma, nata durante la guerra fredda, che vieta l'esportazione di certi algoritmi di cifratura fuori dagli Stati Uniti. Così ad esempio gli algoritmi RSA e RC4 non sono legalmente utilizzabili negli USA, mentre IDEA non lo è in Europa.

Le limitazioni relative alla lunghezza delle chiavi sono codificate direttamente all'interno del software, che viene venduto nelle versioni per il mercato USA e internazionale, e perciò sono impossibili da eludere.

Una volta generate le chiavi si può far generare al server una richiesta di certificato, che viene spedita alla CA prescelta, la quale, generalmente entro alcuni giorni, invierà il certificato vero e proprio, pronto per essere inserito nel programma.

Una alternativa free

Per chi tuttavia desideri fare le cose in casa, è disponibile SSLeay, una implementazione libera, gratuita e completa di sorgenti, del protocollo SSL. SSLeay è disponibile per i principali sistemi operativi e non è un prodotto pensato esclusivamente per l'uso nel WWW, bensì una libreria di uso generico, libssl.a, che può essere utilizzata per rendere sicura qualunque connessione TCP/IP basata sui socket. Il prodotto inoltre contiene una libreria di funzioni generali (libcrypto.a) per la cifratura dei dati. Essa fornisce i metodi di codifica più diffusi, compresi quelli necessari per l'SSL (DES, RSA, RC4, IDEA, Blowfish), nonché alcune funzioni utili, come un'implementazione veloce del crypt usato per le password di sistema, oppure le routine necessarie per la codifica in base64 e per leggere file di configurazione nel formato .ini di Windows.

Oltre alle librerie vi sono i programmi che permettono di compiere, tramite interfaccia a linea di comando, le stesse operazioni precedentemente descritte per il server della Netscape: generazione delle chiavi, gestione delle stesse, richiesta e installazione del certificato.

Nel caso il client utilizzato lo consenta, esiste tutto il software necessario per divenire noi stessi delle CA, ad esempio in grado di fornire certificati ai diversi utenti della nostra Intranet aziendale.

Gli esempi di programmazione permettono infine di imparare velocemente come costruire le proprie applicazioni client/server sicure.

Applicazioni che fanno uso di SSLeay

Le seguenti applicazioni sono già disponibili pronte all'uso nel sito ftp ftp://ftp.psy.uq.oz.au/pub/Crypto/SSLapps/ :

* SSLtelnet: server e client telnet;
* SSLftp: server e client FTP;
* NCSA Mosaic;
* NCSA httpd;
* Apache;
* CERN httpd;
* Lynx.
* MSQL

La libreria SSL è utilizzata anche in alcuni prodotti commerciali, ad esempio nei server WWW Stronghold, Sioux e Roxen che abbiamo già incontrato.

Conclusioni

Mettere in piedi un sistema di commercio elettronico con Linux può sembrare a prima vista una operazione abbastanza semplice, in realtà il problema della sicurezza deve essere tenuto in seria considerazione. Tale scelta non deve però essere dettata solamente da considerazioni economiche (il presunto guadagno dovuto al basso costo del sistema operativo), bensì è necessario essere consapevoli che comunque c'è da effettuare un investimento importante, non solamente in termini di acquisto di software e di certificazioni, ma, soprattutto, come acquisizione di conoscenza riguardo alle problematiche connesse. Linux, al contrario di altre soluzioni, permette di capire come funziona realmente il sistema e ciò è un grande vantaggio, in quanto la coscienza dei pericoli, delle soluzioni proposte e dei limiti intrinseci in esse, è l'arma più importante per evitare in seguito problemi più grandi.

MC

FINALMENTE SPIEGATA LA FOTOGRAFIA DIGITALE

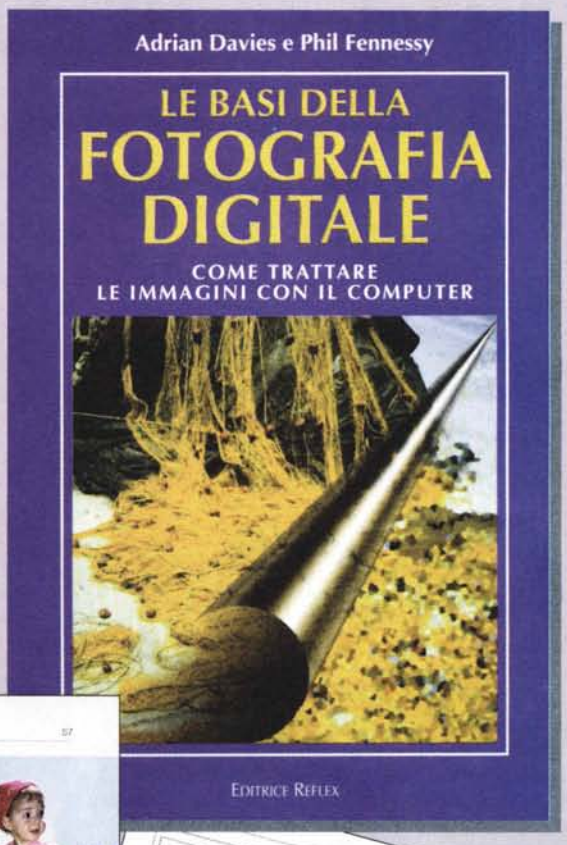
LE BASI DELLA FOTOGRAFIA DIGITALE

L'evoluzione digitale della fotografia fornirà ai fotografi professionisti e agli amatori appassionati di computer molte nuove opportunità. Questo libro spiega la tecnica degli strumenti (computer, scanner, stampa, trasmissione, ecc.) soffermandosi sul trattamento delle immagini con Photoshop: la camera oscura del 2000. Il testo è scritto con un linguaggio semplice ma esauriente e completo, mentre l'ampio glossario assicura che ogni termine sia perfettamente chiaro al lettore. Scritto da fotografi per i fotografi il libro descrive con precisione e chiarezza tutto quello che è necessario conoscere per orientarsi nel mondo della fotografia digitale. Un testo consigliato a tutti per risolvere i vostri dubbi sul fenomeno digitale.

LE BASI DELLA FOTOGRAFIA DIGITALE

~~***L. 36.000***~~ ***L. 25.000***

136 pagine, 15x21cm.



Alcune tecniche spiegate nel libro

IN VENDITA NEI MIGLIORI NEGOZI DI FOTOGRAFIA ED IN LIBRERIA

POTETE RICHIEDERE IL VOLUME DIRETTAMENTE ALLA EDITRICE REFLEX.
PAGAMENTO CON ASSEGNO BANCARIO OPPURE VERSANDO L'IMPORTO SUL CCP N. 82707001 INTESTATO A :
EDITRICE REFLEX, VIA DI VILLA SEVERINI 54, 00191 ROMA.
ORDINI TELEFONICI CON CARTA DI CREDITO, (AMERICAN EXPRESS o CARTA SI)
TEL. 06-36308595 - 36301756 FAX 06-3295648