Riservatezza e certificazione delle comunicazioni

44.1 Introduzione ai problemi legati alla crittografia e alla firma digitale

«

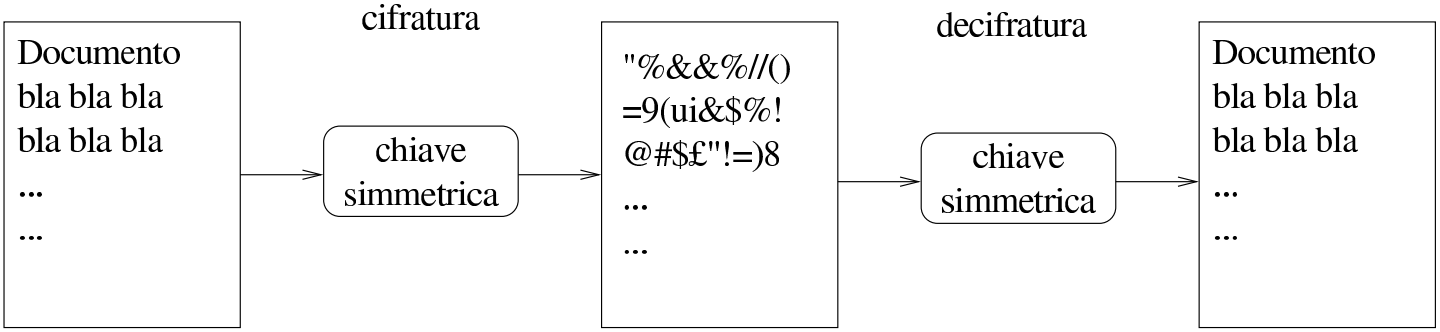
La comunicazione meccanica (elettronica) pone dei problemi legati alla riservatezza e alla facilità con cui questa può essere contraffatta. Per fare un esempio, un messaggio di posta elettronica può essere intercettato facilmente da parte di chiunque abbia un accesso privilegiato ai nodi di rete attraverso cui transita; nello stesso modo, un messaggio può essere manomesso, anche senza lasciare tracce apparenti. Per risolvere questi problemi si possono usare dei metodi di cifratura dei dati e per evitare contraffazioni si possono usare delle firme digitali[1].

44.1.1 Crittografia

La crittografia è una tecnica attraverso la quale si rendono illeggibili i dati originali, permettendo al destinatario di recuperarli attraverso un procedimento noto solo a lui. Si distinguono due forme fondamentali: la crittografia ***simmetrica***, ovvero ***a chiave segreta***, e quella ***asimmetrica***, nota meglio come crittografia ***a chiave pubblica***.

La crittografia simmetrica è quella più semplice da comprendere; si basa su un algoritmo che modifica i dati in base a una ***chiave*** (di solito una stringa di qualche tipo) che permette il ripristino dei dati originali soltanto conoscendo la stessa chiave usata per la cifratura. Per utilizzare una cifratura simmetrica, due persone si devono accordare sull'algoritmo da utilizzare e sulla chiave. La forza o la debolezza di questo sistema, si basa sulla difficoltà o meno che ci può essere nell'indovinare la chiave, tenendo conto anche della possibilità elaborative di cui può disporre chi intende spiare la comunicazione.

Figura 44.1. Crittografia simmetrica.

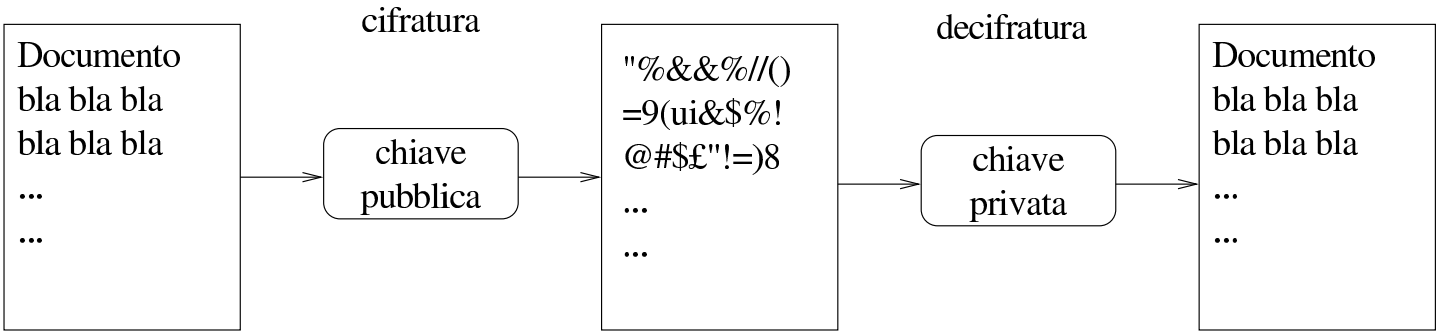


La crittografia a chiave pubblica è un metodo molto più complesso, ma ha il vantaggio di essere più pratico quando riguarda la comunicazione con molte persone. Il principio di funzionamento si basa sul fatto che esistono due chiavi complementari, assieme a un algoritmo in grado di cifrare con una chiave e di decifrare utilizzando l'altra. In pratica, la cifratura avviene a senso unico attraverso la chiave di cui

dispone il mittente di un messaggio, mentre questo può essere decifrato esclusivamente con l'altra che possiede solo il destinatario. Le due chiavi vengono chiamate ***chiave pubblica*** e ***chiave privata***, attribuendogli implicitamente un ruolo specifico. In pratica, chi vuole mettere in condizione i propri interlocutori di inviare dei messaggi, o altri dati cifrati, che nessun altro possa decifrare, deve costruire una propria coppia di chiavi e quindi distribuire la chiave pubblica. Chi vuole inviare informazioni cifrate, può usare la chiave pubblica diffusa dal destinatario, perché solo chi ha la chiave complementare, ovvero la chiave privata, può decifrarle. In questa situazione, evidentemente, **la chiave privata deve rimanere segreta a tutti**, tranne che al suo proprietario; se venisse trafugata permetterebbe di decifrare i messaggi che fossero eventualmente intercettati.

Per questa ragione, il proprietario di una coppia di chiavi asimmetriche deve essere la stessa persona che se le crea.

Figura 44.2. Crittografia a chiave pubblica.



La cifratura può anche essere ibrida, utilizzando in pratica entrambe le tecniche. Per attuarla, di solito si utilizza prima la cifratura simmetrica con una chiave determinata in modo casuale ogni volta: la ***chiave di sessione***. Questa chiave di sessione viene allegata al

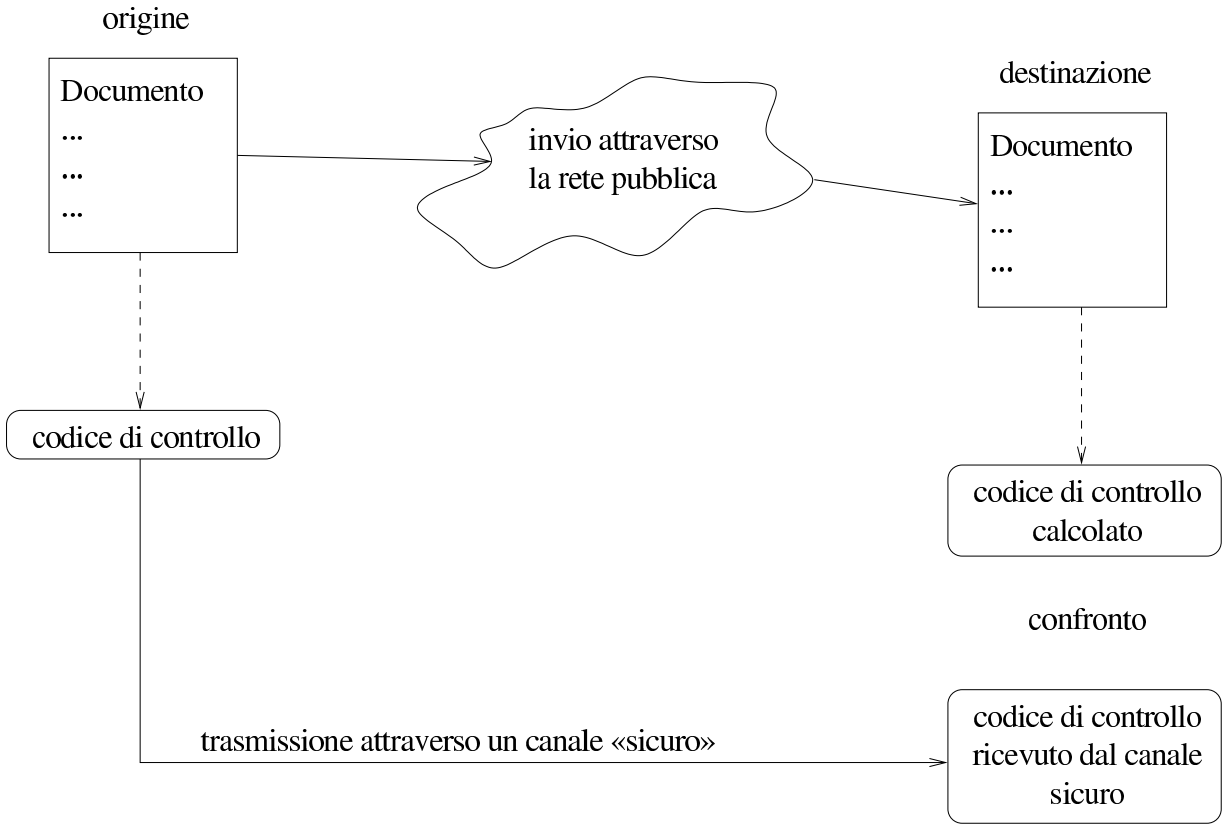
messaggio, o ai dati trasmessi, cifrandola a sua volta (eventualmente assieme agli stessi dati già cifrati) attraverso il sistema della chiave pubblica, ovvero quello che si basa sulla coppia di chiavi complementari. Il destinatario di questi dati deve fare il percorso inverso, decifrando il documento con la sua chiave privata, quindi decifrandolo nuovamente utilizzando la chiave di sessione che ha ottenuto dopo il primo passaggio.

44.1.2 Firma digitale

La firma digitale ha lo scopo di certificare l'autenticità dei dati. Per ottenere questo risultato occorre garantire che l'origine di questi sia autentica e che i dati non siano stati alterati.

Per dimostrare che un documento elettronico non è stato alterato, si utilizza la tecnica del codice di controllo, costituito da un numero o una stringa che si determinano in qualche modo in base al contenuto del documento stesso. L'algoritmo che genera questo codice di controllo è tanto più buono quanto è minore la probabilità che due documenti diversi generino lo stesso codice di controllo. Questo valore è una sorta di «riassunto» matematico del documento elettronico originale che può essere fornito a parte, attraverso un canale ritenuto sicuro, per permettere al destinatario di verificare che il documento è giunto intatto, ricalcolando il codice di controllo che deve risultare identico.[2]

Figura 44.3. Trasmissione di un documento abbinato a un codice di controllo separato.

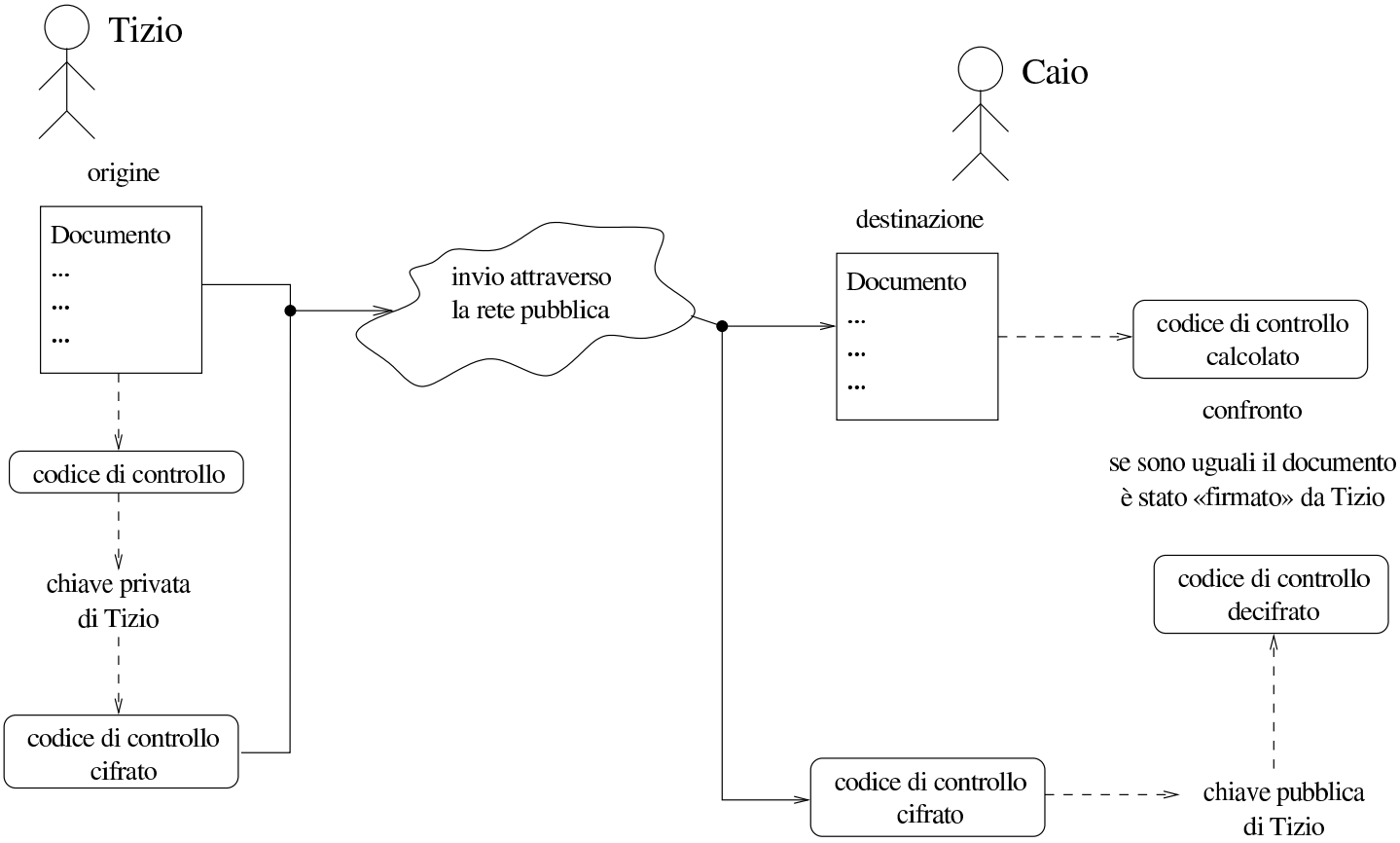


La firma digitale deve poter dimostrare che l'origine è autentica e che il codice di controllo non è stato alterato. Evidentemente, per non creare un circolo vizioso, serve qualcosa in più. Per questo si utilizza di solito la cifratura del codice di controllo assieme ai dati, oppure solo del codice di controllo, lasciando i dati in chiaro. Per la precisione, si utilizza la tecnica delle chiavi complementari, ma in questo caso, le cose funzionano in modo inverso, perché chi esegue la firma, deve usare la sua chiave privata (quella segreta), in maniera tale che tutti gli altri possano decifrare il codice di controllo attraverso la chiave pubblica.

Naturalmente, una firma digitale di questo tipo può essere verificata solo se si può essere certi che la chiave pubblica attribuita al mittente che ha firmato il documento, appartenga effettivamente a quella per-

sona. In altre parole, un impostore potrebbe diffondere una chiave pubblica corrispondente a una chiave privata di sua proprietà, indicandola come la chiave del signor Tizio, potendo così inviare documenti falsi a nome di questo signor Tizio, che in realtà non ne è il responsabile.

Figura 44.4. Principio di funzionamento della firma digitale applicata a un documento trasmesso in chiaro.



44.1.3 Gestione delle chiavi, certificazione e fiducia

I sistemi crittografici a chiave pubblica richiedono attenzione nell'uso di queste chiavi, in particolare è importante la gestione corretta delle chiavi pubbliche appartenenti ai propri corrispondenti. Queste chiavi sono conservate all'interno di «portachiavi», di solito distinti a seconda che si tratti di chiavi private o di chiavi pubbliche. Infat-

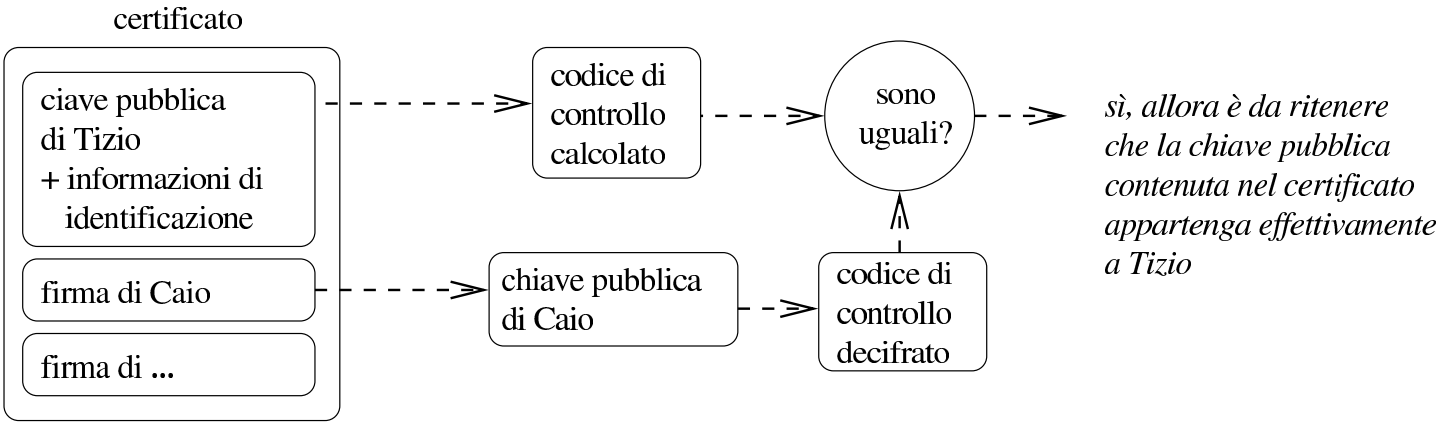
ti, la chiave privata deve rimanere segreta e va difesa in ogni modo, mentre le chiavi pubbliche non richiedono questa attenzione. I portachiavi in questione sono normalmente dei file, gestiti in modo più o meno automatico dai programmi che si utilizzano per queste cose.

A parte il problema di custodire gelosamente la propria chiave privata, bisogna considerare la necessità di verificare che le chiavi pubbliche appartengano effettivamente alle persone a cui sembrano essere attribuite, così si intuisce che il modo migliore per questo è quello di ottenere personalmente da loro le rispettive chiavi pubbliche.

Per semplificare un po' le cose, si introduce la possibilità di controfirmare le chiavi pubbliche che si ritiene siano di provenienza certa; questa firma ha il valore di una certificazione, che conta in funzione della credibilità di chi la dà. Le chiavi pubbliche firmate, portano con sé l'informazione di chi le ha firmate, ma la verifica della firma si può fare solo possedendo la chiave pubblica di questa persona. In pratica, il meccanismo della controfirma permette di creare una rete di fiducia, attraverso la diffusione di chiavi pubbliche firmate da altre persone: chi è sicuro della chiave pubblica di una persona, della quale ha anche fiducia, può decidere di fidarsi delle chiavi pubbliche che questa ha firmato a sua volta.

Una chiave pubblica contiene anche le informazioni che servono ad attribuirla al suo proprietario; di solito si tratta del nome e cognome, assieme a un indirizzo di posta elettronica. Per garantire che questi dati allegati non siano stati alterati, il proprietario delle sue stesse chiavi può firmare la sua chiave pubblica. Ciò serve a garantire che quella chiave pubblica è collegata correttamente a quei dati personali, anche se non può garantire che sia stata creata effettivamente da quella persona.

Figura 44.5. Verifica di un certificato, ovvero di una chiave pubblica controfirmata.



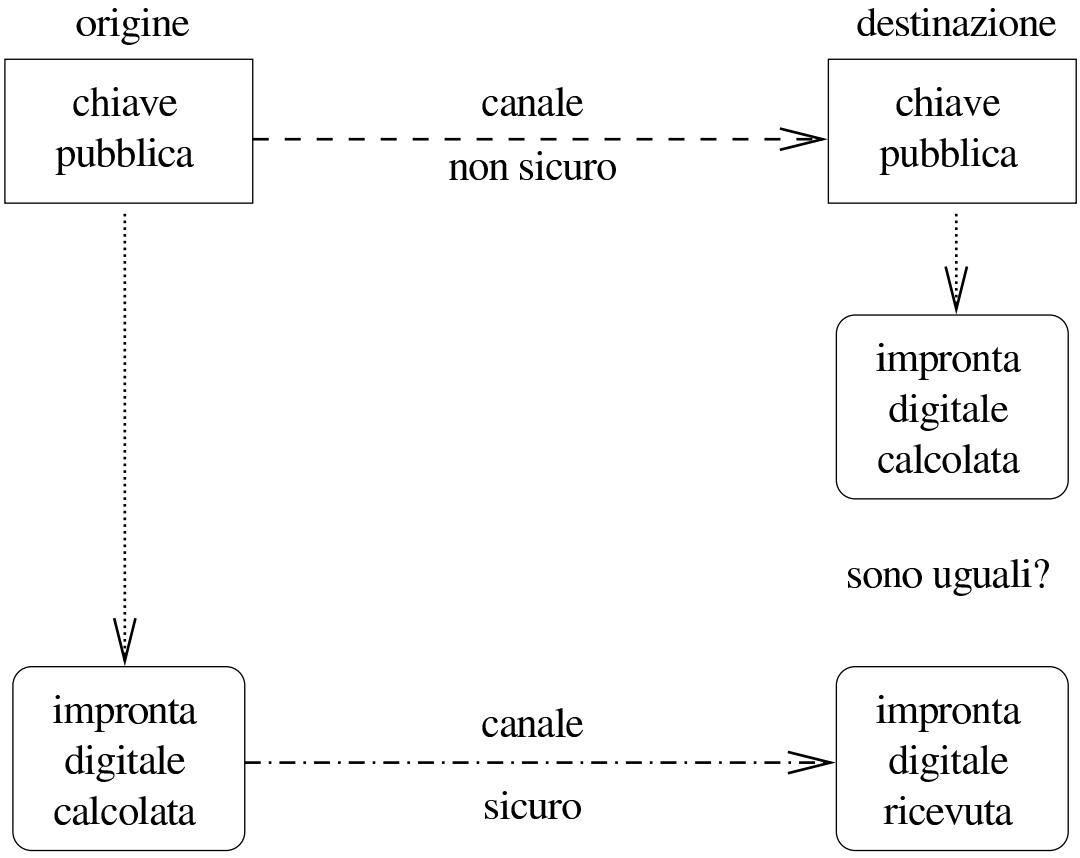
Quando l'uso dei sistemi crittografici a chiave pubblica diventa una pratica regolata attraverso le leggi, soprattutto per ciò che riguarda la firma digitale, diventa indispensabile l'istituzione di un'autorità in grado di garantire e verificare l'autenticità delle chiavi pubbliche di ognuno. Nello stesso modo, in mancanza di una tale istituzione, quando queste tecniche vengono usate per scopi professionali, diventa necessario affidarsi alla certificazione fatta da aziende specializzate in questo settore, che hanno la credibilità necessaria. Tecnicamente si parla di ***autorità di certificazione*** e nella documentazione tecnica inglese si indica con l'acronimo «CA»: *Certificate authority*.

È l'autorità di certificazione che stabilisce quali siano i dati di identificazione che devono accompagnare la chiave nel certificato che si vuole ottenere.

Anche in presenza di un'autorità di certificazione delle chiavi, la coppia di chiavi asimmetriche dovrebbe essere creata esclusivamente dal suo titolare (il suo proprietario), che solo così potrebbe essere effettivamente l'unico responsabile della segretezza della sua chiave privata.

Tornando alle situazioni pratiche, la verifica di una chiave pubblica può essere semplificata attraverso l'uso di un'***impronta digitale***. Si tratta di un altro codice di controllo calcolato su una chiave pubblica, con la proprietà di essere ragionevolmente breve, tanto da poter essere scambiato anche su un foglio di carta. Quando due persone vogliono scambiarsi le chiavi pubbliche personalmente, al posto di farlo realmente, possono limitarsi a scambiarsi l'impronta digitale della chiave, in modo da poter poi verificare che la chiave pubblica avuta attraverso i canali normali corrisponde effettivamente a quella giusta.

Figura 44.6. Impronta digitale della chiave pubblica.



Data l'importanza che ha la segretezza della chiave privata, è normale che i sistemi crittografici prevedano la protezione di questa informazione attraverso una parola d'ordine. In generale, viene data la facoltà di lasciare la chiave privata in chiaro, o di cifrarla attraverso una stringa, la parola d'ordine, che in questo contesto particolare è conosciuta meglio come *passphrase*. L'utilizzo di una chiave privata cifrata si traduce in pratica nella necessità, ogni volta che serve, di inserire il testo utilizzato per cifrarla. L'utilizzo di chiavi private protette in questo modo, è indispensabile in un sistema multiutente, in cui l'amministratore di turno può avere accesso a tutto quello che vuole nel file system; dall'altra parte, in questo modo si riduce il pericolo che qualcun altro possa usare una chiave privata trafugata.

Dovrebbe essere chiaro, ormai, che il file contenente la chiave pub-

blica e i dati identificativi del suo titolare, assieme a una o più firme di certificazione, è un ***certificato***. Come nei certificati normali, quando le informazioni che vengono attestate in questo modo non sono definitive per loro natura (si pensi all'indirizzo di posta elettronica che può cambiare anche molto spesso), è importante prevedere una scadenza tra i dati che compongono il certificato stesso. Oltre a questo, ci deve essere la possibilità di revocare un certificato prima della sua scadenza normale: sia per la possibilità che i dati relativi siano cambiati, sia per premunirsi in caso di furto della chiave privata. La revoca di un certificato si ottiene attraverso un ***certificato di revoca***. A seconda del sistema crittografico che si utilizza, il certificato di revoca può essere predisposto dalla stessa persona che si costruisce le chiavi, oppure può essere compito dell'autorità di certificazione che si occupa di rilasciare i certificati. Il problema viene ripreso più avanti.

44.1.4 Cosa può succedere se...

«

È il caso di soffermarsi sul significato pratico di alcune cose che possono succedere, in modo da capire meglio l'importanza di certi aspetti che riguardano la crittografia a chiave pubblica.

Se si perde la chiave privata, non si possono più decifrare i messaggi ricevuti dagli interlocutori, quando questi li hanno cifrati con la chiave pubblica relativa; inoltre non si possono decifrare più nemmeno quelli che sono stati ricevuti in passato.

Se qualcuno ruba una copia della chiave privata,[3] questa persona può leggere i messaggi cifrati inviati al proprietario di quella chiave e può sostituirsi a quella persona in generale; può anche firmare a suo nome.

L'unica cosa che si può fare quando si perde la chiave privata, o si sospetta che qualcuno sia riuscito a ottenerne una copia, è la diffusione del certificato di revoca.

Se si utilizza una chiave pubblica senza averla verificata, si rischia di far recapitare il messaggio o i dati a una persona diversa da quella che si intende veramente. Infatti, un estraneo potrebbe intercettare sistematicamente le comunicazioni della persona a cui si vuole scrivere o inviare altri dati. In tal modo, questo estraneo riceverebbe dei messaggi che può decifrare con la sua chiave privata, provvedendo poi a cifrarli nuovamente nel modo giusto per inviarli al destinatario reale, in modo che nessuno si accorga dell'intercettazione.

44.1.5 Servizi per la diffusione delle chiavi pubbliche

Ci possono essere molti modi di diffondere la propria chiave pubblica, oppure quella di altri, dopo che questa è stata controfirmata. Il metodo standard dovrebbe consistere nell'utilizzo di un servente specifico per questo. Normalmente, questi serventi di chiavi (*key-server* o *cert-server*) sono collegati tra loro in modo da aggiornarsi a vicenda, limitandosi comunque ad accumulare le chiavi pubbliche che vengono inviate, senza certificare implicitamente la genuinità di queste. Per prelevare una chiave pubblica occorre conoscere il numero di identificazione di questa (si tratta di un numero attribuito automaticamente dal programma che crea la coppia di chiavi), tenendo conto che tale informazione può essere ottenuta dalla stessa persona con la quale si vuole comunicare in modo cifrato, magari perché la aggiunge sistematicamente in coda ai suoi messaggi di posta elettronica.

Nel caso della crittografia usata per la posta elettronica si utilizza generalmente lo standard OpenPGP, con il quale, per accedere ai serventi di chiavi non si usano i protocolli normali e occorre affidarsi direttamente agli strumenti di gestione della crittografia e delle firme. Il servente a cui si fa riferimento di solito è *certserver.pgp.com*, comunque non è necessario servirsi proprio di questo. Tenendo conto che di solito i nomi dei nodi che offrono questo tipo di servizio corrispondono a un modello del tipo ∗*.pgp.net*, ∗*.pgp.org*, oppure ∗*.pgp.com*, o simili, si potrebbe fare una ricerca attraverso un motore di ricerca comune.

44.1.6 Problemi legali

«

L'utilizzo di sistemi di comunicazione cifrata potrebbe essere regolato dalle leggi dei paesi coinvolti. Il problema è che bisogna verificare le norme del paese di origine di una trasmissione del genere e anche quelle del paese di destinazione. Per quanto riguarda l'Italia, la cosa non è chiara.[4]

Questo serve per ricordare che si tratta di una materia delicata; anche se si ritiene di poter utilizzare la crittografia in Italia, bisogna pensarci bene prima di inviare messaggi cifrati all'estero, o di usare altre forme di comunicazione cifrate. Il problema si può porre anche nell'ambito della stessa Unione Europea.

44.2 GnuPG: GNU Privacy Guard

«

GnuPG[5] è uno strumento per la gestione della crittografia e delle firme digitali, compatibile con le specifiche OpenPGP pubblicate nell'RFC 2440. Rispetto al noto PGP, si tratta di software libero e in particolare non vengono utilizzati algoritmi proprietari.

GnuPG è composto da due eseguibili: '**gpg**' e '**gpgm**'. Di solito, il secondo viene richiamato dal primo, in base alle necessità, senza che ci sia bisogno di utilizzarlo direttamente. La distinzione in due eseguibili serve a trattare in modo particolare le operazioni delicate dal punto di vista della sicurezza, rispetto a quelle che non hanno questo problema: nel primo caso si deve fare uso di memoria «sicura». Tra le altre cose, da questo problema legato alla memoria dipende la limitazione pratica nella dimensione delle chiavi che si possono gestire.

Una volta chiarito che basta utilizzare solo l'eseguibile '**gpg**', perché questo si avvale di '**gpgm**' quando necessario, occorre vedere come sono organizzati gli argomenti nella sua riga di comando:

```
gpg [opzioni] comando [argomenti_del_comando]
```

In pratica, si utilizza '**gpg**' esattamente con l'indicazione di un comando. Il funzionamento generale può essere definito attraverso le opzioni che precedono tale comando, mentre il comando stesso potrebbe richiedere l'indicazione di altri argomenti.[6]

Le opzioni «lunghe», cioè quelle che andrebbero indicate con due trattini iniziali, possono essere inserite in un file di configurazione, avendo però l'accortezza di eliminare i due trattini. Il file di configurazione di GnuPG è sempre solo personale, il nome predefinito è '`~/.gnupg/options`' e di solito viene creato automaticamente la prima volta che si usa il programma (assieme alla directory che lo precede). Come in molti altri tipi di file del genere, il carattere '**#**' viene utilizzato per iniziare un commento, mentre le righe bianche e quelle vuote vengono ignorate nello stesso modo. In particolare, ne-

gli esempi che vengono mostrati successivamente, si fa riferimento alla situazione tipica, in cui non viene modificato il file di configurazione creato automaticamente e tutto quello che serve deve essere definito attraverso la riga di comando.

Come si può intuire, la directory '`~/.gnupg/`' serve anche per contenere altri file relativi al funzionamento di GnuPG, tenendo conto, comunque, che in condizioni normali viene creata la prima volta che si avvia l'eseguibile '**`gpg`**'. I file più importanti che si possono trovare sono: '`~/.gnupg/secring.gpg`' che rappresenta il portachiavi delle chiavi private (file che deve essere custodito e protetto con cura); '`~/.gnupg/pubring.gpg`' che rappresenta il portachiavi delle chiavi pubbliche (ovvero dei certificati); '`~/.gnupg/trustdb.gpg`' che contiene le informazioni sulla propria fiducia nei confronti di altre persone, le quali possono avere firmato (certificato) le chiavi pubbliche di altri.

Una volta creata la propria coppia di chiavi, occorre decidere la politica di sicurezza da utilizzare per proteggere il portachiavi privato. Oltre alla necessità di farne delle copie da conservare in un luogo sicuro, si può considerare la possibilità di mettere questo file in un altro luogo; per esempio in un disco rimovibile, da inserire solo quando si deve usare la propria chiave privata. In questo caso, si potrebbe sostituire il file '`~/.gnupg/secring.gpg`' con un collegamento simbolico al file reale in un altro disco innestato solo per l'occasione.

Ogni volta che c'è bisogno di accedere a questi file, viene creato un file lucchetto, con lo stesso nome del file a cui si riferisce e l'aggiun-

ta dell'estensione '`.lock`'. Alle volte, se si interrompe il funzionamento dell'eseguibile '**gpg**', possono rimanere questi file, i quali poi impediscono di accedere ai dati. Se ciò accade, viene segnalato dal programma, il quale indica anche il numero che dovrebbe avere il processo che li ha bloccati: se questo processo non c'è, vuol dire che i file lucchetto possono essere rimossi.

Nelle sezioni successive, viene mostrato il funzionamento di GnuPG, attraverso l'eseguibile '**gpg**', mostrando l'interazione con questo quando si fa riferimento a una localizzazione di lingua inglese. Se si utilizza un sistema configurato correttamente per quanto riguarda proprio la localizzazione, si ottengono i messaggi in italiano (quelli che sono stati tradotti), ma in italiano vanno date anche le risposte. In particolare, quando una domanda prevede che si risponda con un «sì», oppure un «no», si devono usare le iniziali, «s» o «n», anche se per qualche motivo la domanda è rimasta in inglese perché manca quella traduzione particolare.

44.2.1 Creazione delle chiavi e del certificato di revoca

La creazione di una coppia di chiavi è un'operazione molto semplice. Quello che occorre considerare prima è il modo in cui viene gestito il file che rappresenta il portachiavi privato, come è già stato descritto. In particolare, occorre considerare subito la possibilità di creare un certificato di revoca.

Si comincia con la creazione di una coppia di chiavi, utilizzando il comando '**--gen-key**'. Se non sono stati creati in precedenza, viene predisposta la directory '`~/.gnupg/`' con i vari portachiavi.

```
tizio$ gpg --gen-key [Invio]

  Please select what kind of key you want:
     (1) DSA and ElGamal (default)
     (2) DSA (sign only)
     (4) ElGamal (sign and encrypt)
```

A questo punto inizia una serie di richieste con le quali si devono stabilire le caratteristiche delle chiavi che si creano. Per vari motivi, è conveniente affidarsi alle scelte predefinite, a meno di avere le idee chiare al riguardo.

```
Your selection? 1 [Invio]

  DSA keypair will have 1024 bits.
  About to generate a new ELG-E keypair.
                minimum keysize is  768 bits
                default keysize is 1024 bits
      highest suggested keysize is 2048 bits

What keysize do you want? (1024) [Invio]

  Please specify how long the key should be valid.
           0 = key does not expire
         <n>  = key expires in n days
         <n>w = key expires in n weeks
         <n>m = key expires in n months
         <n>y = key expires in n years
```

Questo può essere un punto delicato. Di solito si crea una coppia di chiavi che non scadono mai, ma per motivi di sicurezza si potrebbe stabilire una scadenza. Ribadendo che in condizioni normali si crea una coppia di chiavi senza scadenza, negli esempi si mostra la creazione di una chiave che scade alla fine di una settimana.

```
Key is valid for? (0) 1w [Invio]
```

```
  Key expires at Fri Oct  8 10:55:43 1999 CEST

Is this correct (y/n)? y[Invio]
```

Per completare questa fase occorre indicare i dati personali che vengono uniti alle chiavi, in modo da facilitarne il riconoscimento.

```
  You need a User-ID to identify your key; the software
  constructs the user id from Real Name, Comment and Email
  Address in this form:
     "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
```

Come si vede, si tratta di indicare il proprio nome e cognome, quindi viene richiesto un indirizzo di posta elettronica, infine viene proposta la possibilità di mettere una nota, costituita da un nomignolo o qualunque altra cosa che possa aiutare a individuare il proprietario della chiave.

```
Real name: Tizio Tizi[Invio]

Email address: tizio@dinkel.brot.dg[Invio]

Comment: Baffo[Invio]

  You selected this USER-ID:
      "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"
```

Il programma mostra i dati inseriti, permettendo di controllarli. Se tutto è in ordine, si conferma.

```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O[Invio]
```

Infine, la cosa più importante: per proteggere la chiave privata, questa viene cifrata utilizzando una parola d'ordine, definita in questo caso *passphrase*, per intendere che si dovrebbe trattare di un testo

più lungo di una sola parola. In pratica, si deve inserire una stringa, possibilmente lunga e complicata, che serve per cifrare la chiave privata; di conseguenza, ogni volta che si deve utilizzare la chiave privata, viene richiesto l'inserimento di questa stringa per potervi accedere.

```
  You need a Passphrase to protect your secret key.

Enter passphrase: digitazione_all'oscuro [Invio]

Repeat passphrase: digitazione_all'oscuro [Invio]
```

Completata questa fase, inizia la procedura di creazione delle chiavi, che avviene in modo automatico.

```
  We need to generate a lot of random bytes. It is a good idea
  to perform some other action (work in another window, move
  the mouse, utilize the network and the disks) during the
  prime generation; this gives the random number generator a
  better chance to gain enough entropy.
  ....+++++.............+++++..+++++.+++++.............+++++..
  ..+++++++++.......+++++..+++++.......+++++++++...........
  ............+++++.+++++.+++++...+++++.......+++++...+++++..
  +++++++..+++++++++++++++.+++++.....+++++.+++++>.....+++++>.
  ++++.<.+++++...........>........++++....<+++++...>.....++.
  +.............................+++++^^^
  public and secret key created and signed.
```

Questo conclude il funzionamento del programma e riappare l'invito della shell. Leggendo il messaggio finale, si osserva che le chiavi sono state firmate. Questa firma garantisce solo che non siano alterate le informazioni abbinate alle chiavi, ma come è già spiegato nella sezione 44.1, ciò non impedisce che qualcuno possa sostituire

completamente le chiavi pubbliche che vengono diffuse.

Una volta creata la propria coppia di chiavi, è importantissimo provvedere a generare anche il certificato di revoca relativo. Questo si traduce in un file di testo da conservare in un posto sicuro. Eventualmente, si può anche stampare il file, per una maggiore sicurezza.

```
tizio$ gpg --output revoca.txt ↩
↪          --gen-revoke tizio@dinkel.brot.dg[Invio]

  sec  1024D/7A6D2F72 1999-10-01   Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>
```

Come si vede, vengono mostrati tutti i dati identificativi della chiave, compreso il numero che è stato generato automaticamente. Per proseguire basta confermare.

```
Create a revocation certificate for this key? y[Invio]
```

Dal momento che questa operazione richiede l'utilizzo della chiave privata, occorre indicare la stringa necessaria per sbloccarla.

```
  You need a passphrase to unlock the secret key for
  user: "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"
  1024-bit DSA key, ID 7A6D2F72, created 1999-10-01

Enter passphrase: digitazione_all'oscuro [Invio]
```

```
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if
Mallory gets access to this certificate he can use it to
make your key unusable.
It is smart to print this certificate and store it away,
just in case your media become unreadable.  But have some
caution:  The print system of your machine might store the
data and make it available to others!
```

E con questo si conclude l'operazione che ha generato il file 'revoca.txt'. Il file è di tipo ASCII, ovvero, da binario è stato convertito in ASCII attraverso l'algoritmo Armor. Vale la pena di vedere come potrebbe essere questo file:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v0.9.3 (GNU/Linux)
Comment: For info see http://www.gnupg.org
Comment: A revocation certificate should follow

iEYEIBECAAYFAjf0gEIACgkQZUnKKXptL3KOAQCdEH5HfbFR5g34fui5y0JMkQxr
PisAn2kHENgFOLtkdDIpK1PwYp9ZArbK
=HGaY
-----END PGP PUBLIC KEY BLOCK-----
```

44.2.2 Scambio di chiavi pubbliche

«

Quando si vuole intrattenere una comunicazione cifrata con qualcuno, si deve disporre della chiave pubblica dell'interlocutore, il quale a sua volta deve disporre di quella della controparte. Di conseguenza, è necessario apprendere subito come si accede al proprio portachiavi, in modo da poter estrarre le chiavi pubbliche (proprie o di altri) e per potervi aggiungere le chiavi delle persone con cui si vogliono

avere contatti in questa forma. Inizialmente, le chiavi pubbliche a disposizione sono solo le proprie; se ne ottiene l'elenco con il comando seguente:

```
tizio$ gpg --list-keys[Invio]

  /home/tizio/.gnupg/pubring.gpg
  ------------------------------
  pub  1024D/7A6D2F72 1999-10-01 Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>
  sub  1024g/D75594A6 1999-10-01
```

Anche se non è stato richiesto esplicitamente, nella creazione della coppia di chiavi complementari, in realtà sono state generate due coppie: una primaria e una secondaria. Si può osservare che la prima colonna suggerisce di che tipo di chiave si tratti: '**pub**' per indicare la chiave pubblica primaria e '**sub**' per indicare la chiave pubblica secondaria.

A questo punto si pone il problema di esportare la propria chiave pubblica (intesa come il complesso rappresentato dalla chiave primaria e da tutte le sue chiavi secondarie) e di importare quella degli interlocutori futuri. In particolare, nel momento in cui si esporta una chiave, occorre decidere se questo debba essere fatto generando un risultato binario, oppure se lo si voglia convertire in ASCII. In generale, dovendo preparare un file da trasmettere attraverso forme di comunicazione tradizionale, come la posta elettronica, conviene richiedere sempre la conversione in ASCII, per mezzo dell'opzione '**--armor**'. Si comincia mostrando l'esportazione.

```
tizio$ gpg --armor --output tizio.gpg ↩
↪          --export tizio@dinkel.brot.dg[Invio]
```

Il file che si ottiene, 'tizio.gpg', potrebbe essere simile a quello seguente (che viene mostrato solo in parte):

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v0.9.3 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDf0ehMRBAC+s8Evv4EXv1eEGDw01mZAwJCPe9uBbE/u9eNlD8J33MCXFRUK
k/4CFU6BRK46RlXFjL9CcWtRIDar/72NIktChpBFebYnX+wiho9Pt2/U7B32MbMX
…
…
vO+Y8kqiOfAHDrL90IhMBBgRAgAMBQI39HpKBQkACTqAAAoJEGVJyil6bS9y0ywA
n3OySw4T4rHtGtE2hULTwj9orwefAKCB3ozbH0x/I9jFrCGe6gx7Fio9FA==
=jTTe
-----END PGP PUBLIC KEY BLOCK-----
```

L'importazione di una chiave pubblica avviene in modo analogo, con la differenza che non è necessario specificare in che formato sia la fonte: ciò viene determinato automaticamente. Si suppone di importare una chiave contenuta nel file '`caio.gpg`'.

```
tizio$ gpg --import caio.gpg[Invio]

  gpg:/home/tizio/caio.gpg: key C38563D0: public key imported
  gpg: Total number processed: 1
  gpg:               imported: 1
```

Dopo l'importazione si può controllare l'elenco delle chiavi pubbliche possedute, come è già stato fatto in precedenza.

```
tizio$ gpg --list-keys[Invio]

  /home/tizio/.gnupg/pubring.gpg
  ------------------------------
  pub  1024D/7A6D2F72 1999-10-01 Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>
  sub  1024g/D75594A6 1999-10-01

  pub  1024D/C38563D0 1999-10-01 Caio Cai <caio@roggen.brot.dg>
  sub  1024g/E3460DB4 1999-10-01
```

È da osservare il fatto che l'esportazione delle chiavi pubbliche, senza indicare a quali persone si vuole fare riferimento, implica l'esportazione completa di tutte le chiavi disponibili.

A questo punto, occorre stabilire se ci si fida o meno delle chiavi pubbliche che si importano. Se si è certi della loro autenticità, è utile controfirmarle. La firma che si aggiunge può servire a qualcun altro, se poi si provvede a diffonderle nuovamente. Per intervenire a questo livello nel portachiavi pubblico, occorre usare il comando '**`--edit-key`**':

```
tizio$ gpg --edit-key caio@roggen.brot.dg [Invio]
```

Con questo comando si richiede di intervenire nella chiave pubblica di Caio. Si ottiene un riassunto della situazione e un invito a inserire dei comandi specifici (attraverso una riga di comando).

```
pub  1024D/C38563D0  created: 1999-10-01 expires: 1999-10-08 trust: -/q
sub  1024g/E3460DB4  created: 1999-10-01 expires: 1999-10-08
(1)  Caio Cai <caio@roggen.brot.dg>
```

Una chiave potrebbe contenere più informazioni riferite all'identità del suo proprietario. Anche se si tratta sempre della stessa persona, questa potrebbe utilizzare diversi indirizzi di posta elettronica e diverse variazioni nel nome (per esempio per la presenza o meno del titolo o di un nomignolo). Nel caso mostrato dall'esempio, si tratta di un nominativo soltanto, a cui è abbinato il numero uno.

Tanto per cominciare, si può controllare lo stato di questa chiave con il comando '**`check`**':

```
Command> check [Invio]
```

```
uid  Caio Cai <caio@roggen.brot.dg>
sig!       C38563D0 1999-10-01   [self-signature]
```

Si può osservare che dispone soltanto della firma del suo stesso proprietario, cosa che non può garantirne l'autenticità. Di solito, per verificare l'origine di una chiave pubblica si sfrutta la sua impronta digitale, ovvero un codice più breve che viene generato univocamente attraverso una funzione apposita:

```
Command> fpr[Invio]
```

Con il comando '**fpr**' si ottiene proprio questa informazione. Se il proprietario di questa chiave ci ha fornito l'impronta digitale attraverso un canale sicuro (di solito ciò significa che c'è stato un incontro personale), si può controllare a vista la sua corrispondenza.

```
pub  1024D/C38563D0 1999-10-01 Caio Cai <caio@roggen.brot.dg>
       Fingerprint: 8153 E6E4 DE1F 6B62 2847  0B5D 9643 B918 C385 63D0
```

Se l'impronta corrisponde e si è finalmente certi dell'autenticità di questa chiave, la si può firmare, certificando a proprio nome che si tratta di una chiave autentica.

```
Command> sign[Invio]
```

```
pub  1024D/C38563D0  created: 1999-10-01 expires: 1999-10-08 trust: -/q
       Fingerprint: 8153 E6E4 DE1F 6B62 2847  0B5D 9643 B918 C385 63D0

     Caio Cai <caio@roggen.brot.dg>

Are you really sure that you want to sign this key
with your key: "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"

Really sign? y[Invio]
```

Dal momento che per farlo occorre utilizzare la propria chiave pri-

vata, ecco che viene richiesto di inserire la stringa necessaria per sbloccarla.

```
You need a passphrase to unlock the secret key for
user: "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"
1024-bit DSA key, ID 7A6D2F72, created 1999-10-01
```

```
Enter passphrase: digitazione_all'oscuro [Invio]
```

A questo punto si può verificare nuovamente lo stato della chiave:

```
Command> check [Invio]
```

```
uid  Caio Cai <caio@roggen.brot.dg>
sig!       C38563D0 1999-10-01   [self-signature]
sig!       7A6D2F72 1999-10-01   Tizio Tizi (Baffo) <tizio@dinkel.brot.dg
```

Come si vede, adesso c'è anche la firma di Tizio. Per concludere questo funzionamento interattivo, si utilizza il comando '**quit**', ma prima si salvano le modifiche con '**save**':

```
Command> save [Invio]
```

```
Command> quit [Invio]
```

44.2.3 Utilizzo della crittografia

Quando si dispone della chiave pubblica del proprio interlocutore, è possibile cifrare i dati che gli si vogliono mandare. In generale, si lavora su un file alla volta, o eventualmente su un archivio compresso contenente più file. Supponendo di volere inviare il file 'documento.txt' a Caio, si potrebbe preparare una versione cifrata di questo file con il comando seguente:

```
tizio$ gpg --output documento.txt.gpg --encrypt ↩
↪          --recipient caio@roggen.brot.dg documento.txt [Invio]
```

In questo modo si ottiene il file ‘`documento.txt.gpg`’. Se questo file viene spedito attraverso la posta elettronica, allegandolo a un messaggio, di solito, il programma che si usa si arrangia a convertirlo in un formato adatto a questa trasmissione; diversamente, può essere conveniente la conversione in formato Armor. Nell’esempio seguente si fa tutto in un colpo solo: si cifra il messaggio e lo si spedisce a Caio (si osservi il trasferimento del messaggio cifrato attraverso lo standard output.)

```
tizio$ gpg --armor --output - --encrypt --recipient ↩
↪          caio@roggen.brot.dg documento.txt ↩
↪      | mail caio@roggen.brot.dg[Invio]
```

Eventualmente si può specificare in modo esplicito l’algoritmo da usare per cifrare. Si ottiene questo con l’opzione ‘**`--cipher-algo`**’, ma prima occorre conoscere gli algoritmi a disposizione:

```
tizio$ gpg --version[Invio]

  Home: ~/.gnupg
  Supported algorithms:
  Cipher: 3DES, CAST5, BLOWFISH, RIJNDAEL, RIJNDAEL192, RIJNDAEL256, TWOFISH
  Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA, ELG
  Hash: MD5, SHA1, RIPEMD160
```

Si possono usare i nomi elencati per la cifratura; per esempio, volendo usare l’algoritmo 3DES:

```
tizio$ gpg --output documento.txt.gpg --encrypt ↩
↪          --cipher-algo 3DES ↩
↪          --recipient caio@roggen.brot.dg ↩
↪          documento.txt[Invio]
```

Per decifrare un documento si agisce in modo simile, utilizzando l’opzione ‘**`--decrypt`**’. A differenza dell’operazione di cifratura, dovendo usare la chiave privata, viene richiesta l’indicazione della

stringa necessaria per sbloccarla. L'esempio che segue, mostra il caso in cui si voglia decifrare il contenuto del file '`messaggio.gpg`', generando il file '`messaggio`':

```
tizio$ gpg --output messaggio --decrypt messaggio.gpg[Invio]

  You need a passphrase to unlock the secret key for
  user: "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"
  1024-bit DSA key, ID 7A6D2F72, created 1999-10-01

Enter passphrase: digitazione_all'oscuro [Invio]
```

Per finire, è il caso di considerare anche la possibilità di usare un sistema di crittografia simmetrica (a chiave segreta), dove non viene presa in considerazione la gestione delle chiavi pubbliche o private che siano. In pratica, tutto si riduce a definire la chiave da usare per la cifratura, chiave che deve essere conosciuta anche dalla controparte per poter decifrare il messaggio.

```
tizio$ gpg --armor --output testo.gpg --symmetric testo[Invio]
```

L'esempio mostra il caso del file '`testo`' che viene cifrato generando il file '`testo.gpg`', in formato ASCII Armor. Per completare l'operazione, occorre fornire la stringa da usare come chiave per la cifratura; per ridurre la possibilità di errori, ciò viene richiesto per due volte:

```
Enter passphrase: digitazione_all'oscuro [Invio]

Repeat passphrase: digitazione_all'oscuro [Invio]
```

Per decifrare questo file, non occorrono comandi speciali, basta l'opzione '**`--decrypt`**'. GnuPG si accorge da solo che si tratta di una cifratura simmetrica, provvedendo a chiedere l'indicazione della

stringa necessaria a decifrarla.

44.2.4 Firma di documenti

La firma digitale serve a certificare l'autenticità e la data di un file. Se il file in questione viene modificato in qualche modo, la verifica della firma fallisce. La firma viene generata utilizzando la chiave privata e di conseguenza può essere verificata utilizzando la chiave pubblica; il controllo ha valore solo se si può dimostrare l'autenticità della chiave pubblica. In generale, la firma viene allegata allo stesso file, che di solito viene cifrato, sempre usando la chiave privata.

```
tizio$ gpg --armor --output documento.firmato ↩
↪          --sign documento [Invio]
```

L'esempio mostra in che modo si può firmare il file 'documento', generando 'documento.firmato' (in particolare si vuole ottenere un file ASCII per facilitarne la trasmissione).

```
You need a passphrase to unlock the secret key for
user: "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"
1024-bit DSA key, ID 7A6D2F72, created 1999-10-01
```

Dal momento che si deve usare la chiave privata per ottenere la firma e anche per cifrare il testo, viene richiesto di inserire la stringa necessaria per sbloccarla.

```
Enter passphrase: digitazione_all'oscuro [Invio]
```

Un documento firmato si controlla semplicemente con l'opzione '**--verify**', come nell'esempio seguente:

```
tizio$ gpg --verify documento.firmato [Invio]
```

```
gpg: Signature made Fri Oct  1 15:56:15 1999 CEST using DSA key ID 7A6D2F72
gpg: Good signature from "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"
```

Dal momento che il documento, così come si trova non è leggibile, occorre richiedere di decifrarlo, cosa che implica anche la verifica della firma:

```
tizio$ gpg --output documento ↩
↪          --decrypt documento.firmato[Invio]
```

In questo caso si ottengono le stesse informazioni di prima, ma in più si ha di nuovo il file ‘documento’ originale.

```
gpg: Signature made Fri Oct  1 15:56:15 1999 CEST
     using DSA key ID 7A6D2F72
gpg: Good signature from
     "Tizio Tizi (Baffo) <tizio@dinkel.brot.dg>"
```

Dal momento che lo scopo della firma non è quello di nascondere il contenuto del file originale, specialmente se si tratta di un file di testo, si può richiedere esplicitamente di firmare un file in chiaro. In pratica, si ottiene il file di partenza, con l’aggiunta della firma. Per questo si usa il comando ‘**--clearsign**’ al posto di ‘**--sign**’:

```
tizio$ gpg --output documento.firmato ↩
↪          --clearsign documento[Invio]
```

Tutto il resto funziona come prima. L’aspetto di un file del genere è simile a quello seguente:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

…
…
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v0.9.3 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iD8DBQE39L/LrL80KSMdTVQRAgUfAJ9tVPiBLuJNpElEF9fpoUO27odWMQCfc8e7
3c6ARR8UGBAO7TIhVlDn7fE=
=amzF
-----END PGP SIGNATURE-----
```

Infine, se può essere opportuno per qualche motivo, la firma si può tenere staccata dal file originale. In questo caso, si utilizza il comando '**`--detach-sig`**':

```
tizio$ gpg --armor --output firma --detach-sig documento [Invio]
```

In questo modo si crea la firma del file '`documento`', inserendola separatamente nel file '`firma`', richiedendo espressamente di utilizzare la codifica ASCII Armor. Per verificare la firma, occorre indicare i due nomi:

```
tizio$ gpg --verify firma documento [Invio]
```

44.2.5 Gestione della fiducia

«

GnuPG permette di annotare il livello di fiducia che si ha nei confronti della certificazione da parte di altre persone. Una volta definiti questi valori, si può automatizzare il calcolo della credibilità di una chiave pubblica della quale si è venuti in possesso. In pratica, se ci si fida ciecamente del giudizio di Sempronio, è ragionevole accettare

come valide tutte le chiavi pubbliche controfirmate da lui. Per accedere a queste funzioni, si utilizza il solito comando '**`--edit-key`**'; quindi, nell'ambito del funzionamento interattivo che si ottiene, si utilizza il comando '**`trust`**'.

```
$ gpg --edit-key caio@roggen.brot.dg [Invio]

  pub  1024D/C38563D0  created: 1999-10-01 expires: 1999-10-08 trust: -/q
  sub  1024g/E3460DB4  created: 1999-10-01 expires: 1999-10-08
  (1)  Caio Cai <caio@roggen.brot.dg>
```

Dopo aver ottenuto la situazione della chiave pubblica di Caio e delle sue sottochiavi, si può richiedere di passare alla gestione della fiducia nei suoi confronti.

```
Command> trust [Invio]

  pub  1024D/C38563D0  created: 1999-10-01 expires: 1999-10-08 trust: -/q
  sub  1024g/E3460DB4  created: 1999-10-01 expires: 1999-10-08
  (1)  Caio Cai <caio@roggen.brot.dg>

  Please decide how far you trust this user to correctly
  verify other users' keys (by looking at passports,
  checking fingerprints from different sources...)?

   1 = Don't know
   2 = I do NOT trust
   3 = I trust marginally
   4 = I trust fully
   s = please show me more information
   m = back to the main menu
```

In breve: il valore uno corrisponde a un livello indefinibile; due fa riferimento a una persona inaffidabile; tre rappresenta una fiducia parziale; quattro è una fiducia completa. Viene mostrato il caso in cui si indica una fiducia parziale.

```
Your decision? 3 [Invio]
```

```
pub  1024D/C38563D0  created: 1999-10-01 expires: 1999-10-08 trust: m/q
sub  1024g/E3460DB4  created: 1999-10-01 expires: 1999-10-08
(1)  Caio Cai <caio@roggen.brot.dg>

Command> quit [Invio]
```

A questo punto è importante definire il significato delle lettere che appaiono sulla destra, nel campo '**`trust:`**'. Come si vede dagli esempi, si tratta di due lettere staccate da un barra obliqua: la prima lettera definisce il grado di fiducia nei confronti della persona; la seconda definisce la fiducia sull'autenticità della sua chiave pubblica. Infatti, la fiducia nei confronti di una firma, è condizionata dal fatto che la chiave pubblica che si dispone per il controllo sia effettivamente quella giusta (e non una contraffazione). La tabella 44.38 mostra l'elenco di queste lettere, assieme alla descrizione del loro significato.

Tabella 44.38. Elenco degli indicatori utilizzati per definire i livelli di fiducia.

Lettera	Significato
`-`	Fiducia indefinita nei confronti della persona.
`e`	Calcolo della fiducia fallito.
`q`	Informazioni insufficienti per il calcolo della fiducia.
`n`	Non viene attribuita alcuna fiducia alla chiave.
`m`	Fiducia parziale nei confronti della persona.
`f`	Fiducia totale nei confronti della persona.

Lettera	Significato
`u`	Certezza assoluta dell'autenticità della chiave.

Una volta stabilito il livello di fiducia nei confronti delle persone e delle loro chiavi pubbliche, si può stabilire in che modo le altre chiavi controfirmate da questi possono essere acquisite nel proprio portachiavi. In generale, salvo la modifica della configurazione predefinita, valgono le regole seguenti:

- una chiave firmata personalmente è valida a tutti gli effetti;
- una chiave firmata da una persona fidata è trattata come autentica se la sua stessa chiave pubblica è ritenuta sicura;
- una chiave firmata da almeno tre persone di cui ci si fida in parte è trattata come autentica se le loro stesse chiavi pubbliche sono ritenute sicure.

Oltre a questo elenco si deve considerare anche il «percorso di fiducia». Forse si comprende meglio il problema pensando per analogia alle girate di un titolo di credito trasferibile: la prima girata è quella della persona a cui è destinato il titolo, mentre le girate successive sono quelle di persone che si sono passate di mano il titolo. Se Sempronio è l'ultimo di questi e ci si fida di lui, mentre degli altri non si sa nulla, diventa difficile accettare un titolo del genere quando l'elenco delle girate comincia a diventare lungo. Ecco quindi il senso di questo percorso di fiducia che rappresenta il numero di persone attraverso le quali la chiave pubblica giunge al nostro portachiavi. In generale, per poter accettare come valida una chiave, è necessario

anche che il percorso di fiducia sia minore o al massimo uguale a cinque passaggi.

44.2.6 Accesso a un servente di chiavi

«

Prima di accedere a un servente di chiavi, occorre determinare quale possa essere quello più comodo rispetto alla propria posizione nella rete. Supponendo di avere scelto il nodo *www.it.pgp.net*, ammesso che si tratti effettivamente di un servente di chiavi, si può utilizzare lo stesso GnuPG per prelevare le chiavi pubbliche a cui si è interessati, purché se ne conosca il numero di identificazione:

```
$ gpg --keyserver www.it.pgp.net --recv-key 0x0C9857A5 [Invio]

  gpg: requesting key 0C9857A5 from www.it.pgp.net ...
  gpg: key 0C9857A5: 1 new signature

  gpg: Total number processed: 1
  gpg:          new signatures: 1
```

Per l'invio della propria chiave pubblica, si agisce in modo simile:

```
$ gpg --keyserver www.it.pgp.net ↩
↪     --send-key tizio@dinkel.brot.dg [Invio]

  gpg: success sending to 'www.it.pgp.net' (status 200)
```

Se per qualche motivo i serventi di chiavi locali non consentono l'accesso, si può sempre riparare presso *certserver.pgp.com*.

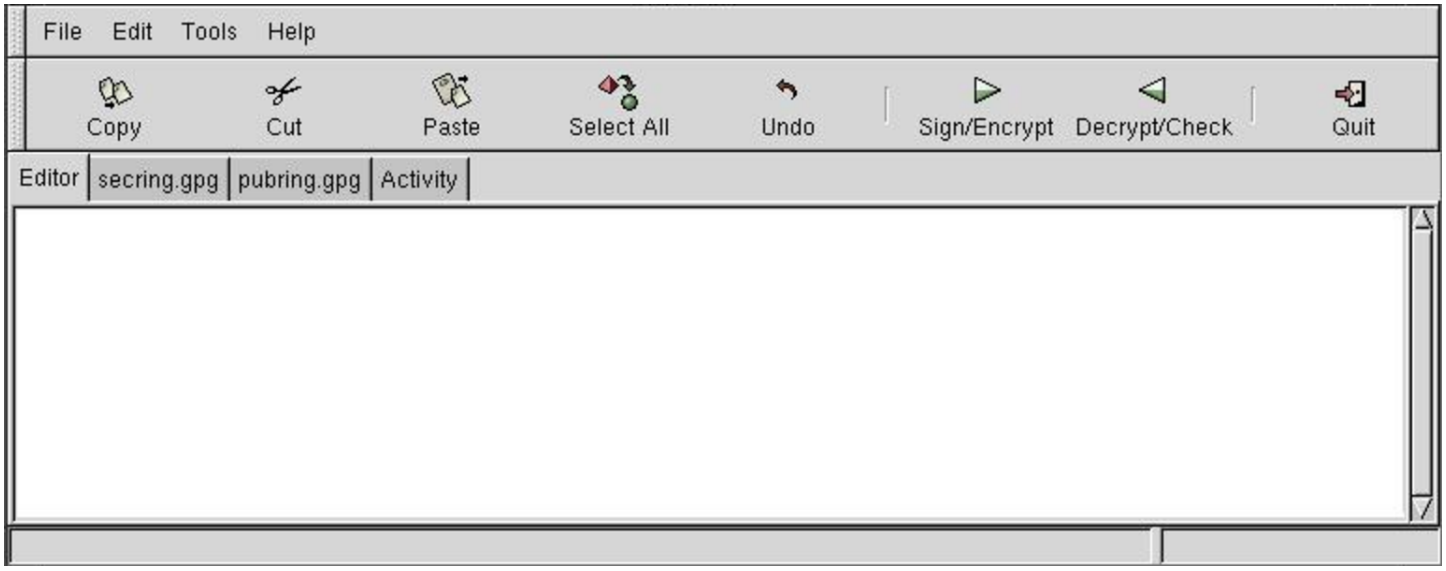
44.2.7 Gnome PGP

Gnome PGP, ovvero GPGP,[7] è un programma frontale, grafico, per semplificare l'uso di GnuPG. Prima di usare Gnome PGP occorre predisporre almeno la propria coppia di chiavi con GnuPG; poi, con Gnome PGP si possono gestire i portachiavi e si possono eseguire più comodamente le operazioni di cifratura, decifratura, firma e verifica delle firme. Gnome PGP si avvia semplicemente con l'eseguibile '**gpgp**', senza bisogno di fornire argomenti:

```
gpgp
```

Se è già stato usato il programma GnuPG per creare la propria coppia di chiavi, l'aspetto iniziale di Gnome PGP è simile a quello della figura successiva.

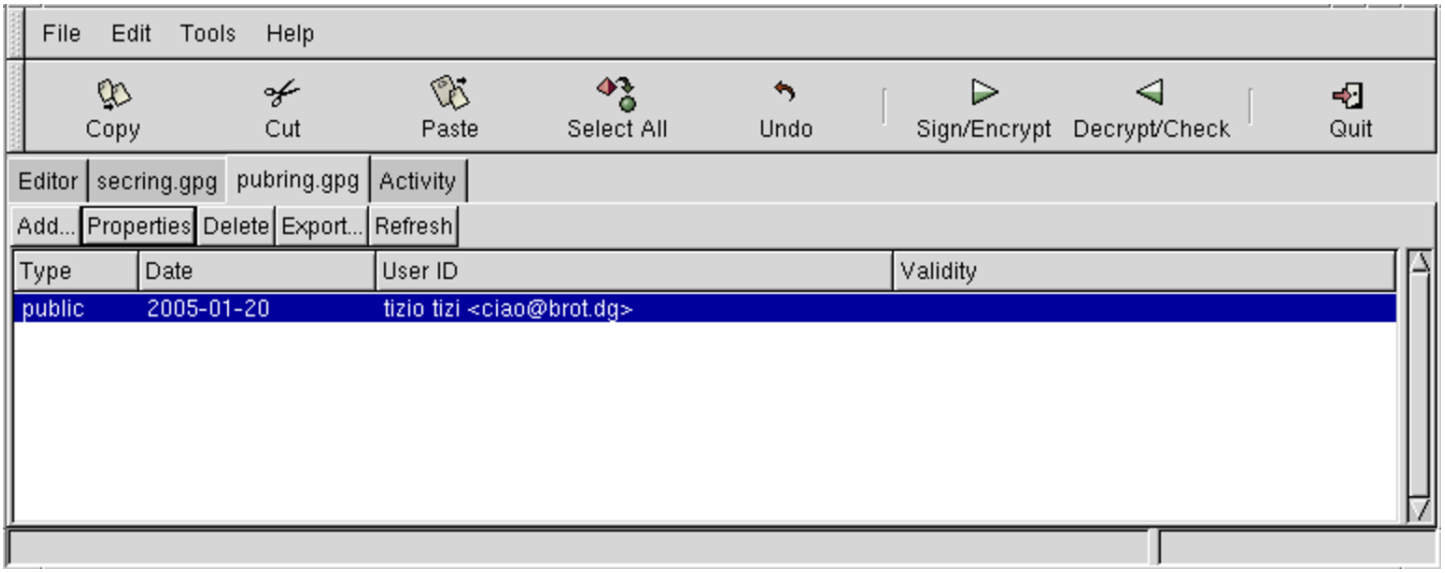
Figura 44.41. Aspetto di Gnome PGP all'avvio.



Come si può vedere dalla figura, appaiono i lembi delle schede associate al portachiavi privato ('`secring.gpg`') e al portachiavi pubblico ('`pubring.gpg`'). I portachiavi sono stati letti automaticamente

dai file previsti normalmente per queste funzioni, secondo l'organizzazione di GnuPG: '`~/.gnupg/secring.gpg`' e '`~/.gnupg/pubring.gpg`'. Selezionando l'etichetta *pubring.gpg* si possono gestire le chiavi pubbliche; nella figura successiva si vede che appaiono dei pulsanti grafici, in particolare per aggiungere chiavi da altri file ed esportarle.

Figura 44.42. Aspetto di Gnome PGP durante la gestione delle chiavi pubbliche.



Per cifrare o per firmare, si comincia selezionando il pulsante grafico SIGN/ENCRYPT, mentre per decifrare o per verificare una firma si usa DECRYPT/CHECK.

44.3 Autorità di certificazione e certificati

«

Il «certificato» è un file contenente alcuni dati identificativi di una persona, in un contesto determinato, abbinati alla chiave pubblica della stessa, firmato da una o più autorità di certificazione. In pratica le firme di queste autorità servono a garantire la veridicità dei dati, confermando che la chiave pubblica abbinata appartiene effettivamente alla persona indicata. Volendo vedere le cose da un altro

punto di vista, la chiave pubblica che è stata controfirmata da altre persone, è un certificato della veridicità della chiave pubblica stessa, il quale è tanto più valido, quanto più credibili sono le persone che hanno aggiunto la loro firma.

Dal momento che la crittografia a chiave pubblica serve per cifrare, ma soprattutto per firmare i documenti in forma elettronica, si tratta di uno strumento strettamente **personale**. Per questa ragione, un certificato dovrebbe essere sempre riferito a una persona particolare, anche se questa lo deve utilizzare nell'ambito del proprio lavoro, per lo svolgimento dei suoi incarichi.

Nel momento in cui la crittografia a chiave pubblica viene usata professionalmente, come nel caso del commercio elettronico, è indispensabile la presenza delle autorità di certificazione, ovvero di enti (privati o pubblici) specializzati nella certificazione. Ogni autorità di certificazione stabilisce e impone la propria procedura per fornire la propria certificazione; questo significa che ogni autorità definisce il proprio ambito di competenza, quali tipi di certificazione elettronica è in grado di fornire (si fa riferimento al formato del certificato elettronico) e quali siano le informazioni che devono essere fornite in modo preciso. È poi compito dell'autorità la verifica della veridicità di tali informazioni.

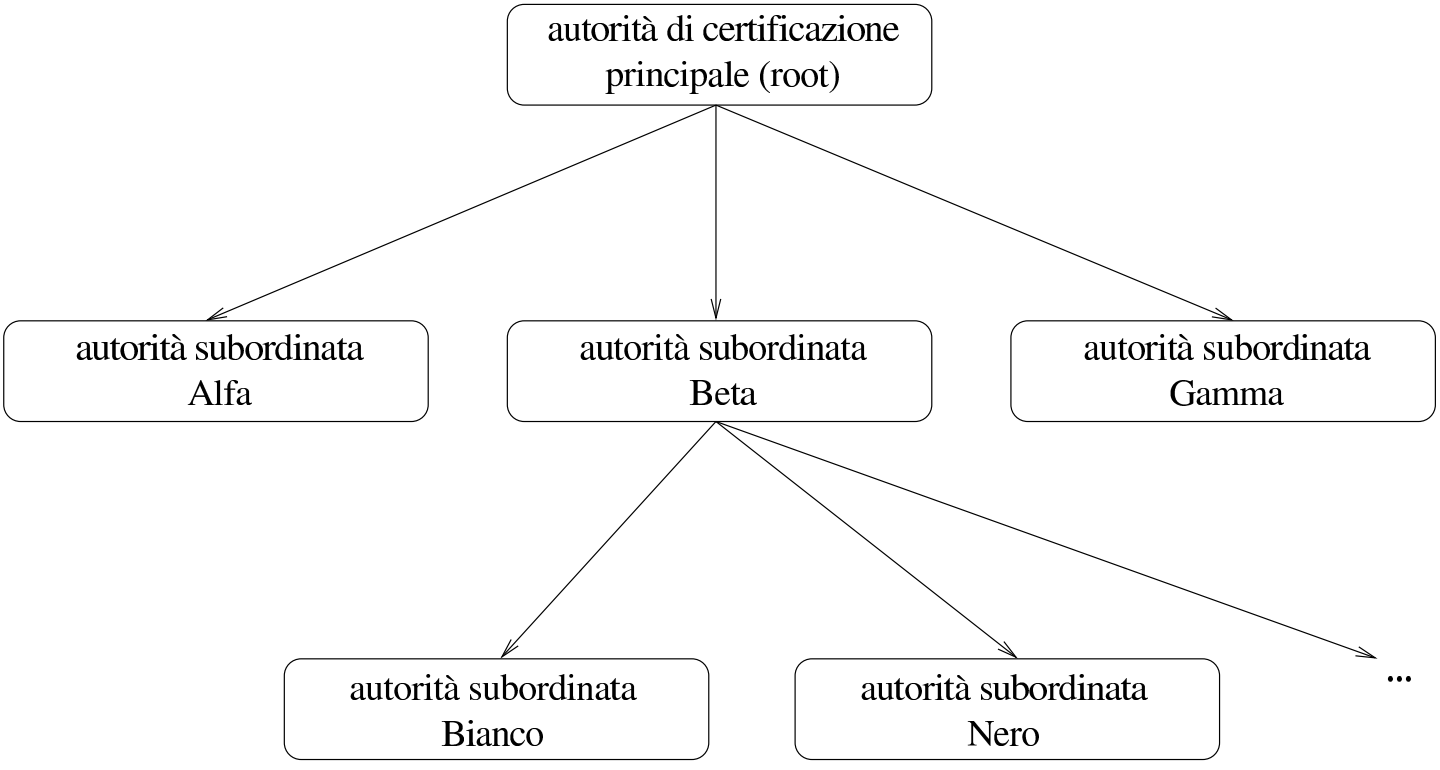
44.3.1 Catena di certificazione

La certificazione da parte di queste autorità, ovvero la loro firma sui certificati elettronici, vale solo se questa è verificabile, per cui è necessario disporre della chiave pubblica di tali autorità. Anche la chia-

ve pubblica di un'autorità di certificazione viene diffusa attraverso un certificato.

Un'autorità di certificazione potrebbe funzionare in modo autonomo, oppure potrebbe appartenere a una struttura più o meno articolata. Infatti, ci potrebbe essere la necessità di suddividere il carico di lavoro in più organizzazioni. La figura 44.43 mostra una struttura gerarchica ad albero, dove si parte da un'autorità principale che si autocertifica, demandando e organizzando il compito di certificazione a strutture inferiori, firmando il loro certificato (con la propria chiave privata). Queste autorità inferiori possono avere a loro volta la responsabilità sulla certificazione di altre autorità di livello ancora inferiore, ecc.

Figura 44.43. Gerarchia tra più autorità di certificazione.



La presenza di una scomposizione gerarchica tra le autorità di certificazione, più o meno articolata, genera una ***catena di certificati***,

ovvero un «percorso di fiducia». Di fronte a questa situazione, sarebbe bene che il tipo di certificato elettronico che si utilizza permettesse di annotare questa catena, in maniera tale che sia possibile il recupero dei certificati mancanti. In pratica, chi ottiene un certificato di Tizio, firmato dall'autorità Bianco, per verificare l'autenticità del certificato di questo signore, deve disporre della chiave pubblica di quell'autorità, o in altri termini, deve avere il certificato dell'autorità stessa (che contiene anche la sua chiave pubblica); altrimenti non potrebbe verificare la firma di questa autorità. Tuttavia, se nel certificato di Tizio è annotato che l'autorità Beta è garante per l'autorità Bianco e inoltre è annotato in che modo procurarsi il certificato di Bianco rilasciato da Beta, se si dispone già del certificato dell'autorità Beta, dopo che è stato prelevato il certificato di Bianco, questo lo si può controllare attraverso quello di Beta. I passaggi si possono rivedere descritti nell'elenco seguente:

- Tizio si presenta con il proprio certificato, contenente la firma di garanzia dell'autorità Bianco;
- l'autorità Bianco è sconosciuta, di conseguenza non si dispone del suo certificato, dal quale sarebbe necessario estrarre la chiave pubblica per verificarne la firma sul certificato di Tizio;
- nel certificato di Tizio c'è scritto in che modo ottenere il certificato dell'autorità Bianco, il quale viene così prelevato attraverso la rete;
- nel certificato di Tizio c'è scritto che l'autorità Bianco è garantita dall'autorità Beta, della quale, per fortuna, si dispone del certificato;

- con la chiave pubblica di Beta si verifica la firma nel certificato di Bianco;
- disponendo del certificato di Bianco e avendo verificato la sua autenticità, si può verificare l'autenticità del certificato di Tizio.

Se non si disponesse del certificato di Beta occorrerebbe ripetere la ricerca per l'autorità garante superiore, nel modo già visto.

44.3.2 Numero di serie, scadenza e revoca dei certificati

«

Un certificato non può essere valido per sempre, così come accade con un documento di riconoscimento: una carta di identità o un passaporto. Un'informazione fondamentale che deve avere un certificato elettronico è la scadenza; questa è sempre l'informazione che viene controllata per prima, chiunque sia il titolare del certificato.

Tuttavia, anche nel periodo di validità di un certificato possono cambiare tante cose, per cui deve essere previsto un meccanismo di revoca: sia su richiesta del titolare; sia a seguito di una decisione dell'autorità di certificazione che lo ha firmato. Infatti, il titolare del certificato potrebbe trovarsi in una condizione diversa rispetto a quella in cui si trovava nel momento del rilascio del certificato stesso, per cui i dati in esso contenuti potrebbero non corrispondere più; dall'altra parte, l'autorità di certificazione potrebbe avere verificato un utilizzo irregolare del certificato e di conseguenza potrebbe decidere il suo ritiro.

Evidentemente, per ottenere questo risultato, occorre che l'autorità che ha rilasciato dei certificati, gestisca anche una base di dati in cui siano indicati quelli che sono stati revocati, identificabili attraverso il loro numero di serie, il quale è quindi un altro elemento indispen-

sabile di un certificato. A questo punto, quando si vuole verificare un certificato, oltre a controllare la scadenza e la validità della firma dell'autorità di certificazione, occorre controllare presso la base di dati di questa che il certificato non sia già stato revocato.

Il meccanismo della revoca o del non-rinnovo dei certificati, serve anche a dare credibilità a una catena di autorità di certificazione: un anello debole della catena -- debole in quanto poco serio -- metterebbe in dubbio tutto il sistema e sarebbe nell'interesse di tutte le altre autorità la sua eliminazione. Si intende che l'azione necessaria per ottenere questo risultato è la semplice pubblicazione della revoca del certificato da parte dell'autorità di livello superiore, oppure il suo mancato rinnovo.

44.3.3 Certificato X.509

Un tipo di certificato importante è quello definito dallo standard X.509. Questo certificato serve ad abbinare un ***nome distintivo*** (conosciuto come *Distinguished name*, ovvero l'acronimo DN) a una chiave pubblica. Questo nome distintivo è in pratica una raccolta di informazioni su una certa persona in un certo contesto. Gli elementi di queste informazioni sono visti come l'assegnamento di valori ad altrettante variabili; anche se non sono utilizzate sempre tutte, è importante tenere conto di questo fatto, ricordando le più importanti, per poter interpretare correttamente le richieste dei programmi che utilizzano questo standard.

Tabella 44.44. Alcuni campi tipici di un nome distintivo nei certificati X.509.

Campo	Descrizione
UID	Nominativo.
CN	Nome comune, o *Common name*.
O	Organizzazione.
OU	Dipartimento all'interno dell'organizzazione.
C	Sigla del paese (nazione).
ST	Regione o provincia.
L	Località.

Le regole per stabilire esattamente quali campi devono essere usati e cosa devono contenere, dipende dalla politica dell'autorità che deve firmare il certificato. In particolare, il campo ***CN***, a cui corrisponde la definizione *Common name*, è l'elemento più vago. Spesso, quando il certificato riguarda la gestione di un servizio, contiene il nome a dominio completo dell'elaboratore dal quale questo viene offerto.

Le informazioni di un certificato X.509 tipico sono organizzate in due parti: la sezione dati e la sezione della firma digitale. La sezione dati contiene in particolare:

- la versione dello standard X.509 a cui fa riferimento il certificato;
- il numero di serie assegnato dall'autorità di certificazione;
- il nome distintivo (DN) dell'autorità di certificazione;
- il periodo di validità del certificato;
- il nome distintivo (DN) del titolare della certificato (*subject*);
- la chiave pubblica del titolare del certificato;

- altre informazioni che rappresentano un'estensione dello standard.

La sezione della firma digitale contiene in pratica la firma fatta dall'autorità di certificazione, ed è in questa parte che potrebbero apparire le informazioni necessarie ad acquisire il certificato dell'autorità stessa. A titolo di esempio si può vedere come può apparire un certificato del genere, quando questo viene tradotto in forma leggibile (la chiave pubblica e la firma sono abbreviate):

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=IT, ST=Italia, L=Milano, O=SuperCA, CN=super.ca.dg…
        Validity
            Not Before: Dec 11 19:39:32 1999 GMT
            Not After : Jan 10 19:39:32 2000 GMT
        Subject: C=IT, ST=Italia, L=Tiziopoli, O=Dinkel, CN=dinkel.brot.dg…
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:f2:c2:7a:4b:11:c0:64:b8:63:9d:fd:7f:b1:b7:
                    1f:55:c1:b7:1a:9b:dc:5f:bc:d8:a8:ad:cb:90:17:
                …
                    a2:7c:f9:be:92:be:1f:7e:9e:27:0e:87:d0:74:22:
                    fd:cd:7e:47:4a:b3:12:56:fd
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        71:88:37:bb:f0:5e:6e:82:fa:90:87:4f:bb:b6:06:a3:da:6a:
        86:b7:78:8d:a6:49:c2:e1:24:2d:37:ae:70:92:b7:68:49:14:
    …
        39:22:3b:41:46:d9:36:3a:85:d0:b2:d3:0d:d0:82:54:00:8e:
        38:b7:fa:52:09:d3:14:ea:18:c2:d5:5b:88:ef:05:18:1e:bd:
        c1:4e
```

È interessante osservare le righe che descrivono l'autorità garante che emette il certificato (*Issuer*) e il titolare (*Subject*). Ognuna di queste due righe rappresenta rispettivamente il nome distintivo dell'autorità e del titolare; si può vedere in che modo sono indicati i vari elementi di questa informazione (i puntini di sospensione finali sono stati aggiunti perché la riga sarebbe più lunga, con altre informazioni):

```
C=IT, ST=Italia, L=Tiziopoli, O=Dinkel-Brot, CN=dinkel.brot.dg…
```

La forma è quella dell'assegnamento di variabili, alcune delle quali sono elencate nella tabella 44.44. La scelta delle variabili da indicare (da assegnare) dipende dall'autorità e dal contesto per il quale viene rilasciato il certificato.

Il certificato è realizzato normalmente in formato PEM (utilizza solo il codice ASCII a sette bit) e il file che lo rappresenta in pratica potrebbe apparire in un modo simile a quello seguente, mostrato qui in forma abbreviata:

```
-----BEGIN CERTIFICATE-----
MIICeTCCAeICAQAwDQYJKoZIhvcNAQEEBQAwgYQxCzAJBgNVBAYTAklUMQ8wDQYD
VQQIEwZJdGFsaWExEDAOBgNVBAcTB1RyZXZpc28xFDASBgNVBAoTC0RpbmtlbC1C
…
t3iNpknC4SQtN65wkrdoSRQb88RpFYCkpISCbutfU4lZ+8XV7ASOJcHOrqqR65PZ
AeP4kVAFLnG+HTGlqHtReWszL6y75c45IjtBRtk2OoXQstMN0IJUAI44t/pSCdMU
6hjC1VuI7wUYHr3BTg==
-----END CERTIFICATE-----
```

44.3.4 Richiesta di certificato X.509

Per ottenere un certificato da un'autorità, utilizzando lo standard X.509, si parte dalla creazione di una ***richiesta di certificato***, che in pratica è un certificato avente già tutte le informazioni, tranne la fir-

ma del garante, firmato direttamente dal richiedente. Ciò che segue potrebbe essere la richiesta di certificato corrispondente all'esempio già visto in precedenza; anche in questo caso si abbreviano la chiave pubblica e la firma:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=IT, ST=Italia, L=Tiziopoli, O=Dinkel, CN=dinkel.brot.dg…
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:f2:c2:7a:4b:11:c0:64:b8:63:9d:fd:7f:b1:b7:
                    1f:55:c1:b7:1a:9b:dc:5f:bc:d8:a8:ad:cb:90:17:
                …
                    a2:7c:f9:be:92:be:1f:7e:9e:27:0e:87:d0:74:22:
                    fd:cd:7e:47:4a:b3:12:56:fd
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :ciao-ciao
            unstructuredName         :Dinkel
    Signature Algorithm: md5WithRSAEncryption
        09:eb:da:65:21:d1:67:65:ec:c3:f7:07:7b:82:fb:3f:d3:9f:
        ed:89:bc:be:38:bd:97:1c:15:f0:2b:2f:ef:6b:1e:00:57:47:
    …
        e7:70:9c:93:30:f1:aa:93:42:37:dc:32:e0:85:50:d9:ed:0e:
        f7:8e
```

Anche la richiesta di certificato è realizzato normalmente in formato PEM; il file che lo rappresenta in pratica potrebbe apparire in un modo simile a quello seguente:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB/TCCAWYCAQAwgYIxCzAJBgNVBAYTAklUMQ8wDQYDVQQIEwZJdGFsaWExEDAO
BgNVBAcTB1ZlbmV6aWExFDASBgNVBAoTC01BUkFNQU8tTUFIMRkwFwYDVQQDFBBj
…
YwJNRXTBdL7J/K+LVYFnnxbu6Z4vyDvqcCxD0hWE3VSkXQ2RHHW3sN1oMbtVfjS7
NMe5qq5noKkraMhq3edwnJMw8aqTQjfcMuCFUNntDveO
-----END CERTIFICATE REQUEST-----
```

44.3.5 Revoca dei certificati

«

L'autorità di certificazione che ha la necessità di pubblicare i certificati che vengono revocati prima della loro scadenza naturale, lo fa attraverso la pubblicazione di un elenco dei certificati revocati, ovvero di ciò che è conosciuto con la sigla CRL (*Certificate revocation list*). Questo elenco è firmato dall'autorità di certificazione che lo pubblica, pertanto si tratta di un tipo di certificato speciale. Nello standard X.509, questo elenco potrebbe apparire come si vede nell'esempio seguente, in cui si vedono due certificati revocati:

```
Certificate Revocation List (CRL):
        Version 1 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: /C=IT/ST=Italia/L=Milano/O=SuperCA/CN=super.ca.dg
        Last Update: Jan 15 20:35:52 2000 GMT
        Next Update: Feb 14 20:35:52 2000 GMT
Revoked Certificates:
    Serial Number: 01
        Revocation Date: Jan 13 19:28:40 2000 GMT
    Serial Number: 02
        Revocation Date: Jan 13 19:28:40 2000 GMT
    Signature Algorithm: md5WithRSAEncryption
        32:e1:97:92:96:2f:0c:e4:df:bb:9c:82:a5:e3:5b:51:69:f5:
        51:ad:1b:b2:98:eb:35:a6:c8:7f:d9:29:1f:b2:1e:cc:da:84:
    …
        31:27:4a:21:4c:7a:bc:85:73:cd:ff:15:9d:cb:81:b3:0b:82:
```

73:50

Osservando l'elenco si vede che il riferimento ai certificati è fatto solo attraverso il numero di serie, stando a indicare che i certificati firmati dall'autorità, con questi numeri di serie, sono revocati a partire dalle date indicate.

44.4 Connessioni cifrate e certificate

Ogni protocollo pensato specificatamente per le connessioni cifrate, ha le sue particolarità, dettate dalle esigenze iniziali per le quali è stato realizzato. In linea di massima si possono individuare le fasi seguenti:

- il cliente negozia con il servente le caratteristiche del protocollo cifrato da adottare;
- il servente invia al cliente la propria chiave pubblica all'interno di un certificato che il cliente può verificare, se ne è in grado e se lo ritiene necessario;
- il servente può pretendere dal cliente un certificato che possa verificare, oppure può pretendere di essere già in possesso della chiave pubblica del cliente (naturalmente già verificata);
- una volta che il cliente dispone della chiave pubblica del servente, può iniziare una prima fase di comunicazione cifrata, in cui solitamente ci si scambia una chiave simmetrica generata in modo casuale, per rendere più sicura la comunicazione.

La verifica dei certificati serve a garantire l'identità dei nodi e delle utenze coinvolte, ovvero, un servente può garantire l'identità del

servizio, mentre un cliente può garantire l'identità dell'utente che lo richiede.

La situazione tipica in cui si richiede una connessione cifrata è quella in cui una persona «qualunque» voglia fare un acquisto presso un negozio telematico, utilizzando il proprio navigatore. Dovendo fornire i propri dati personali, compresi quelli della carta di credito, questa persona vuole essere sicura di trasmettere le informazioni alla controparte giusta. Per questo, il suo navigatore che instaura la comunicazione cifrata, deve garantire all'utilizzatore l'identità della controparte attraverso la verifica della chiave pubblica del servizio, chiave che deve essere già in suo possesso, all'interno di un certificato ritenuto valido.

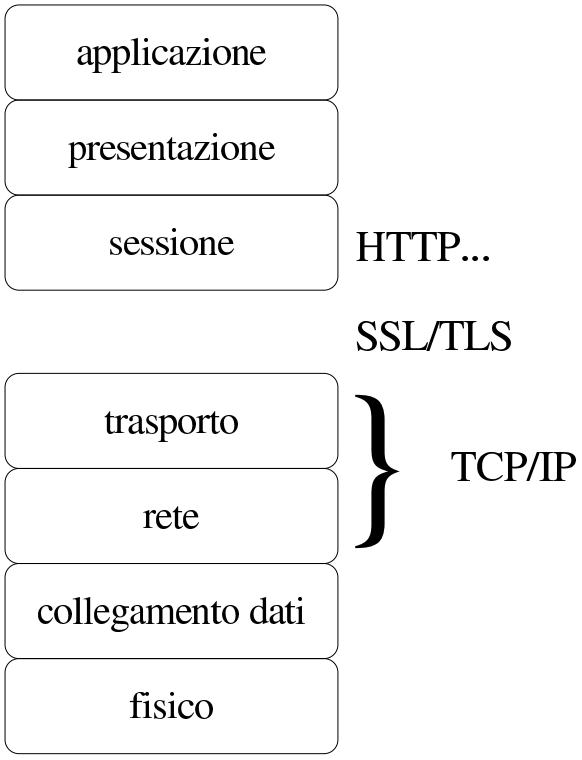
Quando l'accesso a un servizio che presuppone una connessione cifrata è soggetto a una forma di registrazione, l'autenticazione dell'accesso da parte del cliente può avvenire attraverso l'uso di un certificato depositato in precedenza. In pratica, in questo modo il servente può chiedere al cliente di iniziare subito una connessione cifrata che da parte sua può decifrare usando la chiave pubblica del cliente stesso, a garanzia della sua identità, senza bisogno di richiedere l'inserimento della solita parola d'ordine.

In tutti i casi, questo tipo di connessioni non dovrebbe tornare mai a trasmettere dati in chiaro. Infatti, anche se lo scopo della procedura fosse solo quello di garantire l'identità delle parti, resta comunque necessario mantenere la connessione cifrata per garantire anche che una delle parti non venga sostituita durante la comunicazione.

44.4.1 SSL/TLS

SSL (*Secure socket layer*) e TLS (*Transport layer security*) sono due protocolli per la certificazione e la comunicazione cifrata. SSL è stato sviluppato originalmente da Netscape; TLS è l'evoluzione del primo, come standard pubblicato da IETF.

Figura 44.51. Collocazione dei protocolli SSL/TLS nel modello ISO-OSI.



Nel modello ISO-OSI, il protocollo SSL/TLS si inserisce tra il livello di trasporto (quarto) e il livello di sessione (quinto). Le sue funzionalità sono essenzialmente:

- autenticazione del servente da parte del cliente, con il quale l'utente di un servizio è in grado di essere certo dell'identità del suo fornitore;
- autenticazione del cliente nei confronti del servente, con il quale il fornitore di un servizio si accerta dell'identità del proprio

cliente, senza dover usare le forme tradizionali (nominativo e parola d'ordine);

- crittografica della comunicazione, per garantire la segretezza delle transazioni.

Attraverso la descrizione del meccanismo di negoziazione che c'è tra cliente e servente di una connessione SSL/TLS, si intendono meglio il significato e il funzionamento di questo sistema. In generale, la negoziazione consente al servente di farsi riconoscere nei confronti del cliente, attraverso la tecnica della chiave pubblica, con la quale le due parti possono poi creare una chiave simmetrica da usare per cifrare la comunicazione; inoltre, è possibile anche richiedere al cliente di identificarsi nello stesso modo in cui fa il servente.

1. Il cliente si presenta presso il servente fornendo alcune informazioni sulla versione del protocollo che è in grado di gestire.
2. Il servente risponde comunicando le scelte fatte in base alla disponibilità del cliente, inviando il proprio certificato; inoltre, se la risorsa richiesta prevede l'identificazione del cliente, richiede anche il suo certificato.
3. Il cliente analizza il certificato (del servente) e determina se può riconoscere o meno il servente; se l'autorità di certificazione che lo ha firmato è sconosciuta, si chiede all'utente di intervenire per decidere il da farsi.
4. Attraverso i dati ottenuti fino a questo punto, il cliente prepara un primo esemplare dell'informazione che serve poi per definire la chiave di sessione, lo cifra attraverso la chiave pubblica del servente e lo invia.

5. Se il servente aveva richiesto l'autenticazione da parte del cliente, verifica l'identità di questo; se il cliente non viene riconosciuto, la sessione termina.
6. Il servente e il cliente determinano la chiave di sessione (simmetrica), in base ai dati che si sono scambiati fino a quel momento, iniziando la comunicazione cifrata con quella chiave.

Leggendo la sequenza di queste operazioni, si intende che la connessione cifrata può avvenire solo perché il servente offre un certificato, contenente la chiave pubblica dello stesso, attraverso la quale il cliente può cifrare inizialmente le informazioni necessarie a entrambi per generare una chiave di sessione. Di conseguenza, con questo modello, non può instaurarsi una comunicazione cifrata se il servente non dispone di un certificato e di conseguenza non dispone della chiave privata relativa.

Dal momento che la disponibilità di un certificato è indispensabile, se si vuole attivare un servizio che utilizza il protocollo SSL/TLS per cifrare la comunicazione, se non è possibile procurarselo attraverso un'autorità di certificazione, è necessario produrne uno fittizio in proprio.

Vale la pena di elencare brevemente i passi che compie il cliente per verificare l'identità del servente:

1. viene verificato che il certificato non sia scaduto, facendo in modo che se la data attuale risulta al di fuori del periodo di validità, l'autenticazione fallisca;[8]

2. viene verificata la disponibilità del certificato dell'autorità che ha firmato quello del servente; se è presente si può controllare la firma e di conseguenza la validità del certificato offerto dal servente;
3. se il cliente non dispone del certificato dell'autorità di certificazione e non è in grado di procurarselo e nemmeno di verificarlo attraverso una catena di certificazioni, l'autenticazione del servente fallisce;[9]
4. infine, viene verificato che il nome a dominio del servente corrisponda effettivamente con quanto riportato nel certificato.[10]

44.4.2 SSH

«

Il protocollo SSH è nato a seguito dello sviluppo di Secure Shell, un sistema per l'accesso remoto «sicuro» che si sostituisce a quello tradizionale dei programmi come Rlogin e Telnet. Secure Shell, ovvero SSH, è oggi un software proprietario, ma esistono diverse realizzazioni, più o meno libere, con funzionalità analoghe, o equivalenti, basate sullo lo stesso protocollo.[11]

Attraverso il protocollo SSH si possono gestire diversi livelli di sicurezza, in cui il minimo in assoluto è rappresentato dalla cifratura della comunicazione, estendendosi a vari metodi di riconoscimento reciproco da parte dei nodi che si mettono in contatto.

Il software che utilizza il protocollo SSH può instaurare un collegamento tra due elaboratori utilizzando diverse modalità, come accennato, in cui l'unica costante comune è la cifratura della comunicazione.

Semplificando molto le cose, da una parte si trova il servente che offre l'accesso e mette a disposizione una chiave pubblica, attraverso la quale i clienti dovrebbero poter verificare l'autenticità del servente a cui si connettono. Appena si verifica la connessione, prima ancora che sia stata stabilita l'identità dell'utente, cliente e servente concordano un sistema di cifratura.

44.4.2.1 Autenticazione RHOST

Alcune realizzazioni del software che utilizza il protocollo SSH consentono ancora, se lo si desidera, di utilizzare il vecchio meccanismo dell'autenticazione attraverso i file '`/etc/hosts.equiv`' e '`~/.rhosts`', corrispondenti in pratica a quelli utilizzati da Rlogin e Rsh.

Attraverso questi file, o un'altra coppia analoga per non interferire con Rlogin e Rsh, si può stabilire semplicemente quali clienti e quali utenti possono accedere senza che venga richiesta loro la parola d'ordine. Si tratta ovviamente di un sistema di riconoscimento molto poco sicuro, che rimane solo per motivi storici, ma in generale viene lasciato disabilitato.

44.4.2.2 Autenticazione RHOST+RSA

Per attenuare lo stato di debolezza causato da un sistema che accetta di autenticare i clienti e gli utenti esclusivamente in base alla configurazione di '`/etc/hosts.equiv`' e '`~/.rhosts`' (o simili), si può aggiungere la verifica della chiave pubblica del cliente.

In pratica, se il cliente dispone di una sua chiave pubblica può dimostrare al servente la sua identità.

44.4.2.3 Autenticazione RSA

A fianco dei metodi di autenticazione derivati da Rlogin si aggiunge il metodo RSA, attraverso cui, ogni utente che intende utilizzarlo deve creare una propria chiave RSA, indicando nel proprio profilo personale presso il servente la parte pubblica di questa chiave. Quando l'utente tenta di accedere in questo modo, le chiavi vengono confrontate e la corrispondenza è sufficiente a concedere l'accesso senza altre formalità.

Quando si utilizza questo tipo di autenticazione, la parte privata della chiave generata dall'utente, viene cifrata generalmente attraverso una parola d'ordine. In questo modo, prima di ottenere l'autenticazione, l'utente deve anche fornire questa parola d'ordine.

Generalmente, quando si utilizza l'autenticazione RSA, occorre osservare attentamente i permessi dei file. Di solito, la presenza di un permesso di scrittura superfluo per la directory che contiene i file della chiave privata, dovrebbe essere abbastanza per fare fallire l'autenticazione. Infatti, ciò potrebbe consentire a un estraneo di sostituire le chiavi.

44.4.2.4 Autenticazione attraverso la parola d'ordine tradizionale

Quando tutti gli altri tipi di autenticazione falliscono, il software che utilizza il protocollo SSH verifica l'identità dell'utente attraverso la parola d'ordine relativa all'accesso normale presso quel sistema.

In pratica, questa forma di autenticazione è quella più comune, dal momento che consente l'accesso senza bisogno di alcuna configura-

zione (a parte la generazione della chiave del nodo). Infatti, il protocollo SSH garantisce che la parola d'ordine viaggi cifrata, essendo questo già un grande risultato per la sicurezza dei sistemi coinvolti.

44.4.2.5 Chiave privata e chiave pubblica

Il software che si avvale del protocollo SSH, deve essere provvisto generalmente di un programma per la preparazione di coppie di chiavi pubbliche e private. Queste servono necessariamente per attivare il servizio, dal momento che un servente del genere non può fare nulla senza queste; inoltre possono servire dal lato cliente per facilitare l'autenticazione.

La chiave pubblica e quella privata vengono conservate in due file separati, con permessi di accesso molto restrittivi nel caso del file della chiave privata. Tuttavia, si tende a considerare che entrambi questi file debbano trovarsi nella stessa directory; inoltre, si intende generalmente che il nome del file della chiave pubblica si distingua solo perché ha in più l'estensione '`.pub`'. In questo modo, per fare riferimento alle chiavi, si indica generalmente solo il nome del file della chiave privata, intendendo implicitamente quale sia il nome del file della chiave pubblica.

Tradizionalmente, questi file hanno nomi molto simili da una realizzazione all'altra che utilizza il protocollo SSH. Nel caso delle chiavi del servente, si tratta di qualcosa del tipo '`/etc/*/*_host_key`' e '`/etc/*/*_host_key.pub`', mentre nel caso di chiavi personali dell'utente, si tratta di nomi del tipo '`~/*/identity`' e '`~/*/identity.pub`'. Gli utenti che predispongono una propria coppia di chiavi, lo fanno generalmente per poter utilizzare un'autenticazione di tipo RSA.

In generale, **la chiave privata del servente non può essere protetta attraverso una parola d'ordine, dal momento che il servizio deve essere gestito in modo automatico**; al contrario, è opportuno che la chiave privata di un utente sia protetta, dal momento che non si può impedire all'amministratore del sistema di accedervi.[12]

44.4.2.6 Verifica dell'identità dei serventi

«

Un elemento importante per la garanzia della sicurezza nelle comunicazioni è la verifica dell'identità del servente. Per farlo, è necessario che il cliente possegga una copia della chiave pubblica del servente a cui si vuole accedere.

In generale, la fiducia dovrebbe essere un fatto personale, per cui tali informazioni dovrebbero essere gestite singolarmente da ogni utente che intenda sfruttare tale protocollo. Tuttavia, alcune realizzazioni tradizionali di software che sfruttano il protocollo SSH, consentono di definire un elenco generale di chiavi pubbliche convalidate. Di solito si tratta di file del tipo '`/etc/*/*_known_hosts`', dove oltre alle chiavi si annotano le informazioni sui serventi a cui si riferiscono (a meno che queste indicazioni siano già inserite in un certificato completo).

Nello stesso modo possono agire gli utenti in file del tipo '`~/*/known_hosts`' e ciò è preferibile in generale.

Di solito, per lo scopo che ha il protocollo SSH, non ci si crea il problema di ottenere la chiave pubblica del servente per vie sicure, accontentandosi di accettarla la prima volta che si ha un contatto. Ciò che si ottiene in questo modo è di verificare che il servente non venga sostituito con un altro durante gli accessi successivi.

A questo proposito, il software che utilizza il protocollo SSH può arrangiarsi a fare tutto da solo, dopo aver richiesto una conferma, oppure può pretendere che gli venga chiesto espressamente di accettare la chiave pubblica della controparte anche se questa non può essere verificata. Quello che segue è un esempio di ciò che potrebbe essere segnalato in tali circostanze.

```
  Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)?yes[Invio]

  Host 'linux.brot.dg' added to the list of known hosts.
```

Ovviamente, nel momento in cui si scopre che la chiave pubblica di cui si dispone non consente più di autenticare un servente, il programma che si utilizza deve dare una segnalazione adeguata. Anche in questo caso ci possono essere modi diversi di reagire: impedire l'accesso, oppure chiedere all'utente il da farsi.

```
  @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
  @       WARNING: HOST IDENTIFICATION HAS CHANGED!         @
  @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
  IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
  Someone could be eavesdropping on you right now
  (man-in-the-middle attack)! It is also possible that the
  host key has just been changed. Please contact your system
  administrator.
```

44.5 Introduzione a OpenSSL

OpenSSL[13] è una realizzazione in forma di software libero dei protocolli SSL/TLS (*Secure socket layer* e *Transport layer security*) per la certificazione e la comunicazione cifrata, noto originariamente come SSLeay.

OpenSSL si compone di alcune librerie che permettono di incorporare le funzionalità dei protocolli SSL/TLS all'interno di programmi di comunicazione, oltre a una serie di programmi di servizio per la gestione delle chiavi e dei certificati, arrivando eventualmente anche alla gestione di un'autorità di certificazione.

Questi programmi, in particolare, potrebbero essere compilati in modo da distinguersi in più file eseguibili, oppure in modo da generare un solo eseguibile monolitico: '**`openssl`**'. Qui si presume che si tratti di un eseguibile unico.

44.5.1 Collocazione e impostazione

«

Non esiste una definizione ben precisa di dove devono essere collocati i file che compongono la configurazione e gli strumenti di OpenSSL. Quando si installa OpenSSL da un pacchetto fatto per la propria distribuzione GNU/Linux, è importante scoprire dove vengono collocati i file delle chiavi e dei certificati, così come la collocazione del file di configurazione '`openssl.cnf`'. Intuitivamente si possono cercare questi file a partire dalla directory '`/etc/`'; in particolare, le chiavi potrebbero essere collocate a partire da '`/etc/ssl/`' o da '`/etc/openssl/`'.

Quando gli strumenti di OpenSSL sono organizzati in un solo eseguibile monolitico, la sintassi per i comandi relativi si esprime sinteticamente nel modo seguente:

```
openssl comando [opzioni]
```

Tabella 44.55. Alcuni comandi di OpenSSL.

Comando	Descrizione
`openssl req`	Gestione delle richieste di certificazione.
`openssl ca`	Gestione relativa all'autorità di certificazione.
`openssl crl`	Gestione del certificato delle revoche.
`openssl genrsa`	Generazione di parametri RSA.
`openssl rsa`	Conversione del formato di una chiave privata o di un certificato.
`openssl x509`	Gestione dei dati dei certificati X.509.

La tabella 44.55 elenca brevemente alcuni dei comandi più importanti. Per avere una guida rapida alle opzioni di ogni comando, basta utilizzare un'opzione non valida, per esempio '**`-h`**':

```
$ openssl ca -h [Invio]
```

L'esempio mostra in che modo ottenere l'elenco delle opzioni del comando '**`openssl ca`**'; comunque, in mancanza di altra documentazione, conviene stampare e tenere a portata di mano queste guide:

```
$ openssl req -h > guida.txt [Invio]

$ openssl crl -h >> guida.txt [Invio]

$ openssl ca -h >> guida.txt [Invio]

$ openssl genrsa -h >> guida.txt [Invio]
```

```
$ openssl x509 -h >> guida.txt [Invio]
```

Alcuni di questi comandi hanno in comune delle opzioni che vale la pena di descrivere subito, prima di mostrare degli esempi, nei quali si può così concentrare l'attenzione sulle altre opzioni specifiche. La tabella 44.56 mostra questo elenco di opzioni tipiche.

Tabella 44.56. Alcune opzioni frequenti nei comandi di OpenSSL.

Opzione	Descrizione
`-in` ***file***	Definisce un file in ingresso adatto al contesto.
`-out` ***file***	Definisce un file in uscita adatto al contesto.
`-noout`	Non emette il risultato.
`-text`	Emette le informazioni in forma di testo leggibile.
`-hash`	Emette il codice di controllo relativo al contesto.
`-inform` ***formato***	Specifica il formato dei dati in ingresso.
`-outform` ***formato***	Specifica il formato dei dati in uscita.

Prima di descrivere la configurazione di OpenSSL, viene mostrato tecnicamente il modo per richiedere un certificato, o per realizzarne uno proprio senza valore. Infatti, in generale, la configurazione standard dovrebbe essere più che sufficiente per il raggiungimento di questo obiettivo. È il caso di ricordare che un certificato è un file contenente la chiave pubblica del suo titolare, firmata da un'autorità di certificazione che garantisce la sua validità e anche la correttezza

degli altri dati.

44.5.2 Procedimento per ottenere un certificato

Per mettere in piedi un servizio che utilizzi i protocolli SSL/TLS, occorre predisporre dei file contenenti chiavi e certificati. Di solito, quando si installano servizi che utilizzano questi protocolli, la procedura di installazione si prende cura di predisporre automaticamente i file necessari per consentire il funzionamento, senza che le certificazioni che si ottengono abbiano alcun valore. In generale si comincia dalla creazione o dalla definizione di un file contenente dati casuali, come punto di partenza per generare una chiave privata, quindi si passa alla creazione di una richiesta di certificazione, oppure alla creazione di un certificato auto-firmato, senza valore.

44.5.2.1 File contenente dati casuali

Un file casuale può essere creato in vari modi, per esempio mettendo assieme alcuni file,

```
$ cat file_a file_b file_c > file_casuale[Invio]
```

magari rielaborandoli in qualche modo, oppure prelevando un po' di caratteri dal file '`/dev/random`':

```
$ dd if=/dev/random of=file_casuale bs=1b count=1k[Invio]
```

44.5.2.2 Chiave privata

Per generare una chiave privata in chiaro, si utilizza il comando '**`openssl genrsa`**', in un modo simile a quello seguente, dove in particolare viene utilizzato il file '`file_casuale`' come origine di dati casuali, ottenendo il file '`chiave_privata.pem`' di 1024 bit:

```
$ openssl genrsa -rand file_casuale ↩
↪        -out chiave_privata.pem 1024 [Invio]
```

Eventualmente, per creare una chiave privata cifrata, basta aggiungere un'opzione a scelta tra '**-des**', '**-des3**' e '**-idea**', che stanno a indicare rispettivamente gli algoritmi DES, DES-triplo e IDEA. Viene mostrato il caso in cui si utilizza l'opzione '**-des3**':

```
$ openssl genrsa -des3 -rand file_casuale ↩
↪        -out chiave_privata_protetta.pem 1024 [Invio]

Enter PEM passphrase: ******** [Invio]

Verifying password - Enter PEM pass phrase: ******** [Invio]
```

Volendo riportare la chiave privata in chiaro, si usa il comando '**openssl rsa**', in modo simile all'esempio seguente:

```
$ openssl rsa -in chiave_privata_protetta.pem ↩
↪        -out chiave_privata.pem [Invio]

Enter PEM passphrase: ******** [Invio]
```

In modo analogo funziona l'operazione di protezione di una chiave; in pratica si aggiunge l'opzione attraverso cui si specifica il tipo di algoritmo:

```
$ openssl rsa -des3 -in chiave_privata.pem ↩
↪        -out chiave_privata_protetta.pem [Invio]
```

44.5.2.3 Richiesta di certificazione

Teoricamente, il certificato che identifica e garantisce l'identità del servizio che si gestisce, deve essere fornito da un'autorità di certificazione. In questo caso, per farlo, deve ricevere un documento intermedio, definibile come una richiesta di certificazione. La chiave

pubblica che vi viene inserita si ottiene a partire dalla chiave privata, mentre gli altri dati necessari per il certificato che si vuole ottenere si inseriscono in modo interattivo. È interessante vedere come avviene:

```
$ openssl req -new -key chiave_privata.pem ↩
↪         -out richiesta.pem[Invio]

  You are about to be asked to enter information that will be
  incorporated into your certificate request.
  What you are about to enter is what is called a
  Distinguished Name or a DN. There are quite a few fields but
  you can leave some blank. For some fields there will be a
  default value. If you enter '.', the field will be left
  blank.

Country Name (2 letter code) [AU]:IT[Invio]

State or Province Name (full name) [Some-State]:Italia[Invio]

Locality Name (eg, city) []:Tiziopoli[Invio]

Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Dinkel[Invio]

Organizational Unit Name (eg, section) []:.[Invio]

Common Name (eg, YOUR name) []:dinkel.brot.dg[Invio]

Email address []:tizio@dinkel.brot.dg[Invio]

  Please enter the following 'extra' attributes
  to be sent with your certificate request

A challenge password []:super segretissimo[Invio]

An optional company name []:Dinkel[Invio]
```

Le informazioni che si inviano in questo modo sono molto importanti e il significato preciso varia a seconda del contesto per il quale si richiede la certificazione. È l'autorità per la certificazione a stabilire quali informazioni servono precisamente.

Per verificare il contenuto del certificato, dato che nel suo formato PEM non è leggibile direttamente, si può usare il comando '**`openssl req`**' con l'opzione '**`-text`**':

```
$ openssl req -text -in richiesta.pem[Invio]

  Certificate Request:
      Data:
          Version: 0 (0x0)
          Subject: C=IT, ST=Italia, L=Tiziopoli, O=Dinkel, CN=dinkel.brot.dg…
          Subject Public Key Info:
              Public Key Algorithm: rsaEncryption
              RSA Public Key: (1024 bit)
                  Modulus (1024 bit):
                      00:ce:0d:cd:08:86:fd:b5:cb:14:56:51:04:73:38:
                      15:77:39:2d:3b:10:17:06:7c:64:0d:69:14:67:cd:
                  …
                      67:f7:ef:b1:71:af:24:77:64:66:64:0f:85:a6:64:
                      16:c2:69:26:59:0a:d9:4b:8d
                  Exponent: 65537 (0x10001)
          Attributes:
              unstructuredName         :Dinkel
              challengePassword        :super segretissimo
      Signature Algorithm: md5WithRSAEncryption
          8f:25:9f:68:3a:67:4c:6d:e6:eb:52:4a:ca:73:74:47:85:14:
          ca:d6:6c:6d:24:3b:6c:37:59:ec:f8:fb:0b:a9:74:d6:1c:0f:
      …
          02:60:16:fd:2e:9b:09:af:11:03:82:74:16:ae:57:a7:90:f5:
          e1:a5
```

44.5.2.4 Certificato fittizio

Per generare in proprio il certificato auto-firmato, in modo da attivare ugualmente il servizio anche se non si può dimostrare di essere chi si afferma di essere, si può aggiungere l'opzione '**-x509**'. Anche in questo caso vengono richieste tutte le informazioni già viste.

```
$ openssl req -new -x509 -key chiave_privata.pem ↩
↪         -out richiesta.pem [Invio]
```

In alcuni casi può essere necessario unire la chiave privata, in chiaro, assieme al certificato; questo accade in particolare quando si allestisce un servente HTTP Apache-SSL. Di solito la chiave privata non può essere cifrata, perché deve essere letta da un servizio autonomo che non può interrogare un utente. Si deve ottenere una cosa simile a quella seguente:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDzUS4vA9NPNGAhHp71jGLk9lyJ6GfFK2R+AtMmWDKWvwhVOA8l
eY13ouz6XW0ts7s91FYlSTbp0Ed5tLKHZFu8guuza3jzpqFE/wrW/eJ7/RYW0cOZ
…
+7JyXBGaA4Srn/iw9cUCQQDEr5yuQa426I6psxfvUiK+HKS2kfRBbKKHj2NYh6nv
GgMhY9NiG+SGEDfkOw9rIVifb9yXs6f4CajQTb4qVl2X
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCAQAwDQYJKoZIhvcNAQEEBQAwYTELMAkGA1UEBhMCcXExCzAJBgNV
BAgTAnd3MQswCQYDVQQHEwJlZTELMAkGA1UEChMCcnIxCzAJBgNVBAsTAnR0MQsw
…
3kNqIB5Iun0kdDqdJYQj9G5Ca+dlRCxrPY6bVCnlD3A8+RULjyGrT6D45QtoXKx+
quIhIni++XBHqe+RyWBD70XTWvw0+zoyrHNHG96k9eLlPIgHrQ==
-----END CERTIFICATE-----
```

L'aggregazione può essere fatta a mano (attraverso '**cat**'), oppure si può utilizzare un comando unico che crea la chiave privata (di dimensione predefinita) e anche il certificato autoprodotto:

```
$ openssl req -new -x509 -nodes -out certificato.pem ↩
↪         -keyout certificato.pem[Invio]
```

In questo esempio è stata usata l'opzione '**-keyout**' per dirigere la chiave privata nello stesso file del certificato; inoltre, è stata usata l'opzione '**-nodes**' per evitare la protezione della chiave che in questi casi deve essere usata in chiaro.

Come viene mostrato anche in seguito, il file del certificato, con o senza la chiave privata acclusa, deve essere raggiungibile attraverso un nome corrispondente al suo codice di controllo, con l'aggiunta dell'estensione '`.0`'. Questo valore si ottiene con un comando simile a quello che si vede:

```
$ openssl x509 -hash -noout -in certificato.pem[Invio]
```

Per generare un collegamento simbolico, come si fa di solito, si potrebbe usare il comando seguente:

```
$ ln -s certificato.pem `openssl x509 -hash -noout ↩
↪    -in certificato.pem`.0[Invio]
```

44.5.3 Cenni sulla configurazione di OpenSSL

«

La configurazione di OpenSSL si attua normalmente attraverso il file '`openssl.cnf`', il quale potrebbe trovarsi collocato nella directory '`/etc/ssl/`'. Osservandone il contenuto, si intuisce che il simbolo '**#**' serve a introdurre un commento, fino alla fine della riga relativa e che le righe vuote e quelle bianche vengono ignorate come i commenti; inoltre, si vede che le direttive del file sono degli assegnamenti a variabili, le quali, se necessario, si espandono con il prefisso '**$**'; infine, le direttive sono raggruppate in sezioni individuabili da un titolo tra parentesi quadre.

È importante osservare che le sezioni sono organizzate in modo gerarchico, a partire dai nomi dei comandi di OpenSSL. In pratica, per il comando '**`openssl req`**' si prende in considerazione la sezione '**`[ req ]`**', che poi può a sua volta richiamare altre sottosezioni.

Dal momento che è già stato mostrato in che modo si ottiene una richiesta di certificato, attraverso il comando '**`openssl req`**', vale la pena di dare un'occhiata a un estratto della configurazione relativa, per comprendere un po' meglio come leggere questo file.

```
[ req ]
default_bits            = 1024
default_keyfile         = privkey.pem
distinguished_name      = req_distinguished_name
attributes              = req_attributes
x509_extensions = v3_ca # The extentions to add to the self signed cert

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = AU
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Some-State

localityName                    = Locality Name (eg, city)
```

È importante osservare che alcune variabili vengono assegnate con il nome di una sottosezione; in questo caso si tratta in particolare di ***distinguished_name*** a cui viene attribuita la sottosezione '**`[ req_distinguished_name ]`**', all'interno della quale vengono definite le informazioni che sono richieste in fase di costruzione del certificato.

Nelle prossime sezioni viene mostrato come simulare la gestione di

un'autorità di certificazione attraverso OpenSSL. Il file di configurazione standard dovrebbe essere neutro rispetto a questo problema, incorporando una sezione '**[ca]**' particolare, utile per fare delle prove:

```
[ ca ]
default_ca      = CA_default            # The default ca section

####################################################################
[ CA_default ]

dir             = ./demoCA              # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/cacert.pem       # The CA certificate
serial          = $dir/serial           # The current serial number
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem# The private key
RANDFILE        = $dir/private/.rand    # private random number file
```

È importante osservare che la sezione '**[ca]**' contiene una sola direttiva, '**default_ca**', con la quale si specifica la sottosezione da prendere in considerazione. In questo caso, la sottosezione è denominata '**[CA_default]**' e viene mostrata solo in parte. Si intende che, volendo fare le cose sul serio, è sufficiente ricopiare la sottosezione '**[CA_default]**', anche più volte, attribuendogli nomi differenti, modificando eventualmente la direttiva '**default_ca**' in modo da selezionare la sottosezione preferita.

Per il momento è bene osservare che la variabile ***dir*** viene presa in considerazione espandendola con l'aggiunta del prefisso '**$**' ('**$dir**'), nei valori da assegnare ad altre variabili. Questa variabile serve a definire la directory di partenza a partire dalla quale

vanno collocati una serie di file che riguardano l'amministrazione dell'autorità di certificazione. Inizialmente, viene indicata una directory che appare volutamente improbabile, '`./demoCA/`', proprio per fare capire che prima di lavorare sul serio occorre pensarci bene e mettere mano alla configurazione. Comunque, per le simulazioni che si vogliono mostrare, vale la pena di creare le directory '`./demoCA/certs/`', '`./demoCA/newcerts/`', '`./demoCA/crl/`' e '`./demoCA/private/`', o altre directory equivalenti in base alla propria configurazione effettiva.

44.5.3.1 Politica dell'autorità di certificazione

Nella sezione che descrive il funzionamento del comando '**`openssl ca`**', deve apparire anche l'indicazione del tipo di politica che l'autorità di certificazione intende attuare per rilasciare i certificati. Naturalmente, quello che può essere definito qui è solo qualche aspetto che riguarda la definizione del nome distintivo del titolare. Quello che segue è un altro estratto del file di configurazione in cui si vede l'assegnamento del nome di una sottosezione alla variabile ***policy***.

```
policy                  = policy_match

# For the CA policy
[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ policy_anything ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
```

In questo caso, la sottosezione '**`[ policy_match ]`**' specifica che i campi del paese, della regione e dell'organizzazione, devono corrispondere con gli stessi dati del certificato dell'autorità di certificazione. In pratica, questo servirebbe a limitare l'accesso all'autorità soltanto a chi appartiene alla stessa area e anche alla stessa organizzazione (ciò fa pensare a un'autorità di certificazione aziendale, competente solo nell'ambito della propria azienda). Per il resto, solo il campo CN deve essere fornito, mentre gli altri sono facoltativi.

Sotto alla sottosezione appena descritta, appare anche un'altra sottosezione simile, con il nome '**`[ policy_anything ]`**', in cui verrebbe concesso quasi tutto, a parte l'obbligo di fornire il ***CN***.

44.5.4 Simulazione dell'allestimento e del funzionamento di un'autorità di certificazione

L'utilizzo di OpenSSL per la gestione di un'autorità di certificazione richiede la conoscenza di molti dettagli sul funzionamento di questo sistema. In generale, il file di configurazione predefinito consente di ottenere delle richieste di certificati o di generare dei certificati fittizi auto-firmati. In questo gruppo di sezioni si vuole mostrare schematicamente l'uso di OpenSSL nella gestione di un'autorità di certificazione, anche con qualche esempio, ma senza la pretesa di arrivare a ottenere dei certificati realistici.

44.5.4.1 Autorità di certificazione autonoma

La creazione di un'autorità di certificazione autonoma, ovvero di un'autorità principale (*root*), che non abbia ottenuto a sua volta un certificato da un'autorità di livello superiore, deve realizzare la sua chiave privata e il suo certificato auto-firmato. Diversamente, se dipendesse dalla certificazione di un'altra autorità, dovrebbe predisporre la propria richiesta, sottoporla all'autorità superiore da cui dovrebbe ottenere il certificato.

Viene mostrato nuovamente il procedimento necessario per creare la chiave privata. In questo caso si fa riferimento alla porzione di configurazione che è stata mostrata in precedenza, dove tutti i file utilizzati si articolano a partire dalla directory '`./demoCA/`'. In particolare, si suppone che '`./demoCA/private/.rand`' sia un file contenente informazioni casuali:

```
$ openssl genrsa -des3 -out ./demoCA/private/cakey.pem ↩
↪         -rand ./demoCA/private/.rand[Invio]
```

Ecco che in questo modo si ottiene la chiave privata nel file '`./demoCA/private/cakey.pem`', cifrata con l'algoritmo DES-triplo. Il certificato auto-firmato viene generato con il comando seguente, con il quale si ottiene il file '`./demoCA/cacert.pem`':

```
$ openssl req -new -x509 -days 730 ↩
↪         -key ./demoCA/private/cakey.pem ↩
↪         -out ./demoCA/cacert.pem [Invio]
```

Si osservi in particolare che è stato indicato espressamente il periodo di validità del certificato, in 730 giorni, pari a due anni. La visualizzazione del contenuto del certificato si può fare con il comando seguente:

```
$ openssl x509 -text -in ./demoCA/cacert.pem [Invio]
```

Il certificato, in quanto tale, va conservato anche nella directory destinata a contenere la copia di quelli rilasciati in qualità di autorità di certificazione. Dal pezzo di configurazione mostrato in precedenza, la directory in questione è '`./demoCA/certs/`'. Questi file devono avere un nome che inizia con il loro numero di serie; dal momento che il numero del certificato dell'autorità stessa è il numero zero, il file deve chiamarsi obbligatoriamente '`./demoCA/certs/00.pem`':

```
$ cp ./demoCA/cacert.pem ./demoCA/certs/00.pem [Invio]
```

Inoltre, i file in quella directory devono essere abbinati, ognuno, a un collegamento simbolico che esprime il codice di controllo del file stesso, più l'estensione '`.0`':

```
$ cd ./demoCA/certs [Invio]

$ ln -s 00.pem `openssl x509 -hash -noout -in 00.pem`.0 [Invio]
```

44.5.4.2 Rilascio di certificazioni

Per le operazioni di rilascio dei certificati, ovvero della firma di questi a partire dai file di richiesta relativi, occorre prendere confidenza con l'uso di alcuni file, contenenti rispettivamente l'indice dei certificati rilasciati e il numero di serie successivo che può essere utilizzato. Come già spiegato, i certificati rilasciati da un'autorità di certificazione hanno un numero seriale progressivo; in base al pezzo di configurazione mostrato in precedenza, questo numero viene conservato nel file '`demoCA/serial`'. Il numero in questione viene annotato secondo una notazione esadecimale, tradotta in caratteri normali, ma senza alcun prefisso. In pratica, dopo aver predisposto il certificato della stessa autorità, occorre mettere in questo file la riga seguente, conclusa da un codice di interruzione di riga finale e nulla altro:

```
01
```

La creazione dei certificati incrementa automaticamente questo numero;[14] inoltre, se non viene specificato il file da creare, si ottiene direttamente un file corrispondente al suo numero di serie, con l'aggiunta dell'estensione consueta, collocato nella directory prevista per l'accumulo provvisorio: '`demoCA/newcerts/`' nel caso della configurazione di esempio a cui si continua a fare riferimento.

La creazione di un certificato aggiorna anche il file che ne contiene l'indice, il quale potrebbe essere '`demoCA/index.txt`'. Inizialmente, dopo la creazione del certificato dell'autorità stessa, questo indice è semplicemente un file vuoto; con la creazione dei certificati successivi, viene aggiunta una riga per ognuno di questi, riga che va intesa come un record suddiviso in campi separati da un ca-

rattere di tabulazione **singolo**. Viene mostrato subito l'esempio del record relativo a un primo certificato (diviso in due righe per motivi tipografici):

```
V       001213190753Z           01      unknown     ↩
↪/C=IT/ST=Italia/O=Dinkel/CN=dinkel.brot.dg/Email=tizio@dinkel.brot.dg
```

Nell'esempio non si vede, ma c'è un terzo campo nullo prima del valore '**01**'. I campi hanno il significato seguente:

1. lo stato del certificato, attraverso una lettera: «R», revocato, «E», scaduto, «V», valido;
2. la data di scadenza, scritta attraverso una stringa di cifre numeriche terminate da una lettera «Z» maiuscola, dove le coppie di cifre rappresentano rispettivamente: anno, mese, giorno, ore, minuti, secondi ('***AAMMGGHHMMSS*Z**');
3. la data di revoca del certificato, scritta esattamente come nel caso del secondo campo, solitamente assente, a indicare che il certificato è ancora valido;
4. il numero di serie in esadecimale;
5. la collocazione del certificato (attualmente si tratta sempre della parola chiave '**unknown**');
6. i dati del titolare del certificato, ovvero il nome distintivo e l'indirizzo di posta elettronica di questo.

La creazione, ovvero la firma di un certificato si ottiene con il comando '**openssl ca**', fornendo in particolare il file contenente la richiesta. Per esempio, se si vuole accettare la richiesta costituita dal file '`richiesta.pem`', si potrebbe agire nel modo seguente:

```
$ openssl ca -in richiesta.pem[Invio]
```

Avendo indicato esclusivamente il nome del file che contiene la richiesta, le altre informazioni sono state prese dalla configurazione. In base a quanto previsto dall'esempio mostrato inizialmente, per la firma è stata usata la chiave contenuta nel file '`demoCA/private/cakey.pem`', il file del certificato è stato creato nella directory '`demoCA/newcerts/`', con un nome corrispondente al suo numero di serie e con la solita estensione '`.pem`', ma soprattutto, è stata usata la sezione predefinita nel file di configurazione, ovvero '**`[ CA_default ]`**'. Volendo dichiarare tutto in modo esplicito, lo stesso comando avrebbe dovuto essere espresso nel modo seguente:

```
$ openssl ca -name CA_default ↩
↪         -keyfile demoCA/private/cakey.pem ↩
↪         -in richiesta.pem ↩
↪         -out demoCA/newcerts/`cat demoCA/serial`[Invio]
```

Questo comando richiede alcune conferme:

```
  Using configuration from /usr/lib/ssl/openssl.cnf
  Check that the request matches the signature
  Signature ok
  The Subjects Distinguished Name is as follows
  countryName           :PRINTABLE:'IT'
  stateOrProvinceName   :PRINTABLE:'Italia'
  localityName          :PRINTABLE:'Tiziopoli'
  organizationName      :PRINTABLE:'Dinkel'
  commonName            :PRINTABLE:'dinkel.brot.dg'
  emailAddress          :IA5STRING:'tizio@dinkel.brot.dg'
  Certificate is to be certified until Dec 13 19:28:38 2000 GMT (365 days)

Sign the certificate? [y/n]:y[Invio]

1 out of 1 certificate requests certified, commit? [y/n]:y[Invio]

  …
  Data Base Updated
```

Una volta creato un certificato nel modo descritto, questo va collocato nella sua posizione definitiva, che in questo caso è la directory ‘`demoCA/certs/`’, dove va creato il solito collegamento simbolico che rappresenta il suo codice di controllo (come è già stato mostrato più volte).

44.5.4.3 Revoca dei certificati

Se si incontra la necessità di revocare dei certificati prima della loro scadenza normale, si deve pubblicare un elenco di revoca, o CRL (*Certificate revocation list*). Questo elenco si produce con OpenSSL a cominciare dalla modifica del file contenente l’elenco dei certificati (‘`./demoCA/index.txt`’), sostituendo la lettera «V» con la lettera «R» e inserendo la scadenza anticipata nel terzo campo. L’esempio seguente mostra il caso di due certificati che vengono revocati prima della scadenza:

```
R       001213192838Z   000113192840Z   01      unknown /C=IT/ST=Italia/…
R       001213202243Z   000113192840Z   02      unknown /C=IT/ST=Italia/…
```

Successivamente, basta usare il comando ‘**`openssl ca`**’, con l’opzione ‘**`-gencrl`**’:

```
$ openssl ca -gencrl -out ./demoCA/crl/crl.pem[Invio]
```

Con questo esempio, viene creato il file ‘`./demoCA/crl/crl.pem`’, contenente questo elenco di revoca, il cui contenuto può essere riletto con il comando seguente:

```
$ openssl crl -text -in ./demoCA/crl/crl.pem[Invio]
```

```
Certificate Revocation List (CRL):
        Version 1 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: /C=IT/ST=Italia/L=Treviso/O=Dinkel/CN=dinkel.brot.dg…
        Last Update: Jan 15 20:35:52 2000 GMT
        Next Update: Feb 14 20:35:52 2000 GMT
Revoked Certificates:
    Serial Number: 01
        Revocation Date: Jan 13 19:28:40 2000 GMT
    Serial Number: 02
        Revocation Date: Jan 13 19:28:40 2000 GMT
    Signature Algorithm: md5WithRSAEncryption
        32:e1:97:92:96:2f:0c:e4:df:bb:9c:82:a5:e3:5b:51:69:f5:
        51:ad:1b:b2:98:eb:35:a6:c8:7f:d9:29:1f:b2:1e:cc:da:84:
    …
        31:27:4a:21:4c:7a:bc:85:73:cd:ff:15:9d:cb:81:b3:0b:82:
        73:50
```

44.5.4.4 Conversione nei formati

In generale, con OpenSSL si lavora con file (richieste, certificati, elenchi di revoca, ecc.) in formato PEM, il quale è in pratica una forma compatta dei dati, utilizzando però solo il codice ASCII a 7 bit. Ci sono situazioni in cui è necessario convertire questo formato in un altro, oppure è necessario acquisire dei dati da un formato diverso dal solito. In generale, quando si usano comandi che possono ricevere dati in ingresso, o quando si devono generare dati in uscita, sempre relativi a certificati e affini, si possono usare rispettivamente le opzioni '**-inform**' e '**-outform**', seguite dalla sigla del formato (non sono disponibili sempre tutti). Vengono mostrati alcuni esempi.

```
$ openssl x509 -in certificato.pem -outform der ↩
↪         -out certificato.der [Invio]
```

In questo modo si ottiene la conversione del certificato

'certificato.pem' nel file 'certificato.der', che risulta in formato DER (binario).

```
$ openssl crl -in crl.pem -outform der -out crl.der[Invio]
```

Converte l'elenco di revoca 'crl.pem' in formato DER, nel file 'crl.der'.

44.6 Applicazioni che usano OpenSSL

«

Alcune versioni di applicazioni comuni che hanno a che fare con la comunicazione di dati, incorporano le funzionalità crittografiche di certificazione e crittografia SSL/TLS, in particolare quelle che utilizzano proprio le librerie OpenSSL. Per fortuna, per alcune di queste applicazioni c'è poco da aggiungere e qui si raccolgono le sole informazioni necessarie per poterle utilizzare.

Oltre alle applicazioni predisposte per il protocollo SSL/TLS, si aggiungono dei programmi che fungono da proxy TCP,[15] per dare queste funzionalità ai servizi che non le hanno già. Tuttavia, proprio perché intervengono solo a livello del protocollo TCP, può essere impossibile l'utilizzo di questi quando il protocollo finale prevede l'apertura di connessioni aggiuntive attraverso porte non prestabilite. In pratica, diventa impossibile il loro uso per servizi FTP.

44.6.1 Aggiornare l'elenco dei servizi

«

Le varianti SSL/TLS dei servizi più comuni, prevedono porte di comunicazione diverse da quelle standard. In particolare, se il proprio file '/etc/services' non è già stato predisposto, è necessario aggiungere le righe seguenti, dove i commenti sono ovviamente opzionali:

```
https           443/tcp         # http TLS/SSL
https           443/udp
ssmtp           465/tcp         # smtp TLS/SSL
ssmtp           465/udp
nntps           563/tcp         # nttp TLS/SSL
nntps           563/udp
telnets         992/tcp         # telnet TLS/SSL
telnets         992/udp
imaps           993/tcp         # imap4 TLS/SSL
imaps           993/udp
ircs            994/tcp         # irc TLS/SSL
ircs            994/udp
pop3s           995/tcp         # POP3 TLS/SSL
pop3s           995/udp
ftps-data       989/tcp         # ftp TLS/SSL
ftps-data       989/udp
ftps            990/tcp         # ftp TLS/SSL
ftps            990/udp
```

È proprio l'utilizzo di queste porte che fa intendere ai servizi in ascolto che si intende instaurare una connessione protetta. Per fare un esempio comune, il fatto di utilizzare un URI che inizi per *https://* implica la richiesta di utilizzare un tunnel SSL/TLS per la certificazione e la crittografia, al contrario di un URI *http://* normale; inoltre, nello stesso modo, il protocollo HTTPS è precisamente il protocollo HTTP nel tunnel SSL/TLS.

44.6.2 Opzioni comuni

Di solito, le applicazioni che incorporano le funzionalità SSL attraverso le librerie di OpenSSL, consentono l'uso dell'opzione '**-z**', alla quale va aggiunto un argomento. La tabella 44.71 mostra sinteticamente l'uso di questa opzione aggiuntiva.

Figura 44.71. Alcune opzioni comuni ai programmi che usano le librerie di OpenSSL.

Opzione	Descrizione
`-z ssl`	Utilizza esclusivamente il protocollo SSL.
`-z secure`	Se fallisce la negoziazione SSL non passa a una connessione normale.
`-z verify=`***n***	Definisce il livello di verifica della certificazione.
`-z cert=`***file***	Definisce il file contenente il certificato.
`-z key=`***file***	Definisce il file contenente la chiave privata RSA.
`-z cipher=`***elenco***	Definisce l'elenco di algoritmi crittografici preferiti.

44.6.3 Certificati dei servizi

«

In generale, per attivare un servizio che consente l'utilizzo del protocollo SSL, occorre che questo disponga di una chiave privata e di un certificato. In particolare, il certificato dovrebbe essere ottenuto da un'autorità di certificazione, ma in mancanza di questo lo si può creare in proprio. I programmi in questione, dal momento che offrono un servizio in modo autonomo, hanno la necessità di accedere alla chiave privata, senza poter interrogare l'amministratore. Di conseguenza, tale chiave non può essere protetta e di solito viene creato un file unico sia per la chiave privata, sia per il certificato.

Il file contenente il certificato e la chiave, ha solitamente un nome corrispondente a quello dell'applicazione, con l'aggiunta dell'estensione '`.pem`', collocato normalmente nella directory '`/etc/ssl/`

`certs/'`, o in un'altra simile. Supponendo che la directory da utilizzare sia proprio questa, si può generare in proprio il certificato dell'applicazione «prova», incorporando anche la chiave privata, nel modo seguente:

```
# cd /etc/ssl/certs [Invio]

# openssl req -new -x509 -nodes -out prova.pem ↩
↪         -keyout prova.pem [Invio]

# chmod 0600 prova.pem [Invio]

# ln -s prova.pem ↩
↪       `openssl x509 -noout -hash -in prova.pem`.0 [Invio]
```

Dal momento che deve essere creata una chiave privata non protetta, altrimenti il servizio non potrebbe funzionare, il file che si genera non deve avere alcun permesso di accesso per gli utenti estranei, esattamente come si vede nell'esempio.

Dal momento che si tratta di un certificato che serve a identificare un servizio, il campo ***CN*** deve contenere il nome a dominio completo attraverso il quale vi si accede.

Di solito, la directory in cui vengono collocati i certificati di questi servizi, non dipende dalla configurazione di OpenSSL. In effetti, a parte il problema di crearli, questi vengono poi gestiti dai servizi stessi: sono questi servizi che eventualmente devono essere configurati per poter ritrovare i loro certificati.

44.6.4 Telnet-SSL

«

Esiste anche una versione di Telnet in grado di utilizzare il tunnel SSL.[16] In generale non c'è alcun problema di configurazione, a parte la necessità di disporre di un certificato, completo di chiave privata in chiaro, rappresentato di solito dal file '`telnetd.pem`', che dovrebbe essere generato automaticamente dal programma di installazione e inserito probabilmente nella directory '`/etc/ssl/certs/`'. Eventualmente, questo file (e il collegamento simbolico relativo) può essere ricostruito attraverso i comandi già visti all'inizio del capitolo.

Una volta installato il demone '**`in.telnetd`**' e il programma cliente '**`telnet`**' nella versione SSL, non serve altro. Al massimo, è il caso di verificare che il cliente sia in grado di connettersi con un servizio SSL. Il modo migliore è quello di farlo attraverso un altro servizio basato su SSL di cui si è già sicuri. L'esempio seguente mostra una connessione con un servente HTTPS, dal quale si preleva la pagina di ingresso al sito; si osservi in particolare l'uso dell'opzione '**`-z ssl`**' per utilizzare espressamente il protocollo SSL:

```
$ telnet -z ssl dinkel.brot.dg https [Invio]

GET / HTTP/1.0 [Invio]

[Invio]
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Dec 1999 16:42:41 GMT
Server: Apache/1.3.3 Ben-SSL/1.29 (Unix) Debian/GNU
Connection: close
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
 <HEAD>
  <TITLE>Index of /</TITLE>
 </HEAD>
 <BODY>
<H1>Index of /</H1>
...
</BODY></HTML>
Connection closed by foreign host.
```

È interessante notare che la connessione TELNET cifrata via SSL può essere negoziata anche attraverso la porta 23 normale. In alternativa, si può distinguere l'avvio del servente TELNET, nell'ambito della configurazione del supervisore dei servizi di rete, in modo da usare o meno la comunicazione cifrata. L'esempio seguente si riferisce a Inetd, con il file '`/etc/inetd.conf`':

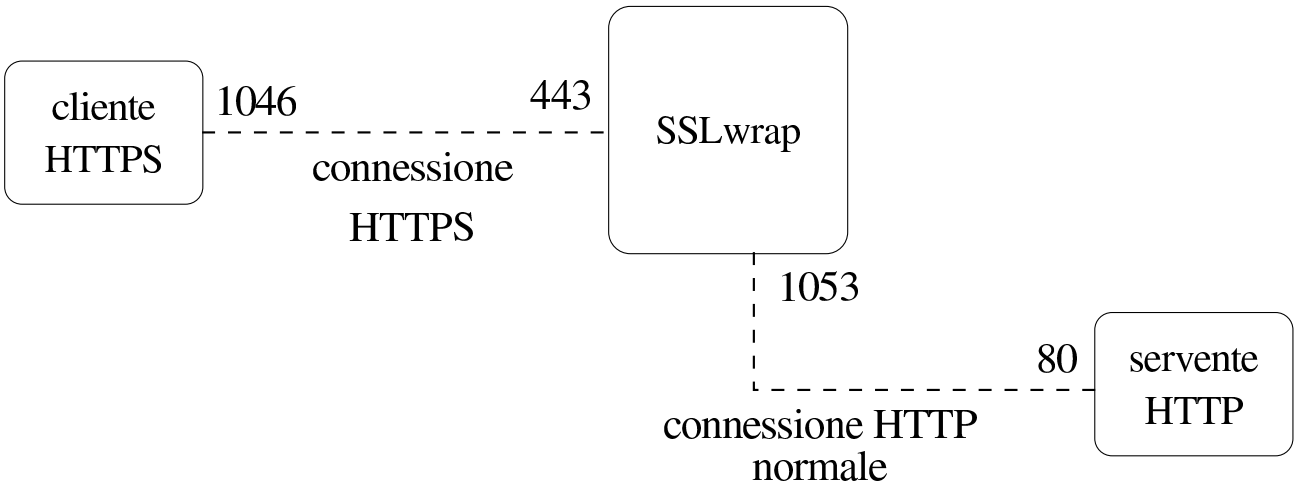
```
…
telnet   stream tcp nowait root /usr/sbin/tcpd  /usr/sbin/in.telnetd
telnets  stream tcp nowait root /usr/sbin/tcpd  /usr/sbin/in.telnetd -z secure
…
```

44.6.5 SSLwrap

SSLwrap[17] è un tunnel SSL/TLS che si inserisce al di sopra di servizi già esistenti che però non sono in grado di gestire direttamente questa funzionalità. In altri termini si tratta di un proxy che, ricevendo

connessioni attraverso le porte SSL/TLS, ripete le richieste ai servizi reali attraverso le porte normali.

Figura 44.74. Principio di funzionamento di SSLwrap.



La figura 44.74 mostra schematicamente un esempio di ciò che avviene. In particolare si vede l'uso delle porte, dove i numeri 1046 e 1053 sono solo un esempio di porte non privilegiate, utilizzate dinamicamente.

Da quanto espresso si dovrebbe intendere anche che SSLwrap può funzionare in un elaboratore distinto rispetto a quello che ospita i servizi per i quali è stato attivato. Naturalmente, nel tragitto che collega SSLwrap al servizio reale, i dati viaggiano in chiaro.

Un effetto collaterale dell'utilizzo di SSLwrap sta nel fatto che i servizi reali si trovano a comunicare sempre con lo stesso nodo, senza sapere da dove vengono realmente le richieste di connessione e senza poter applicare alcuna politica di filtro. SSLwrap è in grado di funzionare sia attraverso il controllo del supervisore dei servizi di rete, sia in modo indipendente; tuttavia, attraverso il supervisore dei servizi di rete e poi anche il TCP wrapper è possibile attuare le consuete politiche di filtro e di controllo degli accessi, anche attraverso il protocollo IDENT.

SSLwrap si compone dell'eseguibile '**sslwrap**', il quale svolge il ruolo di demone, autonomo o sottoposto al controllo del supervisore dei servizi di rete.

```
sslwrap [opzioni] -port porta-servizio-originale ↩
↪       [-accept porta-servizio-ssl]
```

Lo schema sintattico mostra in particolare l'uso obbligato dell'opzione '**-port**', con la quale si specifica la porta del servizio originale, a cui ridirigere le richieste che invece provengono dalla porta SSL corrispondente. Si vede anche che l'opzione '**-accept**' permette di stabilire il numero di porta SSL da utilizzare per attendere le richieste; porta che non va indicata se si opera attraverso il controllo del supervisore dei servizi di rete (perché in tal caso i dati provengono dallo standard input).

In condizioni normali, si presume che il servizio standard sia collocato nello stesso nodo in cui è in funzione SSLwrap, per cui si intende implicitamente che si tratti di 127.0.0.1. Diversamente si deve utilizzare l'opzione '**-addr**'.

La tabella 44.75 elenca le opzioni più importanti della riga di comando di '**sslwrap**'.

Tabella 44.75. Alcune opzioni della riga di comando di '**sslwrap**'.

Opzione	Descrizione
`-addr` ***indirizzo-ip***	Indirizzo IP del servizio originale.

Opzione	Descrizione
`-port` ***porta***	Porta del servizio originale.
`-accept` ***porta***	Porta SSL per ricevere le richieste.
`-verify`	Attiva la verifica del certificato della controparte.
`-Verify`	La controparte deve avere un certificato valido.
`-cert` ***file***	Certificato in formato PEM.
`-key` ***file***	Chiave privata in formato PEM (se non è già nel certificato).
`-without_pid`	Non crea il file contenente il numero del processo.

È probabile che la propria distribuzione sia organizzata in modo tale da configurare interattivamente il funzionamento di SSLwrap, aggiornando il file '`/etc/inetd.conf`' (nel caso si utilizzi Inetd come supervisore dei servizi di rete), oppure predisponendo gli script necessari nell'ambito della procedura di inizializzazione del sistema. Tuttavia, vale la pena di vedere ugualmente cosa si dovrebbe fare intervenendo manualmente.

Qui si presume che si utilizzi un certificato unico, completo di chiave privata, corrispondente al file '`/etc/ssl/certs/sslwrap.pem`'.

Nel caso del funzionamento sotto il controllo del supervisore dei servizi di rete, basta modificare il file '`/etc/inetd.conf`' aggiungendo le righe seguenti, che qui appaiono tutte spezzate a metà per motivi tipografici:

```
https           stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 80  -without_pid
```

```
ssmtp           stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 25  -without_pid
nntps           stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 119 -without_pid
telnets         stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 23  -without_pid
imaps           stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 143 -without_pid
ircs            stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 194 -without_pid
pop3s           stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 110 -without_pid
ftps-data       stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 20  -without_pid
ftps            stream  tcp     nowait  root    /usr/sbin/tcpd    ↩
↪/usr/sbin/sslwrap  -cert /etc/ssl/certs/sslwrap.pem -port 21  -without_pid
```

Naturalmente, non è necessario attivare tutti i presunti servizi SSL, eventualmente commentando le righe che non servono.[18] Inoltre, nel caso che i servizi reali si trovino in un altro elaboratore, si può aggiungere l'opzione '**`-addr`**', come già descritto.

Per utilizzare '**`sslwrap`**' come demone autonomo, si può usare un comando simile a quello seguente, che si riferisce al caso del protocollo HTTPS:

```
# sslwrap -cert /etc/ssl/certs/sslwrap.pem -port 80 ↩
↪         -accept 443 & [Invio]
```

Logicamente, questo e altri comandi simili per gli altri servizi SSL vanno messi convenientemente in uno script adatto alla procedura di inizializzazione del sistema.

44.6.6 Stunnel

Stunnel[19] è un tunnel SSL/TLS che si inserisce al di sopra di servizi già esistenti che però non sono in grado di gestire direttamente questa funzionalità. Ma in aggiunta a quanto fa già SSLwrap, può

essere usato anche per la funzionalità opposta, a vantaggio di un cliente che non è in grado di gestire da solo il protocollo SSL/TLS. In particolare, Stunnel non può essere messo sotto il controllo del supervisore dei servizi di rete, mentre può controllare i programmi che lo stesso supervisore dei servizi di rete gestisce.

Stunnel si compone dell'eseguibile '**`stunnel`**', che svolge il ruolo di demone autonomo, in grado di contattare un servizio già in ascolto di una porta TCP o di avviare un programma come fa il supervisore dei servizi di rete.

```
stunnel [opzioni]
```

Tabella 44.77. Alcune opzioni della riga di comando di '**`stunnel`**'.

Opzione	Descrizione
`-c`	Modalità «cliente»: il cliente si connette in chiaro e il servizio originale è SSL/TLS.
`-T`	Proxy trasparente, quando il sistema lo consente.
`-p` *file*	Certificato in formato PEM, il quale però non si usa nella modalità «cliente».
`-v [1|2|3]`	Attiva la verifica del certificato.
`-v 1`	Verifica il certificato della controparte se presente.
`-v 2`	Verifica il certificato della controparte.

Opzione	Descrizione
`-v 3`	Verifica la controparte con i certificati disponibili localmente.
`-a` ***directory***	Directory contenente i certificati per la verifica '**`-v 3`**'.
`-d` ***porta***	Porta di ascolto per le richieste di connessione.
`-l` ***programma*** [`--` ***argomenti***]	Avvio di un programma compatibile con il supervisore dei servizi di rete.
`-r` [***indirizzo-ip*** `:`] ***porta***	Servizio remoto da contattare.

Stunnel non ha una destinazione di utilizzo ben precisa, per cui occorre decidere prima cosa farne e quindi intervenire in modo appropriato nella configurazione del sistema. In generale, trattandosi di un demone che può funzionare solo in modo autonomo, non si deve intervenire nella configurazione del supervisore dei servizi di rete; al massimo si possono predisporre degli script per la procedura di inizializzazione del sistema. Vengono mostrati alcuni esempi, tenendo conto che il certificato riferito al servente si trova nel file '`/etc/ssl/certs/stunnel.pem`'.

- `# stunnel -p /etc/ssl/certs/stunnel.pem -d 443 -r 80` [*Invio*]

  In questo caso, molto semplice, si avvia il demone in modo da dare al servizio HTTP locale la possibilità di essere raggiunto attraverso il protocollo HTTPS. In pratica, il demone resta in ascolto della porta locale 443, per connessioni SSL/TLS, funzionando come proxy nei confronti della porta locale 80, con la quale la comunicazione avviene in chiaro.

- # **stunnel -p /etc/ssl/certs/stunnel.pem -d 443 ↩**
  ↪ **-r 192.168.1.2:80** [*Invio*]

  Come nell'esempio precedente, ma il servizio HTTP si trova in un nodo preciso, 192.168.1.2, il quale si presume essere diverso da quello locale.

- # **stunnel -c -d 80 -r 192.168.1.5:443** [*Invio*]

  Il demone funziona in modalità cliente in attesa di connessioni in chiaro attraverso la porta locale 80, mentre contatta per converso la porta 443, nel nodo 192.168.1.5, utilizzando in questo caso la crittografia SSL/TLS.

- # **stunnel -p /etc/ssl/certs/stunnel.pem -d 993 ↩**
  ↪ **-l /usr/sbin/imapd -- imapd** [*Invio*]

  Il demone resta in ascolto della porta 993 (IMAPS) e utilizza lo standard output per comunicare con una copia di '**imapd**', in chiaro. Si osservi la necessità di ripetere il nome del demone '**imapd**' come primo argomento dello stesso.

- # **stunnel -p /etc/ssl/certs/stunnel.pem -d 993 ↩**
  ↪ **-l /usr/sbin/tcpd -- /usr/sbin/imapd** [*Invio*]

  Come nell'esempio precedente, ma aggiungendo il controllo da parte del TCP wrapper.

44.7 OpenSSH

«

Secure Shell, ovvero SSH, è software proprietario, benché non lo fosse all'inizio della sua storia. Dai sorgenti originali di Secure Shell, delle edizioni originariamente «libere», si sono sviluppati diversi lavori alternativi, in cui sono stati eliminati in particolare gli algoritmi crittografici più problematici da un punto di vista legale.

Tra questi lavori alternativi spicca quello conosciuto come OpenSSH,[20] che ha mantenuto molte affinità con il software originale di Secure Shell.

OpenSSH può gestire due tipi diversi di protocolli SSH, identificati come versione 1 e versione 2. In generale si considera più sicura la versione 2, ma esistono ancora molti programmi clienti che sono in grado di comunicare solo con la prima versione.

L'utilizzo di una o dell'altra versione ha delle conseguenze nella configurazione e nel modo di generare le chiavi; pertanto, negli esempi si cerca di richiamare l'attenzione a tale riguardo.

44.7.1 Preparazione delle chiavi

La prima cosa da fare per attivare e utilizzare OpenSSH è la creazione della coppia di chiavi pubblica e privata per il servente, cosa che si ottiene con l'ausilio del programma '**`ssh-keygen`**'. Queste chiavi vanno memorizzate normalmente nei file '`/etc/ssh/ssh_host_key`' e '`/etc/ssh/ssh_host_key.pub`', dove in particolare la chiave privata (il primo dei due file) non deve essere protetto con una parola d'ordine.

Dal momento che questa coppia di chiavi viene realizzata in modo diverso a seconda del protocollo SSH usato, può essere conveniente predisporre tre coppie di file: '`/etc/ssh/ssh_host_key[.pub]`' per una coppia RSA adatta al protocollo 1; '`/etc/ssh/ssh_host_rsa_key[.pub]`' e '`/etc/ssh/ssh_host_dsa_key[.pub]`' per una coppia RSA e DSA adatte al protocollo 2.

Eventualmente può essere necessario creare un'altra coppia di file anche nei clienti che intendono sfruttare un'autenticazione RHOST+RSA, anche in questo caso, senza parola d'ordine. Infine, ogni utente che vuole utilizzare un'autenticazione RSA pura e semplice deve generare una propria coppia di chiavi, proteggendo possibilmente la chiave privata con una parola d'ordine.

Quando si creano coppie di chiavi da collocare nell'ambito della propria directory personale, se ne prepara solitamente una coppia sola, decidendo implicitamente la versione del protocollo SSH che poi deve essere usato per quello scopo.

Il modello sintattico complessivo di '**`ssh-keygen`**' è molto semplice e si può riassumere così:

```
ssh-keygen [opzioni]
```

Il suo scopo è quello di generare e modificare una coppia di chiavi in altrettanti file distinti: uno per la chiave privata, che eventualmente può essere anche cifrata, e uno contenente la chiave pubblica, a cui generalmente viene aggiunta l'estensione '`.pub`'.

La cifratura della chiave privata viene fatta generalmente perché questa non possa essere rubata; infatti, se non si utilizza questa precauzione, occorre fare in modo che nessuno possa riuscire a raggiungere il file in lettura. In pratica, una chiave privata di un utente comune, **deve** essere sempre cifrata, perché l'utente '**`root`**' potrebbe accedere al file corrispondente.

La coppia di chiavi che si genera, sia nel file della parte privata, sia in quello della parte pubblica, può contenere un commento utile ad annotare lo scopo di quella chiave. Convenzionalmente, viene generato automaticamente un commento corrispondente all'indirizzo di posta elettronica dell'utente che l'ha generata.

In corrispondenza della creazione di una chiave, viene generato anche il file '`~/.ssh/random_seed`', che serve come supporto alla creazione di chiavi sufficientemente «casuali». Ogni volta che lo stesso utente genera una nuova chiave, il vecchio file '`~/.ssh/random_seed`' viene riutilizzato e aggiornato di conseguenza.

Il file '`~/.ssh/random_seed`' e quelli delle chiavi private, devono essere accessibili solo all'utente proprietario.

Segue l'elenco delle opzioni più comuni:

`-b` ***n_bit***	permette di definire la dimensione della chiave in bit, tenendo conto che la dimensione minima è di 768 bit, mentre il valore predefinito è di 2048, ritenuto sufficiente per un livello di sicurezza normale;
`-f` ***file***	permette di definire esplicitamente il nome del file della chiave privata da generare, dove poi il nome della chiave pubblica è ottenuto semplicemente con l'aggiunta dell'estensione '`.pub`';
`-p`	consente di modificare la parola d'ordine che protegge una chiave privata già esistente, in modo interattivo;

`-N` ***parola_d'ordine***	permette di indicare la parola d'ordine da usare per proteggere la chiave privata nella riga di comando;

`-t rsa1`
`-t rsa`
`-t dsa`
	permette di specificare il tipo di chiavi da generare, tenendo conto che il tipo '**`rsa1`**' è utilizzabile solo per la versione 1 del protocollo SSH, mentre gli altri due tipi sono adatti alla versione 2.

A seconda del tipo di chiavi che si generano, i file predefiniti hanno un nome differente, allo scopo di consentire la gestione simultanea di tutti i tipi di chiave disponibili:

'`~/.ssh/identity`' '`~/.ssh/identity.pub`'	per una coppia di chiavi RSA adatta alla versione 1 del protocollo SSH;
'`~/.ssh/id_rsa`' '`~/.ssh/id_rsa.pub`'	per una coppia di chiavi RSA adatta alla versione 2 del protocollo SSH;
'`~/.ssh/id_dsa`' '`~/.ssh/id_dsa.pub`'	per una coppia di chiavi DSA adatta alla versione 2 del protocollo SSH.

Una volta installato OpenSSH, se si intende far funzionare il servente in modo da accettare tutti i tipi di protocollo, vanno create le varie coppie di chiavi nella directory '`/etc/ssh/`', attraverso i passaggi seguenti. In particolare, si osservi che non si possono proteggere le chiavi private con una parola d'ordine, altrimenti il servente non potrebbe lavorare in modo autonomo.

`# ssh-keygen -t rsa1 ↩`
`↪-f /etc/ssh/ssh_host_key ↩`
`↪-N ''` [*Invio*]
	Crea la coppia di chiavi RSA per la versione 1 del protocollo, nei file '`/etc/ssh/ssh_host_key`' e '`/etc/ssh/ssh_host_key.pub`'.

`# ssh-keygen -t rsa ↩`
`↪-f /etc/ssh/ssh_host_rsa_key ↩`
`↪-N ''` [*Invio*]
	Crea la coppia di chiavi RSA per la versione 2 del protocollo, nei file '`/etc/ssh/ssh_host_rsa_key`' e '`/etc/ssh/ssh_host_rsa_key.pub`'.

`# ssh-keygen -t dsa ↩`
`↪-f /etc/ssh/ssh_host_dsa_key ↩`
`↪-N ''` [*Invio*]
	Crea la coppia di chiavi DSA per la versione 2 del protocollo, nei file '`/etc/ssh/ssh_host_dsa_key`' e '`/etc/ssh/ssh_host_dsa_key.pub`'.

Naturalmente, se lo si desidera, si può usare anche l'opzione '**-b**' per specificare una lunghezza della chiave diversa dal valore predefinito.

L'utente comune che desidera creare le proprie coppie di chiavi, per utilizzare poi delle forme di autenticazione basate sul riconoscimento delle chiavi stesse, può agire secondo i passaggi seguenti, avendo cura di definire una parola d'ordine per proteggere le chiavi private. Si osservi che non viene indicato il nome dei file, perché si fa ri-

ferimento alle collocazioni predefinite. Naturalmente, anche in questo caso l'utente può usare l'opzione '**-p**' se intende ottenere una dimensione particolare della chiave.

# **ssh-keygen -t rsa1** [*Invio*]	Crea la coppia di chiavi RSA per la versione 1 del protocollo, nei file predefiniti '`~/.ssh/identity`' e '`~/.ssh/identity.pub`'.
# **ssh-keygen -t rsa** [*Invio*]	Crea la coppia di chiavi RSA per la versione 2 del protocollo, nei file predefiniti '`~/.ssh/id_rsa`' e '`~/.ssh/id_rsa.pub`'.
# **ssh-keygen -t dsa** [*Invio*]	Crea la coppia di chiavi DSA per la versione 2 del protocollo, nei file predefiniti '`~/.ssh/id_dsa`' e '`~/.ssh/id_dsa.pub`'.

44.7.2 Verifica dell'identità dei serventi

«

Nei clienti è possibile predisporre il file '`/etc/ssh/ssh_known_hosts`' con l'elenco delle chiavi pubbliche dei serventi a cui ci si collega frequentemente. In aggiunta, ogni utente dei clienti può avere il proprio file '`~/.ssh/known_hosts`', per le chiavi pubbliche che non siano già presenti nel file '`/etc/ssh/ssh_known_hosts`'.

Quando un cliente si collega la prima volta a un servente OpenSSH, se la sua chiave pubblica non è già stata inserita nel file '`/etc/ssh/`

`ssh_known_hosts`', viene proposto all'utente di aggiungere quella chiave pubblica nel file '`~/.ssh/known_hosts`'.

```
The authenticity of host 'dinkel.brot.dg (192.168.1.1)' can't be established.
RSA key fingerprint is dc:16:d5:2b:20:c5:2b:7b:69:1c:72:cc:d1:26:99:8b.
Are you sure you want to continue connecting (yes/no)?
```

`yes` [*Invio*]

```
Host 'dinkel.brot.dg' added to the list of known hosts.
```

In un secondo momento, se per qualche motivo la chiave di un servente, già conosciuta in precedenza da un cliente (attraverso il file '`/etc/ssh/ssh_known_hosts`', oppure attraverso i file '`~/.ssh/known_hosts`'), dovesse essere cambiata, tale cliente non riconoscerebbe più il servente e avviserebbe l'utente:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now
(man-in-the-middle attack)!
It is also possible that the RSA host key has just been
changed. The fingerprint for the RSA key sent by the remote
host is
dc:16:d5:2b:20:c5:2b:7b:69:1c:72:cc:d1:26:99:8b.
Please contact your system administrator.
Add correct host key in /home/tizio/.ssh/known_hosts to get
rid of this message. Offending key in
/home/tizio/.ssh/known_hosts:6
RSA host key for localhost has changed and you have
requested strict checking. Host key verification failed.
```

In questo caso, come suggerisce il messaggio, è sufficiente modifi-

care il file '`~/.ssh/known_hosts`' alla sesta riga, per fare in modo che questo contenga il riferimento alla nuova chiave pubblica del servente.

Volendo intervenire a mano in questo file ('`~/.ssh/known_hosts`' o '`/etc/ssh/ssh_known_hosts`'), conviene conoscere come questo è organizzato. Il file può contenere commenti, rappresentati dalle righe che iniziano con il simbolo '**#**', righe vuote, che vengono ignorate ugualmente; per il resto si tratta di righe contenenti ognuna l'informazione sulla chiave pubblica di un servente particolare. Queste righe significative sono composte in uno dei modi seguenti, dove i vari elementi sono separati da uno o più spazi.

nodo lunghezza_della_chiave esponente modulo

nodo tipo_di_chiave chiave_pubblica

Tanto per fare un esempio, l'ipotetico elaboratore *linux.brot.dg* potrebbe richiedere la riga seguente (abbreviata per motivi tipografici) per una chiave RSA adatta al protocollo SSH versione 1:

```
…
roggen.brot.dg 1024 35 136994665376544565821…04907660021407562333675433
…
```

Oppure, potrebbe trattarsi di una riga simile a quella seguente per una chiave RSA adatta al protocollo SSH versione 2:

```
…
roggen.brot.dg ssh-rsa AAAAB3NzaC1yc2EAAAAB…IwAAAgEAnhvScnWn3hCXk7W90=
…
```

Evidentemente, data la dimensione delle chiavi, è improbabile che

queste vengano ricopiate attraverso la digitazione diretta. Questi dati vengono ritagliati normalmente dal file della chiave pubblica a cui si riferiscono. A titolo di esempio, i file delle chiavi pubbliche corrispondenti a quanto già mostrato, avrebbero potuto essere composti dalla riga:

```
…
1024 35 136994665376544565821…04907660021407562333675433 root@roggen.brot.dg
…
```

oppure:

```
…
ssh-rsa AAAAB3NzaC1yc2EAAAAB…IwAAAgEAnhvScnWn3hCXk7W90= root@roggen.brot.dg
…
```

Comunque, quando si vuole intervenire nel file ‘`/etc/ssh/ssh_known_hosts`’, anche se questa operazione può avvenire solo in modo manuale, rimane sempre la possibilità di ottenere la prima volta l’aggiornamento automatico del file ‘`~/.ssh/known_hosts`’, dal quale poi si può tagliare e incollare quanto serve nel file ‘`/etc/ssh/ssh_known_hosts`’, senza altre modifiche.

44.7.3 Autenticazione RHOST

L’autenticazione RHOST, come già accennato, è un metodo semplice e insicuro di autenticare l’accesso attraverso la tecnica dei file ‘`/etc/hosts.equiv`’ e ‘`~/.rhosts`’ già utilizzata da ‘**`rlogin`**’. In alternativa a questi file, OpenSSH può utilizzare la coppia ‘`/etc/ssh/shosts.equiv`’ e ‘`~/.shosts`’, in modo da poter essere configurato indipendentemente da ‘**`rlogin`**’ e ‘**`rsh`**’.

Perché questa tecnica di autenticazione possa essere utilizzata, è necessario configurare ‘**`sshd`**’, ovvero il demone di OpenSSH. Diver-

samente, in modo predefinito, l'autenticazione RHOST non viene concessa.

È bene sottolineare l'accesso facilitato basato sull'autenticazione RHOST è assolutamente sconsigliabile e la sua disponibilità si giustifica solo per motivazioni storiche collegate all'uso di programmi come Rsh. In ogni caso, occorre considerare che OpenSSH non consente di usare questo sistema di autenticazione se i permessi di accesso ai file di configurazione relativi non sono abbastanza ristretti. Pertanto, il più delle volte, quando si tenta di sfruttare il sistema RHOST, l'autenticazione fallisce.

L'esempio seguente mostra il contenuto del file '`/etc/ssh/shosts.equiv`', oppure di '`/etc/hosts.equiv`', di un elaboratore per il quale si vuole consentire l'accesso da parte di *dinkel.brot.dg* e di *roggen.brot.dg*.

```
dinkel.brot.dg
roggen.brot.dg
```

In questo modo, gli utenti dei nodi *dinkel.brot.dg* e *roggen.brot.dg* possono accedere al sistema locale senza la richiesta formale di alcuna identificazione, purché esista per loro un utente con lo stesso nome.

L'elenco di nodi equivalenti può contenere anche l'indicazione di utenti particolari, per la precisione, ogni riga può contenere il nome di un nodo seguito eventualmente da **uno spazio** e dal nome di un utente. Si osservi l'esempio seguente:

```
dinkel.brot.dg
roggen.brot.dg
dinkel.brot.dg tizio
dinkel.brot.dg caio
```

Come nell'esempio precedente, viene concesso agli utenti dei nodi *dinkel.brot.dg* e *roggen.brot.dg* di accedere localmente attraverso lo stesso nominativo utilizzato nei sistemi remoti. In aggiunta a questo, però, viene concesso agli utenti '**`tizio`**' e '**`caio`**' del nodo *dinkel.brot.dg*, di accedere identificandosi con il nome di qualunque utente, senza la richiesta di alcuna parola d'ordine.

Si può intuire che fare una cosa del genere significa concedere a tali utenti privilegi simili a quelli che ha l'utente '**`root`**'. In generale, tali utenti non dovrebbero essere in grado di utilizzare UID molto bassi, comunque ciò non è un buon motivo per configurare in questo modo il file '`/etc/ssh/shosts.equiv`' o '`/etc/hosts.equiv`'.

Indipendentemente dal fatto che il file '`/etc/ssh/shosts.equiv`', oppure '`/etc/hosts.equiv`', sia presente o meno, ogni utente può predisporre il proprio file '`~/.shosts`', oppure '`~/.rhosts`'. La sintassi di questo file è la stessa di '`/etc/ssh/shosts.equiv`' (e di '`/etc/hosts.equiv`'), ma si riferisce esclusivamente all'utente che predispone tale file nella propria directory personale.

In questo file, l'indicazione di utenti precisi è utile e opportuna, perché quell'utente potrebbe disporre di nominativi-utente differenti sui nodi da cui vuole accedere.

```
dinkel.brot.dg tizi
roggen.brot.dg tizio
```

L'esempio mostra l'indicazione precisa di ogni nominativo-utente dei nodi che possono accedere senza richiesta di identificazione.[21]

44.7.4 Autenticazione RHOST sommata al riconoscimento della chiave pubblica

«

L'autenticazione RHOST può essere sommata a quella del riconoscimento della chiave pubblica, utilizza gli stessi file già visti nell'autenticazione RHOST normale, ma in più richiede che il cliente sia riconosciuto. Perché ciò avvenga, occorre che il cliente abbia una propria chiave, cioè abbia definito la coppia di file '`/etc/ssh/ssh_host_key`' e '`/etc/ssh/ssh_host_key.pub`', e che la sua parte pubblica sia annotata nel file '`/etc/ssh/ssh_known_hosts`' del servente, oppure nel file '`~/.ssh/known_hosts`' riferito all'utente che dal cliente vuole accedere.

In generale, non è necessario questo tipo di autenticazione mista, la quale di solito è anche disabilitata in modo predefinito. Infatti, è sufficiente che sia disponibile un'autenticazione basata sul controllo della chiave pubblica, senza altre restrizioni.

44.7.5 Autenticazione basata sul controllo della chiave pubblica

«

L'autenticazione basata sul controllo della chiave pubblica, pura e semplice, permette di raggiungere un livello di garanzia ulteriore. Per il suo utilizzo, l'utente deve creare una propria coppia

di chiavi per ogni tipo di protocollo che intenda usare (i file '`~/.ssh/identity`' e '`~/.ssh/identity.pub`', oppure '`~/.ssh/id_rsa`' e '`~/.ssh/id_rsa.pub`', oppure '`~/.ssh/id_dsa`' e '`~/.ssh/id_dsa.pub`') presso l'elaboratore cliente. Data la situazione, come è già stato descritto, è opportuno che la chiave privata sia protetta con una parola d'ordine.

Per accedere a un servente utilizzando questo tipo di autenticazione, occorre che l'utente aggiunga nel file '`~/.ssh/authorized_keys`' presso il servente, le sue chiavi pubbliche definite nel nodo cliente.

Perché il sistema di autenticazione basato sulla verifica delle chiavi funzioni, è necessario che i permessi dei file coinvolti e delle stesse directory non consentano l'intromissione di estranei. In particolare, può darsi che venga rifiutato questo tipo di autenticazione se la directory personale o anche solo '`~/.ssh/`' dispongono dei permessi di scrittura per il gruppo proprietario.

L'utente che utilizza il sistema di autenticazione basato sul controllo della chiave pubblica, potrebbe usare le stesse chiavi da tutti i clienti da cui intende accedere al servente, oppure potrebbe usare chiavi differenti, aggiungendole tutte al file '`~/.ssh/authorized_keys`' del servente.

Quando si stabilisce una connessione con questo tipo di autenticazione, se la chiave privata dell'utente è cifrata attraverso una parola d'ordine, si ottiene un messaggio come quello seguente:

```
Enter passphrase for RSA key 'tizio@roggen.brot.dg':
```

Diversamente, se le chiave privata coinvolta non è cifrata, per l'accesso non è richiesto altro.

In pratica, per concedere l'accesso attraverso questa forma di autenticazione, è sufficiente aggiungere nel file '`~/.ssh/authorized_keys`' le chiavi pubbliche delle utenze che interessano, prelevandole dai file '`~/.ssh/id*.pub`' contenuti nei nodi clienti rispettivi.

L'esempio seguente mostra un ipotetico file '`~/.ssh/authorized_keys`' contenente il riferimento a sei chiavi. La parte finale, quella alfabetica, è la descrizione della chiave, il cui unico scopo è quello di permetterne il riconoscimento a livello umano.

```
1024 33 12042598236…28121136693267811750183946 71 tizio@roggen.brot.dg
ssh-rsa AAAAB3NzaC1…erMIqmsserVBqIuP1JHUivfY7VU= tizio@dinkel.brot.dg
ssh-dss AAAAB3NzaC1…kc3MgA83UkVTtCLsS42GBGR3wA== tizio@dinkel.brot.dg
1024 33 13485193076…78116723252836146045720169 19 caio@dinkel.brot.dg
ssh-rsa AAAAB3NzaC1…erGTRDbMIqmssIuP1JHUivfY7VU= caio@dinkel.brot.dg
ssh-dss AAAAB3NzaC1…kc3MgA8HYjGrDCLsS42GBGR3wA== caio@dinkel.brot.dg
```

In realtà, le righe di questo file potrebbero essere più complesse, con l'aggiunta di un campo iniziale, contenente delle opzioni. Queste opzioni, facoltative, sono rappresentate da direttive separate da una virgola e senza spazi aggiunti. Eventualmente, le stringhe contenenti spazi devono essere racchiuse tra coppie di apici doppi; inoltre, se queste stringhe devono contenere un apice doppio, questo può essere indicato proteggendolo con la barra obliqua inversa ('`\"`').

`from="`***elenco_modelli***`"`	Permette di limitare l'accesso. Con un elenco di modelli, eventualmente composto con dei metacaratteri ('**`*`**', '**`?`**'), si possono indicare i nomi dei nodi a cui è concesso oppure è negato l'accesso. Per la precisione, i modelli che iniziano con un punto esclamativo si riferiscono a nomi cui l'accesso viene vietato espressamente.
`command="`***comando***`"`	Permette di abbinare una chiave a un comando. In pratica, chi accede utilizzando questa chiave, invece di una shell ottiene l'esecuzione del comando indicato e subito dopo la connessione ha termine. Di solito, si abbina questa opzione a '**`no-pty`**' e a '**`no-port-forwarding`**'.
`no-port-forwarding`	Vieta espressamente l'inoltro del TCP/IP.
`no-X11-forwarding`	Vieta espressamente l'inoltro del protocollo X11.
`no-pty`	Impedisce l'allocazione di uno pseudo terminale (pseudo TTY).

Vengono mostrati alcuni esempi nell'elenco seguente.

`from="*.brot.dg,!schwarz.brot.dg" ↩` `↪1024 35 234…56556 tizio@dinkel.brot.dg`	Concede l'accesso con la chiave indicata, solo al dominio *brot.dg*, escludendo espressamente il nome *schwarz.brot.dg*.

`command="ls" 1024 35 2346543…8757465456556 ↩` `↪tizio@dinkel.brot.dg`	Chi tenta di accedere utilizzando questa chiave, ottiene semplicemente l'esecuzione del comando '**`ls`**' nella directory corrente, cioè la directory personale dell'utente corrispondente.

`command="tar czpf ↩`
`↪/home/tizio/backup/lettere.tar.gz ↩`
`↪/home/tizio/lettere" ↩`
`↪1024 35 234…56556 tizio@dinkel.brot.dg`
	Chi tenta di accedere utilizzando questa chiave, ottiene semplicemente l'archiviazione della directory '`/home/tizio/lettere/`'.

`command="ls",no-port-forwarding,no-pty ↩`
`↪1024 35 2346543…8757465456556 ↩`
`↪tizio@dinkel.brot.dg`
	Chi tenta di accedere utilizzando questa chiave, ottiene semplicemente l'esecuzione del comando '**`ls`**'; inoltre, per sicurezza viene impedito l'inoltro del TCP/IP e l'allocazione di uno pseudo TTY.

44.7.6 Autenticazione normale

«

Quando OpenSSH non è in grado di eseguire alcun altro tipo di autenticazione, ripiega nell'uso del sistema tradizionale, in cui viene richiesta la parola d'ordine abbinata al nominativo-utente con cui si vuole accedere.

Ciò rappresenta anche l'utilizzo normale di OpenSSH, il cui scopo principale è quello di garantire la sicurezza della connessione attra-

verso la cifratura e il riconoscimento del servente. Infatti, per ottenere questo livello di funzionamento, è sufficiente che nel servente venga definita la chiave, attraverso i file '`/etc/ssh/ssh_host_key`' e '`/etc/ssh/ssh_host_key.pub`', mentre nei clienti non serve nulla, a parte l'installazione di OpenSSH.

Quando un utente si connette per la prima volta a un servente determinato, da un cliente particolare, la chiave pubblica di quel servente viene annotata automaticamente nel file '`~/.ssh/known_hosts`', permettendo il controllo successivo su quel servente.

Quindi, attraverso l'autenticazione normale, tutti i problemi legati alla registrazione delle varie chiavi pubbliche vengono risolti in modo automatico e quasi trasparente.

44.7.7 Servente OpenSSH

Il servizio di OpenSSH viene offerto tramite un demone, il programma '**`sshd`**', il quale deve essere avviato durante l'inizializzazione del sistema, oppure, se compilato con le opzioni necessarie, può essere messo sotto il controllo del supervisore dei servizi di rete. Tuttavia, generalmente si preferisce avviare '**`sshd`**' in modo indipendente dal supervisore dei servizi di rete, perché a ogni avvio richiede un po' di tempo per la generazione di chiavi aggiuntive utilizzate per la cifratura.

La sintassi per l'utilizzo di questo demone si può riassumere semplicemente nel modello seguente:

```
sshd [opzioni]
```

Il programma '**sshd**', una volta avviato e dopo aver letto la sua configurazione, si comporta in maniera un po' diversa, a seconda che sia stato abilitato l'uso della versione 1 o 2 del protocollo SSH.

In generale, quando un cliente si connette, '**sshd**' avvia una copia di se stesso per la nuova connessione, quindi, attraverso la chiave pubblica del servente inizia una sorta di negoziazione che porta alla definizione di un algoritmo crittografico da usare e di una chiave simmetrica che viene scambiata tra le parti, sempre in modo cifrato. Successivamente, si passa alla fase di autenticazione dell'utente, secondo uno dei vari metodi già descritti, in base a quanto stabilito nella configurazione di '**sshd**'. Infine, il cliente richiede l'avvio di una shell o di un altro comando.

OpenSSH ignora il file '`/etc/securetty`', per cui gli accessi dell'utente '**root**' possono essere regolati solo attraverso la configurazione del file '`/etc/ssh/sshd_config`'.

Vengono descritte alcune opzioni di '**sshd**':

`-f` ***file_di_configurazione***	Permette di fare utilizzare a '**sshd**' un file di configurazione differente da quello standard, ovvero '`/etc/ssh/sshd_config`'.
`-h` ***file_della_chiave_del_nodo***	Permette di fare utilizzare a '**sshd**' una chiave del nodo diversa da quella contenuta nel file standard. Si deve indicare solo il nome della chiave privata, intendendo che il nome del file contenente la chiave pubblica si ottiene con l'aggiunta dell'estensione '`.pub`'.

`-d`	Fa sì che '**sshd**' funzioni in primo piano, allo scopo di seguire una sola connessione per verificarne il funzionamento.
`-e`	Si usa in abbinamento con '**-d**', per ottenere le informazioni diagnostiche attraverso lo standard error.

Il file di configurazione '`/etc/ssh/sshd_config`' permette di definire il comportamento di '**sshd**'. Il file può contenere righe di commento, evidenziate dal simbolo '**#**' iniziale, righe vuote (che vengono ignorate) e righe contenenti direttive, composte da coppie ***nome valore***, spaziate, senza alcun simbolo di assegnamento.

Quello che segue è un file '`/etc/ssh/sshd_config`' tipico, adatto per le due versioni del protocollo SSH, in modo simultaneo:

```
# La porta usata per ricevere le richieste di comunicazione.
Port 22

# Direttive per restringere l'accessibilità del servizio.
#ListenAddress ::
#ListenAddress 0.0.0.0

# Definizione delle versioni del protocollo utilizzabili.
Protocol 2,1

# Collocazione della coppia di chiavi per il protocollo 1.
HostKey /etc/ssh/ssh_host_key

# Collocazione delle coppie di chiavi per il protocollo 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key

# Durata di validità per la chiave generata automaticamente
```

```
# per la versione 1.
KeyRegenerationInterval 3600
ServerKeyBits 768

# Livello di informazioni nel registro
SyslogFacility AUTH
LogLevel INFO

# Autenticazione
LoginGraceTime 600
PermitRootLogin yes
StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Disabilita l'autenticazione RHOSTS e la sua combinazione
# con il sistema della chiave pubblica.
RhostsAuthentication no
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
IgnoreUserKnownHosts yes

# Non consente l'uso di parole d'ordine vuote.
PermitEmptyPasswords no

# Uncomment to disable s/key passwords
#ChallengeResponseAuthentication no

# Consente l'autenticazione basata sul riconoscimento della
# parola d'ordine.
PasswordAuthentication yes
```

```
# Use PAM authentication via keyboard-interactive so PAM
# modules can properly interface with the user.
PAMAuthenticationViaKbdInt yes

# To change Kerberos options.
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#AFSTokenPassing no
#KerberosTicketCleanup no

# Kerberos TGT Passing does only work with the AFS kaserver.
#KerberosTgtPassing yes

X11Forwarding no
X11DisplayOffset 10
PrintMotd no
#PrintLastLog no
KeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net
#ReverseMappingCheck yes

Subsystem       sftp    /usr/lib/sftp-server
```

Si osservi che i nomi usati nelle direttive sono sensibili alla differenza tra maiuscole e minuscole. Segue la descrizione di alcune direttive di configurazione.

`Protocol` ***n*** [, ***m***] ...	Consente di indicare quali versioni del protocollo SSH utilizzare.

`AllowUsers` ***modello***… `Deny` ***modello***…	Queste due direttive permettono di definire uno o più modelli (attraverso l'uso dei metacaratteri '**`*`**' e '**`?`**') riferiti a nomi di utenti a cui si intende concedere, oppure vietare l'accesso. Se queste direttive non vengono usate, si concede a qualunque utente di accedere.
`HostKey` ***file***	Questa direttiva può essere usata anche più volte, per indicare i file contenenti le chiavi private del nodo. L'utilizzo multiplo della direttiva serve proprio per indicare chiavi diverse, adatte ai diversi protocolli.
`LoginGraceTime` ***durata***	Permette di stabilire il tempo massimo concesso per completare la procedura di accesso. Il valore predefinito è di 600 s, pari a 10 minuti.
`PasswordAuthentication` ↩ ↪`{yes|no}`	Stabilisce se l'autenticazione attraverso la parola d'ordine è consentita oppure no. Il valore predefinito è '**`yes`**', cosa che permette questo tipo di autenticazione.
`PermitEmptyPasswords` ↩ ↪`{yes|no}`	Se l'autenticazione attraverso una parola d'ordine è consentita, permette di stabilire se sono ammesse le parole d'ordine nulle. Il valore predefinito è '**`yes`**'.

`PermitRootLogin {yes↩ ↪|without-password↩ ↪|forced-commands-only|no}`	Permette di abilitare o meno l'accesso da parte dell'utente '**root**'. Il valore predefinito è '**yes**' che consente questo accesso in qualunque forma di autenticazione, '**no**' lo esclude in ogni caso, mentre '**without-password**' esclude solo la forma di autenticazione attraverso una parola d'ordine e '**forced-commands-only**' consente di eseguire solo dei comandi remoti, sempre escludendo l'autenticazione basata sulla parola d'ordine.
`IgnoreRhosts {yes|no}`	Permette di ignorare i file '`~/.rhosts`' e '`~/.shosts`', mentre, per quanto riguarda questa direttiva, i file '`/etc/hosts.equiv`' e '`/etc/shosts.equiv`' continuano a essere presi in considerazione. Il valore predefinito è '**no**'.
`RhostsAuthentication ↩ ↪{yes|no}`	Permette di abilitare o meno l'autenticazione RHOST, cioè quella basata esclusivamente sul file '`/etc/hosts.equiv`' (o '`/etc/shosts.equiv`') ed eventualmente '`~/.rhosts`' (o '`~/.shosts`'). Per motivi di sicurezza, il valore predefinito è '**no**', per non autorizzare questa forma di autenticazione.

`RhostsRSAAuthentication {yes|no}`	Permette di abilitare o meno l'autenticazione RHOST sommata al riconoscimento della chiave pubblica, per il protocollo della versione 1. Il valore predefinito è '**no**', per non autorizzare questa forma di autenticazione.
`HostbasedAuthentication {yes|no}`	Permette di abilitare o meno l'autenticazione RHOST sommata al riconoscimento della chiave pubblica, per il protocollo della versione 2. Il valore predefinito è '**no**', per non autorizzare questa forma di autenticazione.
`IgnoreUserKnownHosts {yes|no}`	Permette di ignorare i file '`~/.ssh/known_hosts`' degli utenti, durante l'autenticazione basata su RHOST sommata al riconoscimento della chiave pubblica. Il valore predefinito è '**no**', con il quale i file in questione vengono letti regolarmente.
`RSAAuthentication {yes|no}`	Permette di abilitare o meno l'autenticazione basata sulle chiavi di ogni singolo utente, per quanto riguarda la versione 1 del protocollo. Il valore predefinito è '**no**' che esclude questa forma di autenticazione.

`PubkeyAuthentication ↩ ↪{yes|no}`	Permette di abilitare o meno l'autenticazione basata sulle chiavi di ogni singolo utente, per quanto riguarda la versione 2 del protocollo. Il valore predefinito è '**yes**' che consente questa forma di autenticazione.
`StrictModes {yes|no}`	Se attivato, fa in modo che '**sshd**' verifichi la proprietà dei file di configurazione nelle directory personali degli utenti, rifiutando di considerare i file appartenenti a utenti «sbagliati» o con permessi non appropriati. Ciò permette di ridurre i rischi di intrusione e alterazione della configurazione da parte di terzi che potrebbero sfruttare le dimenticanze degli utenti inesperti per sostituirsi a loro. Il valore predefinito è '**yes**'.

44.7.8 Cliente OpenSSH

Il programma usato come cliente per le connessioni con OpenSSH è '**ssh**', il quale emula il comportamento del suo predecessore, '**rsh**', almeno per ciò che riguarda la sintassi fondamentale. A fianco di '**ssh**' ci sono anche '**scp**' e '**sftp**' per facilitare le operazioni di copia tra elaboratori.

Il programma '**ssh**' richiede una configurazione che può essere fornita in modo globale a tutto il sistema, attraverso il file '`/etc/ssh/`

`ssh_config`' e in modo particolare per ogni utente, attraverso il file '`~/.ssh/config`'.

Il modello sintattico per l'utilizzo di '**`ssh`**', si esprime semplicemente nel modo seguente:

```
ssh [opzioni] nodo [comando]
```

L'utente può essere riconosciuto nel sistema remoto attraverso uno tra diversi tipi di autenticazione, a seconda delle reciproche configurazioni; al termine dell'autenticazione, l'utente ottiene una shell oppure l'esecuzione del comando fornito come ultimo argomento (come si vede dalla sintassi).

Tabella 44.98. Alcune opzioni di uso più frequente.

Opzione	Descrizione
`-l` ***utente***	Permette di richiedere l'accesso utilizzando il nominativo-utente indicato nell'argomento. Diversamente, si intende accedere con lo stesso nominativo usato nel cliente dal quale si utilizza '**`ssh`**'.
`-i` ***file_di_identificazione***	Permette di fare utilizzare a '**`ssh`**' una chiave di identificazione personale diversa da quella contenuta nel file standard, ovvero '`~/.ssh/id*`' (e poi anche '`~/.ssh/id*.pub`'). Si deve indicare solo il nome della chiave privata, intendendo che il nome del file contenente la chiave pubblica si ottiene con l'aggiunta dell'estensione '`.pub`'.
`-1`	Richiede espressamente l'uso del protocollo nella versione 1.

Opzione	Descrizione
`-2`	Richiede espressamente l'uso del protocollo nella versione 2.
`-4`	Utilizza indirizzi IPv4.
`-6`	Utilizza indirizzi IPv6.

Seguono alcuni esempi di utilizzo di '**ssh**'.

- `$` **ssh -l tizio roggen.brot.dg** [*Invio*]

  Accede all'elaboratore *roggen.brot.dg*, utilizzando lì il nominativo-utente '**tizio**'.

- `$` **ssh -l tizio roggen.brot.dg ls -l /tmp** [*Invio*]

  Esegue il comando '**ls -l /tmp**' nell'elaboratore *roggen.brot.dg*, utilizzando lì il nominativo-utente '**tizio**'.

- `$` **ssh -l tizio roggen.brot.dg** ↩
  ↪ **tar czf - /home/tizio > backup.tar.gz** [*Invio*]

  Esegue la copia di sicurezza, con l'ausilio di '**tar**' e '**gzip**' ('**tar**' con l'opzione '**z**'), della directory personale dell'utente '**tizio**' nell'elaboratore remoto. L'operazione genera il file '`backup.tar.gz`' nella directory corrente dell'elaboratore locale.

A proposito dell'esempio con cui si esegue una copia di sicurezza attraverso la rete, è bene sottolineare che il file generato, contiene dei caratteri aggiuntivi oltre la fine del file. Ciò può causare delle segnalazioni di errore quando si estrae il file compresso, ma il contenuto dell'archivio dovrebbe risultare intatto.

La configurazione di '**ssh**' può essere gestita globalmente attraverso il file '`/etc/ssh/ssh_config`' e singolarmente attraverso '`~/.ssh/config`'.

Il file può contenere righe di commento, evidenziate dal simbolo '**#**' iniziale, righe vuote (che vengono ignorate) e righe contenenti direttive, composte da coppie ***nome valore***, oppure ***nome=valore***.

In questi file di configurazione possono essere distinte diverse sezioni, riferite a gruppi di nodi. Ciò si ottiene attraverso la direttiva '**Host** ***modelli***', in cui, anche attraverso i metacaratteri '*****' e '**?**', si indicano i nodi a cui sono riferite le direttive successive, fino alla prossima direttiva '**Host**'.

Quello che segue è il file '`/etc/ssh/ssh_config`' tipico, tutto commentato, ma utile ugualmente per comprenderne il funzionamento.

```
# Host *
#   ForwardAgent no
#   ForwardX11 no
#   RhostsAuthentication no
#   RhostsRSAAuthentication yes
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   FallBackToRsh no
#   UseRsh no
#   BatchMode no
#   CheckHostIP yes
#   StrictHostKeyChecking yes
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_rsa
#   Port 22
#   Protocol 2,1
```

```
#   Cipher blowfish
#   EscapeChar ~
```

Anche in questo caso, si deve ricordare che i nomi usati nelle direttive sono sensibili alla differenza tra maiuscole e minuscole.

Tabella 44.100. Alcune direttive.

Direttiva	Descrizione
`Cipher {des|3des↩ ↪|blowfish|none}`	Permette di indicare il tipo di cifratura preferita per il protocollo della versione 1. Se si specifica il tipo '**none**' si intende di non volere alcun tipo di cifratura, cosa utile solo a scopo di analisi diagnostica.
`Ciphers` ***tipo_cifratura***`↩ ↪[ , tipo_cifratura ] ...`	Consente di indicare un elenco di cifrature utilizzabili per il protocollo della versione 2.
`Compression {yes|no}`	Se attivato, permette di utilizzare una comunicazione di dati compressa, in modo da migliorare il rendimento di una connessione lenta. Il valore predefinito è '**no**'.
`IdentityFile` ***file***	Permette di indicare il file contenente la chiave privata dell'utente, in alternativa a quello standard. Questa direttiva si può usare anche più volte, per fare riferimento a coppie di chiavi distinte per i vari tipi di protocolli.

Direttiva	Descrizione

`Protocol` ***n*** `[,` ***m*** `]…`
 	
`RhostsAuthentication {yes|no}`
 	
`RhostsRSAAuthentication {yes|no}`
 	
`RSAAuthentication {yes|no}`
 	
`PubkeyAuthentication {yes|no}`
 	
`PasswordAuthentication {yes|no}`
	Queste direttive hanno lo stesso significato e utilizzo di quelle corrispondenti alla configurazione del servente.

`StrictHostKeyChecking {yes|no|ask}`	Se attivato, fa in modo che le chiavi pubbliche dei serventi contattati non possano essere aggiunte automaticamente nell'elenco personale, il file '`~/.ssh/known_hosts`', impedendo la connessione a nodi sconosciuti o irriconoscibili. Il valore predefinito è '**`ask`**', con cui si chiede all'utente come comportarsi.

Direttiva	Descrizione
`User` ***utente***	Permette di indicare l'utente da utilizzare nella connessione remota. Ciò è particolarmente utile nella configurazione personalizzata, in cui si potrebbe specificare l'utente giusto per ogni nodo presso cui si ha accesso.

Per copiare dei file in modo cifrato, si può usare '**`scp`**', il quale si avvale di '**`ssh`**' in modo trasparente:

`scp` [***opzioni***] [[***utente*** `@`] ***nodo*** **:**] ***origine*** … [[***utente*** `@`] ***nodo*** **:**] ***destinazione***

Il principio di funzionamento è lo stesso della copia normale, con la differenza che i percorsi per identificare i file e le directory, sono composti con l'indicazione dell'utente e del nodo. Nella tabella successiva vengono descritte alcune opzioni.

Tabella 44.101. Alcune opzioni.

Opzione	Descrizione
`-p`	Fa in modo che gli attributi originali dei file vengano rispettati il più possibile nella copia.
`-r`	Permette la copia ricorsiva delle directory.
`-1`	Richiede espressamente l'uso del protocollo nella versione 1.
`-2`	Richiede espressamente l'uso del protocollo nella versione 2.
`-4`	Utilizza indirizzi IPv4.

Opzione	Descrizione
`-6`	Utilizza indirizzi IPv6.

Seguono alcuni esempi.

- `$` **`scp`** ↩
  ↪**`tizio@roggen.brot.dg:/etc/profile`** ↩
  ↪`.` [*Invio*]

  Copia il file '`/etc/profile`' dall'elaboratore *roggen.brot.dg* utilizzando il nominativo-utente '**`tizio`**', nella directory corrente dell'elaboratore locale.

- `$` **`scp -r`** ↩
  ↪**`tizio@roggen.brot.dg:/home/tizio/`** ↩
  ↪`.` [*Invio*]

  Copia tutta la directory '`/home/tizio/`' dall'elaboratore *roggen.brot.dg* utilizzando il nominativo-utente '**`tizio`**', nella directory corrente dell'elaboratore locale.

Quando si richiede un trasferimento di file più complesso e '**`scp`**' si mostra scomodo per i propri fini, si può optare per '**`sftp`**', il quale si comporta in modo simile a un programma cliente per il protocollo FTP, ma si avvale invece di un servente SSH compatibile con questa estensione.

Il servente OpenSSH può accettare connessioni attraverso '**sftp**' solo se nella sua configurazione è prevista tale gestione. Precisamente, nel file '`/etc/ssh/sshd_config`' deve essere presente la direttiva seguente:

```
Subsystem       sftp    /usr/lib/sftp-server
```

In pratica, per la gestione di questa funzionalità particolare, il demone '**sshd**' si avvale di un programma di appoggio, corrispondente a '**sftp-server**'.

La sintassi per l'utilizzo di '**sftp**' si articola in diverse forme differenti:

`sftp` [*opzioni*] *nodo*

`sftp` [*utente*]`@`*nodo*

`sftp` [*utente*]`@`*nodo*`:`*file*...

`sftp` [*utente*]`@`*nodo*`:`*directory*

In pratica, si può avviare '**sftp**' con l'indicazione di un nodo, assieme a delle opzioni eventuali; oppure si saltano le opzioni e si indicano dei file che si vogliono prelevare; infine si può indicare una directory di partenza che si vuole aprire immediatamente presso il nodo remoto, per i comandi da impartire successivamente in modo interattivo.

In generale, il comportamento di '**sftp**' è molto simile a quello di un cliente FTP tradizionale, con la differenza che la comunicazione avviene in modo cifrato (si veda eventualmente il capitolo 38). La tabella 44.102 elenca alcuni comandi che vengono utilizzati durante il funzionamento interattivo di '**sftp**'. Per altre informazioni, si può consultare la pagina di manuale *sftp(1)*.

Tabella 44.102. Alcuni comandi interattivi di '**sftp**'.

Comando	Descrizione
`bye` `quit`	I comandi '**bye**' e '**quit**' sono sinonimi e hanno lo scopo di terminare il collegamento e l'attività di '**sftp**'.
`help` `?`	Elenca i comandi disponibili.
`cd` [*directory_remota*]	Cambia la directory corrente nel sistema remoto.
`ls` [`-l`] [*directory_remota*]	Elenca il contenuto della directory remota specificata, oppure di quella corrente se non viene indicata.
`chmod` *permessi file_remoto*	Cambia i permessi sul file remoto.
`chown` *utente file_remoto*	Cambia l'utente proprietario del file remoto indicato.
`chgrp` *gruppo file_remoto*	Cambia il gruppo abbinato al file remoto indicato.

Comando	Descrizione
`mkdir` ***directory_remota***	Crea una directory nel sistema remoto.
`pwd`	Visualizza il nome della directory corrente del sistema remoto.
`ln` ***percorso_esistente collegamento_da_creare***	Crea un collegamento simbolico presso il sistema remoto.
`rename` ***nome_originale nome_nuovo***	Cambia il nome o sposta un file presso il sistema remoto.
`rm` ***file_remoto***	Cancella il file indicato presso il sistema remoto.
`rmdir` ***directory_remota***	Elimina la directory indicata presso il sistema remoto.
`lcd` [***directory_locale***]	Cambia la directory corrente nel sistema locale.
`lls` [`-l`] [***directory_locale***]	Elenca il contenuto della directory locale specificata, oppure di quella corrente se non viene indicata.
`lmkdir` ***directory_locale***	Crea una directory nel sistema locale.
`lpwd`	Visualizza il nome della directory corrente del sistema locale.

Comando	Descrizione
`!` [*comando* [*argomenti*]]	Avvia una shell sull'elaboratore locale, oppure esegue localmente il comando indicato con gli argomenti che gli vengono forniti.
`get` [`-P`] *file_remoto* [*file_locale*]	Riceve il file remoto indicato, eventualmente rinominandolo come indicato. Se si usa l'opzione '**`-P`**', vengono preservati i permessi originali.
`put` [`-P`] *file_locale* [*file_remoto*]	Invia il file locale indicato, eventualmente rinominandolo come indicato. Se si usa l'opzione '**`-P`**', vengono preservati i permessi originali.

44.7.9 Verifica del funzionamento di un servente OpenSSH

«

In condizioni normali, la configurazione tipica di OpenSSH consente delle connessioni dove il riconoscimento degli utenti avviene attraverso l'inserimento della parola d'ordine. Per ragioni di sicurezza, le forme di autenticazione «RHOST», ovvero quelle basate sull'uso dei file '`/etc/hosts.equiv`', '`/etc/shosts.equiv`', '`~/.rhosts`' e '`~/.shosts`', sono disabilitate.

Di solito, l'autenticazione basata sulla verifica della chiave pubblica è abilitata, ma si richiede che i permessi e la proprietà dei file relativi siano coerenti per il contesto a cui si riferiscono.

In generale, è bene evitare le forme di autenticazione RHOST, anche quando sono mediate dal riconoscimento concorrente della chiave pubblica; pertanto, se è necessario accedere senza l'indicazione di una parola d'ordine, il modo più corretto rimane quello del riconoscimento della chiave, senza altre interferenze.

Spesso, quando si cerca di realizzare una connessione senza bisogno di inserire la parola d'ordine, si incappa in qualche problema che impedisce di ottenere il risultato. Per scoprire dove sia il problema, è necessario avviare il demone '**sshd**' in modalità diagnostica, per seguire una connessione singola e vedere cosa succede veramente:

```
# sshd -e -d 2>&1 | less[Invio]
```

All'avvio, ciò che si ottiene sono i messaggi relativi allo stato della configurazione. Per esempio:

```
debug1: Seeding random number generator
debug1: sshd version OpenSSH_3.0.2p1 Debian 1:3.0.2p1-9
debug1: private host key: #0 type 0 RSA1
debug1: read PEM private key done: type RSA
debug1: private host key: #1 type 1 RSA
debug1: read PEM private key done: type DSA
debug1: private host key: #2 type 2 DSA
debug1: Bind to port 22 on 0.0.0.0.
Server listening on 0.0.0.0 port 22.
Generating 768 bit RSA key.
RSA key generation complete.
```

Se dal nodo *dinkel.brot.dg* l'utente '**tizio**' tenta di collegarsi, si può leggere, in particolare, l'estratto seguente:

```
Connection from 192.168.1.1 port 32773
…
debug1: trying public key file /home/tizio/.ssh/authorized_keys
```

```
debug1: matching key found: file /home/tizio/.ssh/authorized_keys, line 3
…
debug1: ssh_rsa_verify: signature correct
Accepted publickey for tizio from 192.168.1.1 port 32773 ssh2
debug1: Entering interactive session for SSH2.
```

In questo caso si evidenzia un'autenticazione basata sul riconoscimento della chiave pubblica. Ecco cosa potrebbe succedere invece se i permessi non vengono ritenuti adeguati:

```
debug1: trying public key file /home/tizio/.ssh/authorized_keys
Authentication refused: bad ownership or modes for directory /home/tizio
```

In questo caso, l'autenticazione basata sul riconoscimento della chiave pubblica, non funziona perché la directory personale dell'utente consente la scrittura al gruppo, pertanto si ricade nella solita autenticazione per mezzo della parola d'ordine.

44.7.10 X in un tunnel OpenSSH

«

OpenSSH è configurato in modo predefinito per gestire automaticamente le connessioni di X. Per comprenderlo è meglio fare subito un esempio pratico. Si immagini di avere avviato X sul proprio elaboratore locale e di avere aperto una finestra di terminale con la quale si effettua una connessione presso un sistema remoto, attraverso '**ssh**'. Dopo avere stabilito la connessione, si vuole avviare su quel sistema un programma che utilizza il servente grafico locale: basta avviarlo e tutto funziona, semplicemente, all'interno di un tunnel cifrato di OpenSSH.

Il meccanismo attuato da OpenSSH per arrivare a questo risultato è molto complesso, garantendo il funzionamento della connessione anche se le autorizzazioni per l'accesso al servente grafico locale non sono state concesse al sistema remoto.

Nel momento in cui si accede al sistema remoto attraverso '**ssh**' da una finestra di terminale di X, la controparte nel sistema remoto, cioè '**sshd**', genera o aggiorna il file '`~/.Xauthority`' nel profilo personale dell'utente utilizzato per accedere, attraverso il proprio canale privilegiato. Se dopo la connessione si prova a visualizzare il contenuto della variabile ***DISPLAY***, si dovrebbe osservare che viene indicato uno schermo speciale nel sistema remoto. Si osservi l'esempio:

```
tizio@dinkel.brot.dg:~$ ssh -l caio roggen.brot.dg[Invio]

caio's password: *****[Invio]
```

In questo modo, l'utente '**tizio**' che si trova presso il nodo *dinkel.brot.dg*, cerca di accedere a *roggen.brot.dg*, utilizzando lì il nominativo-utente '**caio**'. La prima volta che lo fa ottiene la creazione del file '`~/.Xauthority`' nel sistema remoto, come mostrato qui sotto:

```
 /usr/X11/bin/xauth: creating new authority file ↩
↪/home/caio/.Xauthority

caio@roggen.brot.dg:~$ echo $DISPLAY[Invio]

 roggen.brot.dg:10.0
```

Contrariamente al solito, lo schermo sembra essere collocato presso il sistema remoto, proprio perché è OpenSSH a gestire tutto. In questo modo però, non contano più le autorizzazioni o i divieti fatti attraverso la gestione normale di X. Inoltre, dal momento che la connessione di X è incapsulata nel protocollo SSH, non valgono più eventuali restrizioni poste nei router per impedire l'utilizzo di tale protocollo.

La connessione instaurata attraverso OpenSSH garantisce che la comunicazione riferita alla gestione del servente grafico sia protetta, risolvendo la maggior parte dei problemi di sicurezza derivati dall'uso di X attraverso la rete. Tuttavia, questo non garantisce che il sistema sia completamente sicuro, dal momento che un aggressore potrebbe collocarsi nel nodo remoto e da lì sfruttare il tunnel predisposto proprio da OpenSSH, come documentato in *The interaction between SSH and X11*, di Ulrich Flegel.

A questo punto, si potrebbe ritenere conveniente di vietare in ogni caso l'utilizzo delle applicazioni per X attraverso la rete, ma dal momento che OpenSSH scavalca i sistemi tradizionali, occorre configurare proprio OpenSSH per questo. In generale, se è questa l'intenzione, si agisce nel file '`/etc/ssh/sshd_config`', con la direttiva '**`X11Forwarding`**', in modo che '**`sshd`**' non si presti alla gestione di X nel modo descritto:

```
…
X11Forwarding no
…
```

Eventualmente, lo stesso utente può impedirsi di usare X attraverso OpenSSH, intervenendo nel file '`~/.ssh/config`' con la direttiva '**`ForwardX11`**':

```
…
ForwardX11 no
…
```

44.7.11 Creazione di un tunnel cifrato generico con OpenSSH

Il cliente OpenSSH è in grado di realizzare un tunnel cifrato tra due elaboratori, attraverso una tecnica chiamata *port forwarding*. In pratica si apre una connessione SSH normale, con o senza l'attivazione di una shell remota, nella quale si inserisce una comunicazione aggiuntiva che collega una porta remota con una porta locale. L'esempio seguente dovrebbe servire per comprendere la tecnica:

1. `tizio@roggen.brot.dg:~$` **`ssh -N -L 9090:dinkel.brot.dg:80 caio@dinkel.brot.dg`**[*Invio*]

   l'utente '**`tizio`**' presso l'elaboratore *roggen.brot.dg* si collega all'elaboratore *dinkel.brot.dg*, con l'utenza '**`caio`**', per aprire un tunnel tra *dinkel.brot.dg:80* e *roggen.brot.dg:9090*;

2. [*Ctrl z*]

   `tizio@roggen.brot.dg:~$` **`bg`**[*Invio*]

   dopo essersi identificato presso l'elaboratore remoto, sospende l'esecuzione del programma e quindi lo riattiva sullo sfondo;

3. `tizio@roggen.brot.dg:~$` **`links http://localhost:9090`**[*Invio*]

   A questo punto si può visitare il sito *http://dinkel.brot.dg:80* utilizzando invece l'indirizzo *http://localhost:9090*, garantendo che la comunicazione tra l'elaboratore locale (*roggen.brot.dg*) e *dinkel.brot.dg* avvenga in modo cifrato.

Tabella 44.110. Opzioni di '**ssh**' specifiche per la realizzazione di un tunnel tra l'elaboratore locale e un nodo remoto, dove sia disponibile un servente OpenSSH attivo.

Opzione	Descrizione
`-N`	Non esegue un comando presso l'elaboratore remoto.
`-L` ***porta_locale*** **:** ***nodo_remoto*** **:** ***porta_remota*** `-L` ***porta_locale*** **/** ***nodo_remoto*** **/** ***porta_remota***	Apre la porta locale indicata e ritrasmette le comunicazioni con questa porta alla porta dell'elaboratore remoto indicato. Se si apre localmente una porta privilegiata, occorre agire in qualità di utente '**root**' nell'elaboratore locale. La prima notazione riguarda IPv4, mentre la seconda riguarda IPv6.
`-R` ***porta_remota*** **:** ***nodo_locale*** **:** ***porta_locale*** `-R` ***porta_remota*** **/** ***nodo_locale*** **/** ***porta_locale***	Apre la porta remota indicata e ritrasmette le comunicazioni con questa porta a quella dell'elaboratore locale indicato. Se si apre una porta privilegiata remota, occorre agire in qualità di utente '**root**' nell'elaboratore remoto. La prima notazione riguarda IPv4, mentre la seconda riguarda IPv6.

44.7.12 Installazione

«

L'installazione di OpenSSH è semplice: si deve predisporre la chiave del nodo, come già descritto più volte; quindi, se si vogliono accettare connessioni, basta avviare il demone '**`sshd`**', possibilmente attraverso uno script della procedura di inizializzazione del sistema.

La configurazione è facoltativa e deve essere fatta solo se si desiderano inserire forme particolari di limitazioni (come nel caso del divieto dell'inoltro di X), oppure se si vuole concedere l'autenticazione RHOST (cosa che è meglio non fare).

Alcune versioni precompilate di OpenSSH sono organizzate in modo da utilizzare la directory '`/etc/ssh/`' per il file di configurazione del sistema (come è stato mostrato qui); altre mettono direttamente tali file nella directory '`/etc/`'.

44.8 VPN: virtual private network

«

Ciò che è noto come VPN (*virtual private network*), ovvero «rete privata virtuale», è un'estensione di una rete privata (LAN) per mezzo di un tunnel che attraversa una rete più grande (Internet). Il tunnel fa sì che si possa lavorare come se si trattasse di una sola rete locale, distinguendo se il collegamento avviene al secondo o al terzo livello del modello ISO/OSI, e di solito utilizza una tecnica di cifratura, per mantenere «privato» il contenuto dei dati che lo attraversano.

Quando esposto in questo capitolo riguarda principalmente i sistemi GNU/Linux e i tunnel considerati sono relativi al terzo livello del modello ISO/OSI.

44.8.1 Interfacce dei tunnel

«

Il tunnel necessario per la realizzazione di una rete privata virtuale, mostra alle sue estremità delle interfacce virtuali. Infatti, il tunnel funziona attraverso la connettività esistente, avvalendosi delle interfacce di rete reali; tuttavia, per creare l'astrazione della rete virtuale privata, si mostra come se ci fossero delle interfacce aggiuntive, software, collegate tra loro in un qualche modo imprecisato.

Le interfacce di rete virtuali tipiche di un tunnel sono di due tipi: TAP e TUN. Le interfacce virtuali «TAP» riproducono il funzionamento di un'interfaccia di rete fisica, al secondo livello del modello ISO/OSI. Le interfacce virtuali «TUN» (dove «tun» sta per «tunnel»), sono interfacce astratte che operano esclusivamente nel terzo livello del modello ISO/OSI.

Un tunnel tra due elaboratori relativamente «lontani», realizzato attraverso interfacce virtuali di tipo TAP, funziona come *bridge*, mentre un tunnel basato su interfacce virtuali di tipo TUN, va gestito attraverso la configurazione corretta degli instradamenti.

Nei sistemi GNU/Linux, la gestione di interfacce virtuali di tipo TUN/TAP richiede la presenza di un file di dispositivo apposito, rappresentato da '`/dev/net/tun`'. Quando si utilizza il sistema uDev per la gestione automatica dei file di dispositivo, questo dovrebbe essere già presente. Tuttavia, in caso di necessità, potrebbe essere creato con il comando seguente:

```
# mknod /dev/net/tun c 10 200 [Invio]
```

Nel kernel Linux può darsi che la funzionalità necessaria alla gestione di queste interfacce sia demandata a un modulo, il quale

eventualmente va attivato:

```
# modprobe tun [Invio]
```

Una volta creato un tunnel, le interfacce virtuali connesse alle sue estremità funzionano come se fossero le interfacce reali di una connessione punto-punto e va considerata la configurazione del filtro dei pacchetti, se da una delle parti si applica una politica di controllo di qualche tipo: in pratica, va verificata tale configurazione per consentire il traffico a cui si è interessati effettivamente.

Per esempio, per consentire l'ingresso di qualunque pacchetto attraverso qualunque interfaccia TUN, in un sistema GNU/Linux si potrebbe usare '**iptables**' nel modo seguente:

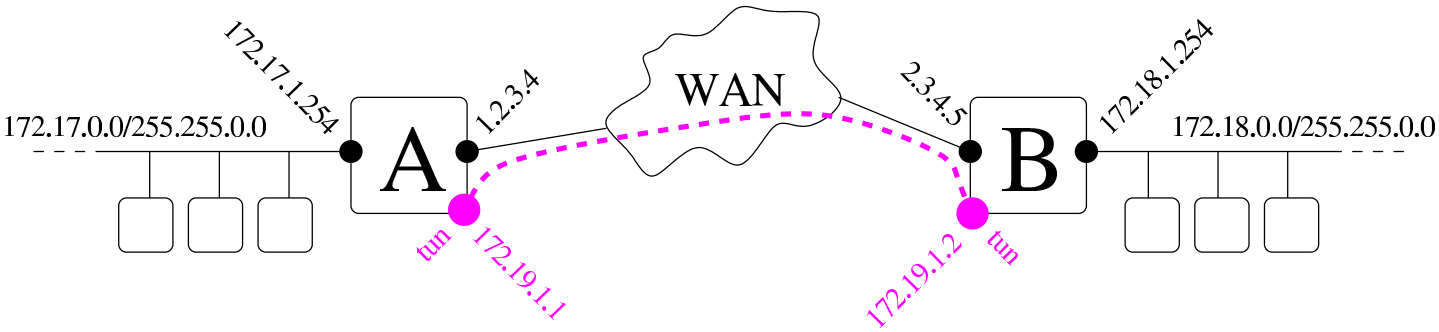
```
# iptables -A INPUT -i tun+ -j ACCEPT [Invio]
```

Lo stesso discorso può valere per l'attraversamento e l'uscita, in base alla politica che si intende attuare in relazione al filtro dei pacchetti. Ma naturalmente si può formulare il filtro in maniera differente, facendo riferimento solo agli indirizzi IP assegnati.

44.8.2 Introduzione a OpenVPN

OpenVPN[22] è un programma, funzionante in qualità di demone, in grado di realizzare un tunnel, cifrato o meno, al secondo o al terzo livello del modello ISO/OSI. OpenVPN consente di realizzare tunnel anche in condizioni avverse, ma qui si considerano solo le situazioni più semplici; in particolare ci si riferisce alla situazione rappresentata dal disegno successivo.

Figura 44.111. Due reti private connesse attraverso un tunnel, in modo da poter formare una sola rete locale estesa.



Il tunnel più semplice che possa essere realizzato tra i nodi «A» e «B», non cifrato, richiede i comandi seguenti, da eseguire rispettivamente presso il primo e il secondo nodo:

«A» # **openvpn --remote 2.3.4.5 --dev tun1** ↩
↪ **--ifconfig 172.19.1.1 172.19.1.2** [*Invio*]

«B» # **openvpn --remote 1.2.3.4 --dev tun1** ↩
↪ **--ifconfig 172.19.1.2 172.19.1.1** [*Invio*]

Dal nodo «A» e dal nodo «B» è possibile verificare la configurazione dell'interfaccia virtuale e l'instradamento relativo ottenuti:

«A» # **ifconfig** [*Invio*]

```
...
tun1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.19.1.1  P-t-P:172.19.1.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:588 (588.0 B)  TX bytes:588 (588.0 B)
...
```

«B» # **ifconfig** [*Invio*]

```
…
tun1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.19.1.2  P-t-P:172.19.1.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:588 (588.0 B)  TX bytes:588 (588.0 B)
…
```

«A» # **route -n** [*Invio*]

```
…
Kernel IP routing table
Destination  Gateway  Genmask         Flags Metric Ref  Use Iface
172.19.1.2   0.0.0.0  255.255.255.255 UH    0      0      0 tun1
…
```

«B» # **route -n** [*Invio*]

```
…
Kernel IP routing table
Destination  Gateway  Genmask         Flags Metric Ref  Use Iface
172.19.1.1   0.0.0.0  255.255.255.255 UH    0      0      0 tun1
…
```

A questo punto, tra i nodi «A» e «B» deve essere possibile comunicare e lo si può verificare inizialmente con un comando come '**ping**':

«A» # **ping 172.19.1.2** [*Invio*]

«B» # **ping 172.19.1.1** [*Invio*]

Tuttavia, per far sì che la rete «A», corrispondente nell'esempio agli indirizzi 172.17.∗.∗, possa comunicare con la rete «B», corrispondente agli indirizzi 172.18.∗.∗, occorre predisporre gli

instradamenti appropriati nei router «A» e «B»:

«A» # **route add -net 172.18.0.0 netmask 255.255.0.0 ↩**
↪ **gw 172.19.1.2** [*Invio*]

«B» # **route add -net 172.17.0.0 netmask 255.255.0.0 ↩**
↪ **gw 172.19.1.1** [*Invio*]

«A» # **route -n** [*Invio*]

```
…
Kernel IP routing table
Destination  Gateway     Genmask         Flags Metric Ref Use Iface
172.19.1.2   0.0.0.0     255.255.255.255 UH    0      0      0 tun1
172.18.0.0   172.19.1.2  255.255.0.0     UG    0      0      0 tun1
…
```

«A» # **route -n** [*Invio*]

```
…
Kernel IP routing table
Destination  Gateway     Genmask         Flags Metric Ref Use Iface
172.19.1.1   0.0.0.0     255.255.255.255 UH    0      0      0 tun1
172.17.0.0   172.19.1.1  255.255.0.0     UG    0      0      0 tun1
…
```

Per realizzare una connessione cifrata tra i due nodi, i comandi iniziali con cui si avvia OpenVPN vanno modificati con l'aggiunta di opzioni appropriate. Il modo più semplice di cifrare la comunicazione consiste nell'utilizzo di una chiave simmetrica (chiave segreta), la quale deve essere usate in entrambi i nodi. Per generare una chiave di questo tipo si usa il comando seguente:

openvpn --genkey --secret chiave_segreta [*Invio*]

In questo modo, si genera il file '`chiave_segreta`' che può avere un aspetto simile a quello seguente:

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
a915cb41c5aebafd10d798df29411649
14d70f15baac22ca6f92e9be6439882e
4e4e685e816c5c27ccd17b28b43867b6
4ba513471bd6370113b2dcf0dceb6057
407d6b18a584238a85f5d5220c3f41b2
4c0847624a214433a4b0afd22fcbe3ab
4778f0b87f73bd1dd2e736647c82e6c9
c94fa563d45e1823c034aedb15ac6149
06ecd71c748c27480cddecfede51f9c6
b7e087b375819602ca350eb13374e9ab
fa27b72993da1802f4ef6acb1101e966
448985e9595d06cabe226781c0b09746
02e96b91f7fd8919fa57eae1e823b50a
6076f32524a14e268e95e019b23712dd
cd6d1b3173e31d15954c28ac429e5ec6
bebab6f9443bdfaf7d2216c9bc221fce
-----END OpenVPN Static key V1-----
```

Questo file deve essere messo a disposizione del nodo «A» e del nodo «B», avendo cura di trasmetterlo attraverso un canale riservato, quindi i comandi con cui si instaura il tunnel diventano i seguenti:

```
«A» # openvpn --remote 2.3.4.5 --dev tun1 ↩
↪           --ifconfig 172.19.1.1 172.19.1.2 ↩
↪           --secret chiave_segreta [Invio]

«B» # openvpn --remote 1.2.3.4 --dev tun1 ↩
↪           --ifconfig 172.19.1.2 172.19.1.1 ↩
↪           --secret chiave_segreta [Invio]
```

Tutto il resto procede nello stesso modo già visto negli esempi prece-

denti. Va comunque osservato che il file contenente la chiave segreta per instaurare il tunnel cifrato, deve essere protetto in modo che non possa risultare accessibile in lettura a utenti non privilegiati.

Naturalmente, negli esempi mostrati è stata omessa la dimostrazione della configurazione delle due reti private. Si può intendere che i nodi «A» e «B» siano router NAT per le reti rispettive e che siano configurati correttamente per tale scopo.

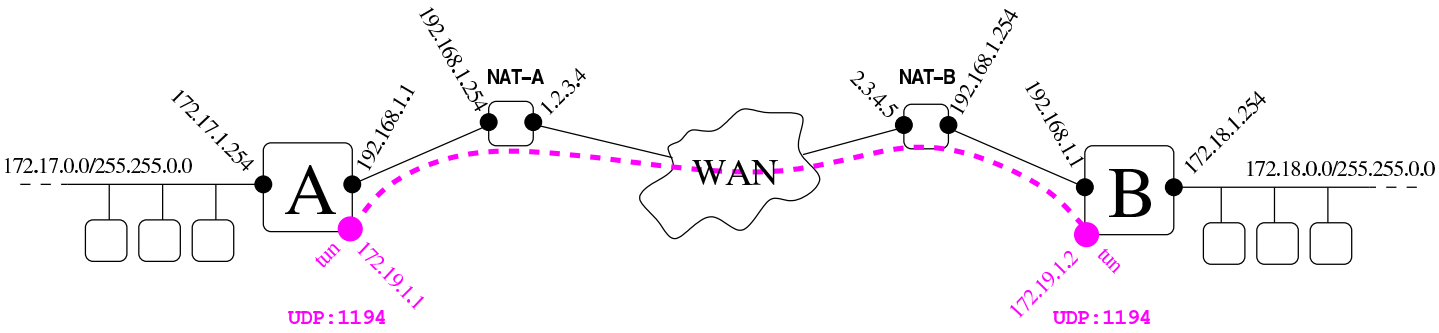
Va poi tenuto in considerazione che OpenVPN potrebbe funzionare come servente in attesa di connessioni multiple (ma per questo occorre consultare la documentazione). In tal caso, però, la scelta di usare una cifratura basata su chiave simmetrica potrebbe essere inadeguata; pertanto, OpenVPN consente di usare un sistema basato su chiavi asimmetriche, con lo scambio di certificati. Naturalmente il procedimento si complica, ma è descritto dettagliatamente nella documentazione originale.

44.8.3 OpenVPN attraverso un router NAT

«

Quando il tunnel realizzato con OpenVPN deve attraversare un router NAT, bisogna fare in modo che questo componente permetta il traffico relativo al tunnel stesso e lo diriga correttamente. OpenVPN si avvale, di norma, del protocollo UDP utilizzando come porta 1 194 (a meno di utilizzare opzioni specifiche per il protocollo TCP o per una porta differente); pertanto, i router NAT devono consentire il passaggio del protocollo UDP, relativo alla porta locale 1194.

Figura 44.119. Attraversamento di un router NAT.



I due router NAT vanno configurati in modo da dirigere il traffico UDP destinato alla porta 1194, rispettivamente al nodo «A» e al nodo «B», togliendo eventuali filtri che ne possono bloccare il passaggio. Inoltre, dato che questi router intervengono nel traffico UDP (e TCP) rimpiazzando le porte ci si deve avvalere dell'opzione '**`--ping` *n***', per far sì che il collegamento instaurato venga «ricordato» dal router NAT. L'argomento dell'opzione indica infatti una quantità di secondi, oltre la quale, in mancanza di traffico attraverso il tunnel, deve essere mandato un pacchetto fittizio per mantenere attivo il collegamento. Ecco quindi come potrebbe essere instaurato il tunnel, tra i nodi «A» e «B», utilizzando una chiave segreta e garantendo che il tunnel rimanga attivo con pause non più lunghe di 10 secondi:

```
«A» # openvpn --remote 2.3.4.5 --dev tun1 ↩
↪           --ifconfig 172.19.1.1 172.19.1.2 --ping 10 ↩
↪           --secret chiave_segreta [Invio]

«B» # openvpn --remote 1.2.3.4 --dev tun1 ↩
↪           --ifconfig 172.19.1.2 172.19.1.1 --ping 10 ↩
↪           --secret chiave_segreta [Invio]
```

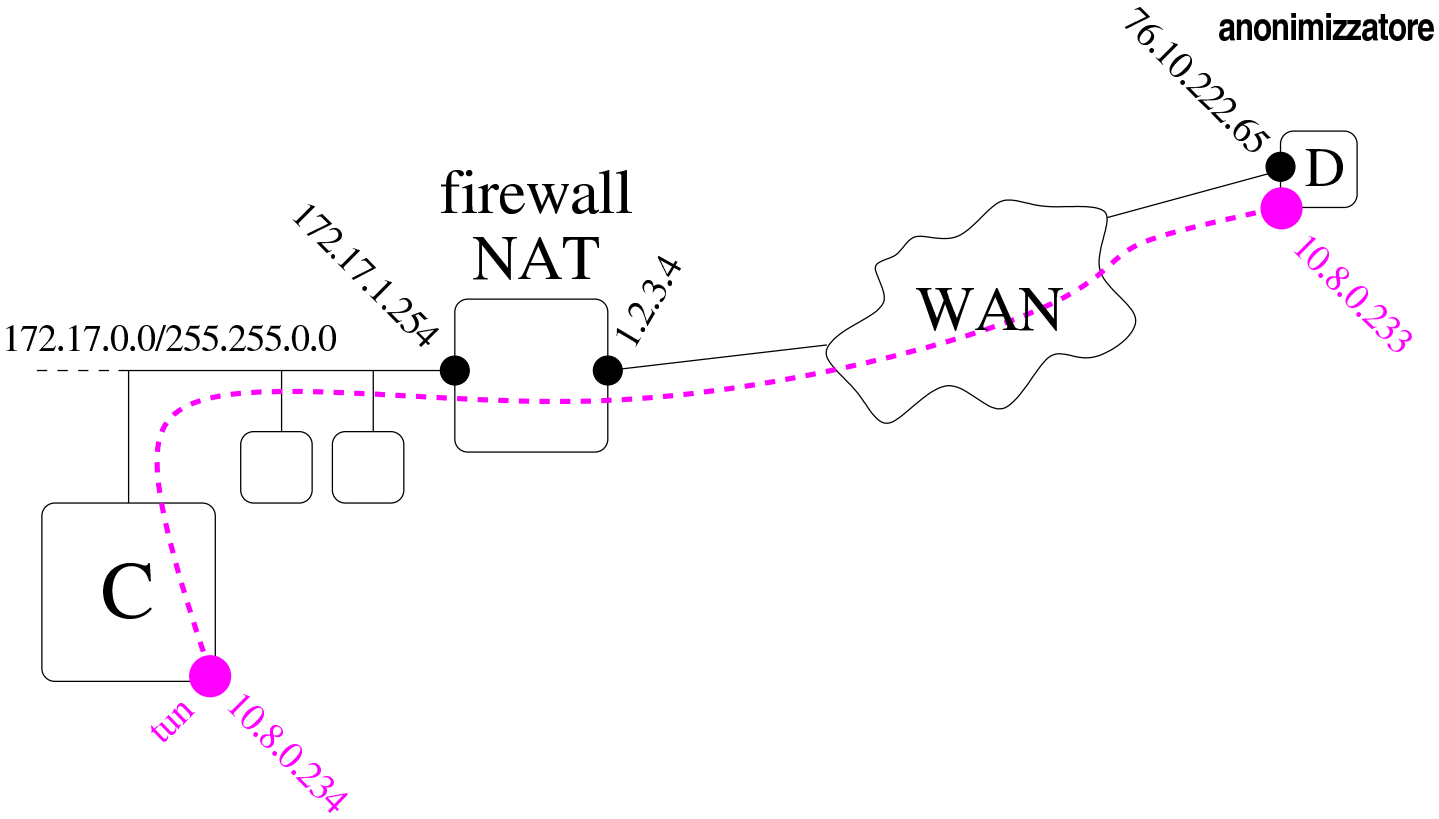
44.8.4 Utilizzare un servizio anonimizzatore con OpenVPN

«

Esistono dei servizi, gratuiti o a pagamento, con i quali è possibile realizzare un collegamento VPN, allo scopo di superare vincoli locali o per nascondere il proprio indirizzo IP. Per esempio, un firewall della propria rete locale potrebbe impedire l'accesso a certi siti o a certi servizi, così la realizzazione di una VPN potrebbe permettere di raggirare l'ostacolo. Ma una VPN di questo tipo potrebbe essere giustificata anche da scopi più nobili: tenendo conto che il tunnel di norma è cifrato, potrebbe servire a garantire che nella prima parte della nostra connessione il traffico non possa essere intercettato.

Va però osservato che avvalendosi di un servizio anonimizzatore si fa in modo che tutto il proprio traffico passi per il nodo che ci offre questo servizio, consentendo a chi lo gestisce, se lo vuole, di raccogliere tutte le informazioni che possono essere intercettate dal nostro traffico, indipendentemente dal fatto che il tunnel fino a lì sia cifrato o meno.

Figura 44.120. Collegamento a un anonimizzatore.



A titolo di esempio viene mostrato in che modo potrebbe essere realizzato un tunnel VPN con il servizio offerto da *http://hostizzle.com* . La figura mostra che il nodo «C» crea un tunnel con il nodo «D», il quale rappresenta l'anonimizzatore. Con questo tunnel, «C» riesce a superare eventuali blocchi inseriti nel firewall che consente di raggiungere la rete esterna. Gli indirizzi che appaiono nella figura sono indicativi, ma conformi agli esempi successivi.

Per realizzare il tunnel VPN, il servizio *http://hostizzle.com* richiede di utilizzare OpenVPN con una configurazione precisa e con un sistema di cifratura basato sullo scambio di certificati. In pratica, il servizio richiede di effettuare una registrazione e poi fa scaricare un pacchetto contenente tutti i file necessari, per esempio:

```
total 20
-rw-r--r--   885  0e24ce2e3a7b385a1f64c734857ff550.ovpn
-rw-r--r--  1220  ca.crt
-rw-r--r--  3779  client.crt
-rw-------   887  client.key
-rw-r--r--   636  ta.key
```

Questi file vanno messi tutti assieme in una collocazione scelta per la configurazione di OpenVPN. Per esempio, si suppone si trovino nella directory '`/etc/openvpn/hostizzle.com/`'. A questo punto, nel nodo «C» è sufficiente lanciare il comando seguente:

```
«C» # openvpn --config ↩
↪/etc/openvpn/hostizzle.com/0e24ce2e3a7b385a1f64c734857ff550.ovpn [ Invio ]
```

Infatti, il file che nell'esempio ha il nome '`0e24ce2e3a7b385a1f64c734857ff550.ovpn`', contiene tutte le informazioni necessarie a OpenVPN per instaurare il tunnel VPN cercando di farsi strada attraverso il firewall. A questo proposito, la lettura del file può essere istruttiva:

```
client
dev tun
proto tcp

# Change my.publicdomain.com to your public domain or IP
# address
remote 76.10.222.65 80
remote 76.10.222.65 1194
remote 76.10.222.65 443
remote 76.10.222.65 35
remote 76.10.222.65 36
remote 76.10.222.65 37
remote 76.10.222.65 38
remote 76.10.222.65 39
```

```
remote 76.10.222.65 40
remote 76.10.222.65 41
remote 76.10.222.65 42
remote 76.10.222.65 43
remote 76.10.222.65 44
remote 76.10.222.65 45
remote 76.10.222.65 46
remote 76.10.222.65 47
remote 76.10.222.65 48
remote 76.10.222.65 49
remote 76.10.222.65 50
remote 76.10.222.65 51
remote 76.10.222.65 52
remote 76.10.222.65 119
remote 76.10.222.65 563

remote-random

resolv-retry infinite
nobind
persist-key
persist-tun

tls-auth ta.key 1

ca ca.crt
cert client.crt
key client.key

ns-cert-type server

#DNS Options here, CHANGE THESE !!
#push "dhcp-option DNS 10.8.0.1"
```

```
comp-lzo

verb 3

ping-restart 10
```

Si può vedere che il nodo remoto dell'anonimizzatore ha l'indirizzo 76.10.222.65 e che si vuole fare provare a OpenVPN di connettersi a varie porte, usando però il protocollo TCP, contando che per almeno una di queste il firewall consenta il passaggio. Evidentemente, l'anonimizzatore offre l'accesso a OpenVPN attraverso tutte quelle porte.

Una volta instaurato il tunnel, nel nodo «C» potrebbe leggersi la configurazione dell'interfaccia virtuale e degli instradamenti seguenti:

«C» # **ifconfig** [*Invio*]

```
…
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.234  P-t-P:10.8.0.233  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:83426 (81.4 KiB)  TX bytes:8574 (8.3 KiB)
…
```

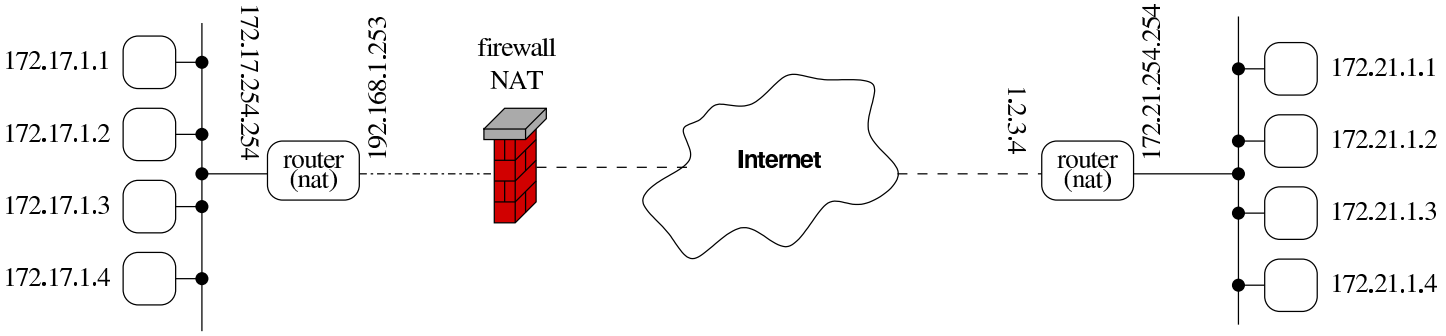
«C» # **route -n** [*Invio*]

```
Kernel IP routing table
Destination  Gateway     Genmask         Flags Metric Ref  Use Iface
…
10.8.0.233   0.0.0.0     255.255.255.255 UH    0      0      0 tun0
…
0.0.0.0      10.8.0.233  0.0.0.0         UG    0      0      0 tun0
```

44.8.5 VPN attraverso OpenSSH

In un sistema GNU/Linux, con l'ausilio di OpenSSH, è possibile creare un tunnel cifrato per collegare tra loro due reti private, attraverso Internet. La creazione del tunnel implica la definizione di un'interfaccia di rete virtuale che viene configurata convenientemente, come se fosse un'interfaccia reale, attraverso una rete fisica.

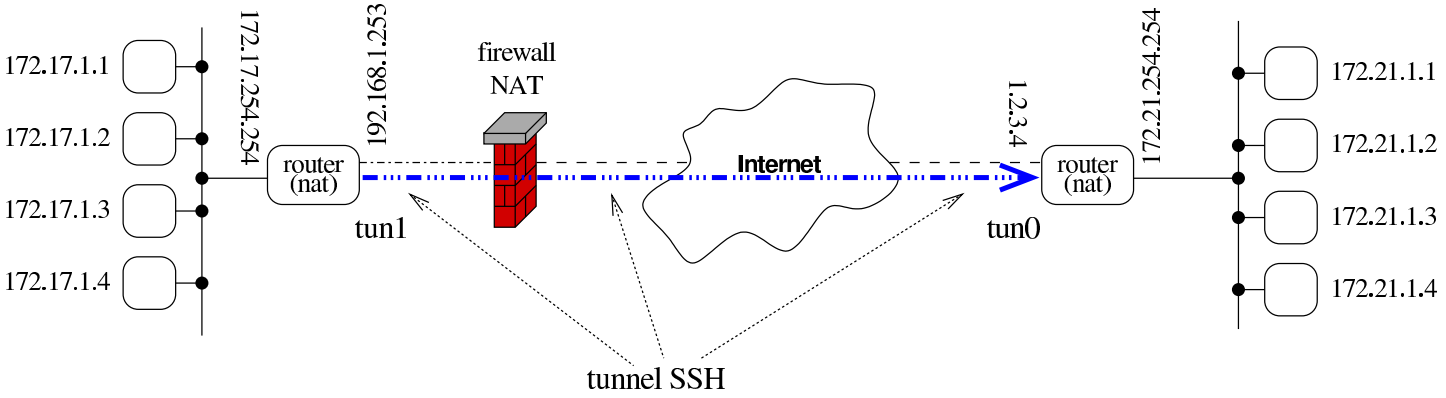
A titolo di esempio, si prendano due reti private separate, come quelle dello schema seguente:



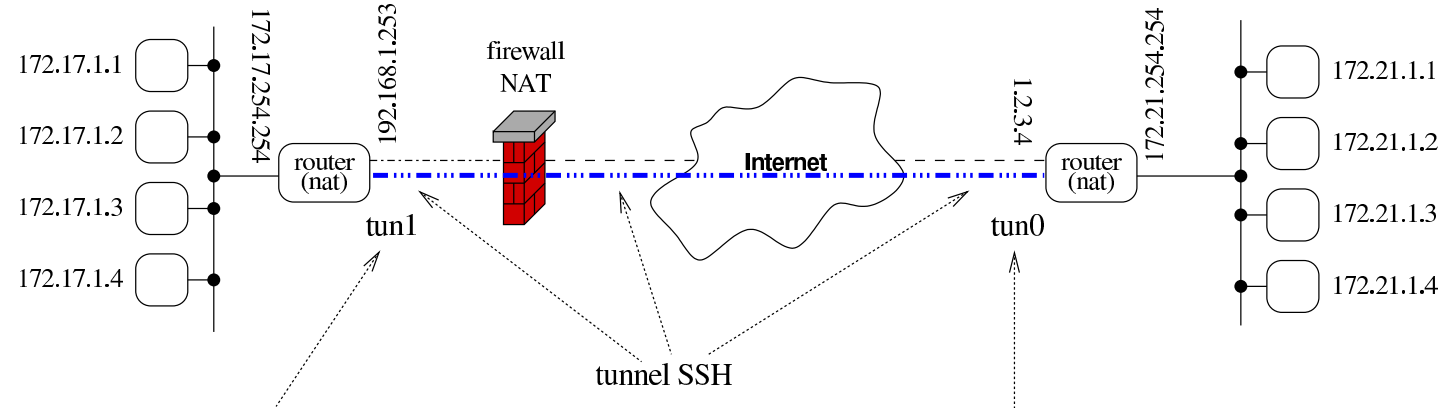
A sinistra si vede una rete locale con indirizzi 172.17.0.0/16, mentre a destra appare un'altra rete locale con indirizzi 172.21.0.0/16. La rete di destra accede a Internet attraverso un elaboratore che svolge il compito di router, avendo all'esterno un indirizzo IPv4 statico raggiungibile (1.2.3.4); la rete a sinistra, invece, ha un router, il quale però è isolato da un firewall (che in più trasforma anche gli indirizzi).

Fortunatamente, dalla rete di sinistra è possibile accedere all'ela-

boratore 1.2.3.4 attraverso il protocollo SSH. Pertanto, dalla rete di sinistra, è possibile attivare un tunnel SSH:



Si suppone che la creazione del tunnel produca l'apparizione, rispettivamente dell'interfaccia di rete virtuale '**`tun1`**' e '**`tun0`**'. Queste interfacce vengono configurate, da una parte e dall'altra, con l'aggiunta di instradamenti appropriati:




```
# ifconfig tun1 172.17.254.21 pointopoint 172.21.254.17
# route add –net 172.21.0.0 netmask 255.255.0.0 gw 172.21.254.17
```

```
# ifconfig tun0 172.21.254.17 pointopoint 172.17.254.21
# route add –net 172.17.0.0 netmask 255.255.0.0 gw 172.17.254.21
```

44.8.5.1 Configurazione e opzioni significative

OpenSSH, dal lato servente (dalla parte che deve ricevere la richiesta di connessione), ovvero nel lato destro degli esempi mostrati, deve essere configurato in modo da accettare la creazione di un tunnel. Per

questo occorre verificare che nel file '`/etc/ssh/sshd_config`' ci sia la direttiva seguente:

```
…
PermitTunnel point-to-point
…
```

Inoltre, considerato che il tunnel deve attraversare un NAT (un sistema di trasformazione degli indirizzi), è necessario che ci sia un minimo di scambio di pacchetti, anche se privi di utilità, per evitare che la connessione venga abbattuta (dimenticata) dal NAT stesso. Per questo si possono usare delle opzioni nella riga di comando di '**`ssh`**', in modo da mantenere attivo il collegamento.

Tabella 44.129. Opzioni utili nell'uso di '**`ssh`**' quando si vuole stabilire un tunnel cifrato.

Opzione	Descrizione
`-C`	Richiede che i dati trasmessi siano compressi, per ridurre l'utilizzo di banda.
`-f`	Richiede che il programma si metta a lavorare sullo sfondo, ma solo prima dell'esecuzione del comando, in modo da consentire, eventualmente, l'inserimento di una parola d'ordine.
`-o ServerAliveInterval` ***n***	Richiede che ogni ***n*** secondi di inattività, venga inviato un pacchetto di richiesta di attenzione al servente, attraverso il canale cifrato.

Opzione	Descrizione
`-o ServerAliveCountMax` ***n***	Dopo ***n*** tentativi falliti di ottenere una risposta dal servente, la connessione viene abbattuta.
`-w` ***tun_loc*** : ***tun_rem***	Stabilisce i nomi delle interfacce di rete virtuali da creare, presso l'elaboratore locale e presso quello remoto. I nomi devono essere compatibili con il sistema operativo e non devono essere già in uso per altri tunnel.

44.8.5.2 Attivazione del tunnel dal lato «cliente»

Dal lato cliente (la parte sinistra degli esempi mostrati), si attiva il tunnel contando di poter creare l'interfaccia '**`tun1`**' e '**`tun0`**' rispettivamente:

```
# ssh -o "ServerAliveInterval 1" ↩
↪     -o "ServerAliveCountMax 700" ↩
↪     -f ↩
↪     -w tun1:0↩
↪     1.2.3.4 true [Invio]
```

Come si può vedere, il tunnel viene creato collegandosi con l'indirizzo IPv4 1.2.3.4, il quale deve essere raggiungibile attraverso Internet; inoltre, è necessario dare un comando, per quanto inutile (in questo caso si tratta di '**`true`**'). Eventualmente viene richiesto di inserire la parola d'ordine:

```
root@1.2.3.4's password: digitazione_all'oscuro [Invio]
```

Si può poi controllare l'esistenza dell'interfaccia '**`tun0`**':

```
# ifconfig tun1 [Invio]

  tun1  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:500
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Quindi si può configurare l'interfaccia e gli instradamenti:

```
# ifconfig tun1 172.17.254.21 pointopoint 172.21.254.17 [Invio]

# route add -net 172.21.0.0 netmask 255.255.0.0 ↩
↪       gw 172.21.254.17 [Invio]
```

44.8.5.3 Configurazione dal lato «servente»

Dal lato servente, ovvero nel lato destro degli schemi di esempio mostrati, dopo che il tunnel è stato creato, è sufficiente configurare l'interfaccia e gli instradamenti:

```
# ifconfig tun0 172.21.254.17 pointopoint 172.17.254.21 [Invio]

# route add -net 172.17.0.0 netmask 255.255.0.0 ↩
↪       gw 172.17.254.21 [Invio]
```

44.8.5.4 Autenticazione automatica

Se per qualche ragione la connessione del tunnel viene abbattuta, gli esempi mostrati non sono sufficienti a ricreare il tunnel stesso. Evidentemente, da entrambe le parti, si rende necessario uno script, che, periodicamente, controlli se è attivo o se deve essere ristabilito il collegamento. Tuttavia, per automatizzare la connessione dal lato cliente, è necessario che l'autenticazione avvenga attraverso l'auto-

rizzazione della chiave pubblica. Sinteticamente, occorre procedere come segue.

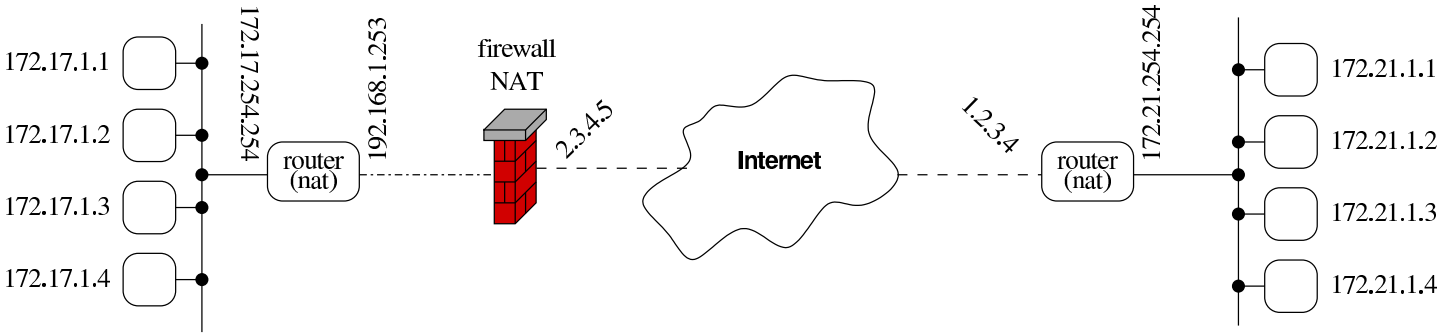
Dal lato cliente, l'utente '**root**' deve disporre di una coppia di chiavi RSA (dove la chiave privata non deve essere cifrata) che può essere creata così:

```
# ssh-keygen -t rsa -N "" -f /root/.ssh/id_rsa[Invio]
```

Così facendo, nella directory '`/root/.ssh/`' si devono ottenere i file '`id_rsa`' (chiave privata) e '`id_rsa.pub`' (chiave pubblica). Il file '`id_rsa.pub`', contenente la chiave pubblica, dovrebbe essere composto da una riga simile a quella seguente:

```
ssh-rsa AAAAB3NzaC1yc2EAAA…ObsDc1WtKtt20= root@localhost
```

A questo punto, dal lato servente, l'utente '**root**' deve dichiarare valido l'accesso da parte di chi è in grado di cifrare qualcosa che può essere decifrato con quella tale chiave pubblica. Ma, seguendo gli esempi mostrati, si pone un problema nuovo: occorre conoscere con quale indirizzo IPv4 si presenta la connessione.



Supponendo che il firewall del lato sinistro disponga di un indirizzo IPv4 statico, corrispondente a 2.3.4.5, nel file '`/root/.ssh/authorized_keys`' del lato servente occorre aggiungere la riga seguente:

```
from="2.3.4.5" ssh-rsa AAAAB3NzaC1…1WtKtt20= root@localhost
```

Naturalmente, anche il file '`/etc/ssh/sshd_config`' del lato servente deve essere redatto in modo tale da consentire un accesso di questo tipo:

```
…
PermitRootLogin yes
RSAAuthentication yes
PubkeyAuthentication yes
…
```

44.9 Steganografia

La ***steganografia*** è un metodo per nascondere delle informazioni all'interno di qualcosa. Nel concetto di steganografia rientra per esempio l'uso dell'inchiostro simpatico. Nel campo delle informazioni digitali, la steganografia avviene frequentemente attraverso la modifica delle immagini o dei suoni, in modo tale da rendere impercettibile la differenza apportata dall'inserimento dell'informazione addizionale.

L'informazione nascosta attraverso la steganografia richiede spazio; evidentemente, rispetto all'informazione apparente che veicola il messaggio nascosto, l'informazione addizionale può essere solo di entità minore. In questo caso si parla di ***portante*** per individuare l'informazione apparente che nasconde quella steganografata.

Nel campo delle immagini e dei suoni digitali, la steganografia si utilizza anche per marchiare i file, con informazioni che contengono i dati sul diritto di autore; in tal caso si parla di ***filigrana*** (*watermark*). Si osservi comunque che l'inserimento di una filigrana all'interno di un file contenente un'immagine o un suono, non dimostra la paternità dell'opera; al massimo può dimostrare chi ha eseguito il marchio. Tuttavia, in questo modo è possibile attribuire un numero di serie

univoco alla copia, della quale si intende controllare la diffusione. Chiaramente tali filigrane potrebbero essere rimosse, al costo di una riduzione sensibile di qualità nell'immagine o nel suono; tuttavia, si tratta di informazioni di cui spesso si ignora l'esistenza e per le quali non esistono strumenti adeguati in grado di verificarlo.

44.9.1 Tecniche steganografiche

«

Le tecniche attraverso cui si realizza la steganografia sono varie e possibilmente sconosciute. Quando la tecnica steganografica è nota, ma soprattutto è noto l'algoritmo usato per inserire le informazioni nella portante, di solito i dati da nascondere sono cifrati, salvo il caso della filigrana in cui l'intento può essere proprio quello di rendere evidente l'informazione.

Nel caso delle immagini, se la portante è costituita da un file in formato grezzo, o comunque non compresso (come può essere il formato PNM o il TIFF), l'informazione può avvenire modificando alcuni bit meno significativi che descrivono il colore di ogni punto grafico (*pixel*). Quando invece l'immagine è costituita da un file in un formato compresso (con perdita di informazioni), la steganografia può sfruttare le caratteristiche dell'algoritmo di compressione stesso per celare le proprie informazioni (la scelta di comprimere in un modo rispetto a un altro determina l'informazione aggiuntiva).

Si possono nascondere delle informazioni in un programma eseguibile, quando esiste la possibilità di sostituire delle istruzioni con altre equivalenti, sfruttando così queste variazioni per inserire delle informazioni. Naturalmente ci possono essere altre possibilità, in base alle caratteristiche del formato eseguibile da utilizzare; quello che conta è che le modifiche al file per introdurre le informazioni stega-

nografiche non interferiscano con il funzionamento del programma stesso.

È possibile usare un file di testo puro per inserire un'informazione addizionale «invisibile», modificando la spaziatura ed eventualmente la punteggiatura. Si può arrivare anche alla sostituzione di parole, attraverso un vocabolario di sinonimi.

Qualunque sia il metodo usato per la steganografia, spesso si richiede che l'informazione aggiunta sia ridondante in qualche modo, per poterla ricostruire in caso di un danneggiamento parziale.

44.9.2 Outguess

Outguess[23] è un programma per la steganografia elettronica in generale, per il quale possono essere scritte delle estensioni relative a diversi tipi di informazioni. Tuttavia, inizialmente è possibile utilizzare soltanto alcuni formati di immagini per inserire informazioni steganografate:

```
outguess [opzioni] file_portante_originale file_steganografato
```

```
outguess -r [opzioni] file_steganografato file_informazione_segreta
```

Il modello sintattico da un'idea di massima dell'utilizzo dell'eseguibile '**`outguess`**': in condizioni normali si inserisce un'informazione segreta, creando così un file steganografato; se si usa l'opzione '**`-r`**', si estrae l'informazione segreta da un file già steganografato in precedenza.

Outguess ha la capacità di inserire due informazioni steganografiche sovrapposte; inoltre, dal momento che l'algoritmo steganografico è noto, le informazioni possono essere cifrate.

Tabella 44.135. Alcune opzioni.

Opzione	Descrizione
`-k` ***chiave*** `-K`***chiave***	Specifica la chiave (la parola d'ordine) da usare per cifrare o decifrare l'informazione segreta. Nel secondo caso si fa riferimento alla seconda informazione incorporata o da incorporare.
`-d` ***file*** `-D` ***file***	Specifica il file contenente i dati da nascondere all'interno di un altro. Nel secondo caso, si tratta del secondo file da inserire.
`-e` `-E`	Con questa opzione si richiede di aggiungere delle ridondanze all'informazione nascosta, in modo da poterla recuperare anche in presenza di qualche piccolo errore nell'informazione portante. Nel secondo caso, si fa riferimento al secondo file da nascondere.
`-r`	Richiede l'estrazione delle informazioni nascoste.

Segue la descrizione di alcuni esempi.

- `$` **`outguess -d foglio.xls danza.jpg danza-steg.jpg`**[*Invio*]

  Con questo comando si vuole utilizzare il file '`danza.jpg`' per nascondere il file '`foglio.xls`', ottenendo così il file '`danza-steg.jpg`'. Purtroppo, il file portante non ha lo spazio sufficiente per questo:

```
Reading danza.jpg....
JPEG compression quality set to 75
Extracting usable bits:   17882 bits
Correctable message size: 7983 bits, 44.64%
Encoded 'foglio.xls': 45056 bits, 5632 bytes
steg_embed: message larger than correctable size 45056 > 7983
```

- `$` **`outguess -d messaggio.txt danza.jpg danza-steg.jpg`**[*Invio*]

  Questo comando è una variante di quello precedente, in cui il file da nascondere è costituito da '`messaggio.txt`'. Questa volta, l'incorporazione ha successo e il file '`danza-steg.jpg`' viene generato:

```
Reading danza.jpg....
JPEG compression quality set to 75
Extracting usable bits:   17882 bits
Correctable message size: 7983 bits, 44.64%
Encoded 'messaggio.txt': 440 bits, 55 bytes
Finding best embedding...
    0:   205(43.4%)[46.6%], bias   197(0.96), saved:     1, total:  1.15%
0, 402: Embedding data: 440 in 17882
Bits embedded: 472, changed: 205(43.4%)[46.6%], bias: 197, tot: 17887, skip: 17415
Foiling statistics: corrections: 93, failed: 0, offset: 30.333333 +- 71.419389
Total bits changed: 402 (change 205 + bias 197)
Storing bitmap into data...
Writing danza-steg.jpg....
```

  Si osservi che il file '`messaggio.txt`' è stato steganografato in chiaro, pertanto chiunque può estrarre l'informazione contenuta nel file '`danza-steg.jpg`'.

- `$` **`outguess -d messaggio.txt -k "ciao a tutti"`** ↩
  ↪ **`danza.jpg danza-steg.jpg`**[*Invio*]

  Questo comando è una variante di quello precedente, in cui il file da nascondere viene cifrato usando la parola d'ordine «ciao a tutti»:

```
Reading danza.jpg....
JPEG compression quality set to 75
Extracting usable bits:   17882 bits
Correctable message size: 7983 bits, 44.64%
Encoded 'messaggio.txt': 440 bits, 55 bytes
Finding best embedding...
    0:   247(52.3%)[56.1%], bias   218(0.88), saved:    -3, total:  1.38%
    3:   236(50.0%)[53.6%], bias   202(0.86), saved:    -2, total:  1.32%
   79:   214(45.3%)[48.6%], bias   217(1.01), saved:     0, total:  1.20%
   87:   225(47.7%)[51.1%], bias   193(0.86), saved:     0, total:  1.26%
  136:   215(45.6%)[48.9%], bias   187(0.87), saved:     0, total:  1.20%
136, 402: Embedding data: 440 in 17882
Bits embedded: 472, changed: 215(45.6%)[48.9%], bias: 187, tot: 17819, skip: 17347
Foiling statistics: corrections: 117, failed: 0, offset: 43.580000 +- 68.673760
Total bits changed: 402 (change 215 + bias 187)
Storing bitmap into data...
Writing danza-steg.jpg....
```

- `$` **`outguess -d messaggio.txt -k "ciao a tutti"`** ↩
  ↪ **`-D messaggio-bis.txt -K "viva le donne"`** ↩
  ↪ **`danza.jpg danza-steg.jpg`**[*Invio*]

Questo comando è una variante di quello precedente, in cui ci sono due file da nascondere, cifrati con parola d'ordine differenti:

```
Reading danza.jpg....
JPEG compression quality set to 75
Extracting usable bits:   17882 bits
Correctable message size: 7983 bits, 44.64%
Encoded 'messaggio.txt': 440 bits, 55 bytes
Finding best embedding...
    0:   247(52.3%)[56.1%], bias   218(0.88), saved:    -3, total:  1.38%
    3:   236(50.0%)[53.6%], bias   202(0.86), saved:    -2, total:  1.32%
   79:   214(45.3%)[48.6%], bias   217(1.01), saved:     0, total:  1.20%
   87:   225(47.7%)[51.1%], bias   193(0.86), saved:     0, total:  1.26%
  136:   215(45.6%)[48.9%], bias   187(0.87), saved:     0, total:  1.20%
136, 402: Embedding data: 440 in 17882
Bits embedded: 472, changed: 215(45.6%)[48.9%], bias: 187, tot: 17819, skip: 17347
Encoded 'messaggio-bis.txt': 440 bits, 55 bytes
Finding best embedding...
  111:   248(52.5%)[56.4%], bias   280(1.13), saved:    -3, total:  1.39%
111, 528: Embedding data: 440 in 17882
Bits embedded: 472, changed: 248(52.5%)[56.4%], bias: 280, tot: 17924, skip: 17452
Foiling statistics: corrections: 239, failed: 0, offset: 46.980892 +- 108.044297
Total bits changed: 930 (change 463 + bias 467)
Storing bitmap into data...
Writing danza-steg.jpg....
```

- `$` **`outguess -r -k "ciao a tutti" danza-steg.jpg ↩`**
  `↪` **`testo.txt`** [*Invio*]

  Questo comando si riferisce all'esempio precedente e si mostra l'estrazione del primo file di informazioni (generando il file '`testo.txt`'). Si osservi che la selezione si ottiene solo in base alla scelta della parola d'ordine corretta:

```
Reading danza-steg.jpg....
Extracting usable bits:   17882 bits
Steg retrieve: seed: 136, len: 55
```

- `$` **`outguess -r -k "viva le donne" ↩`**
  `↪` **`danza-steg.jpg testo-bis.txt`** [*Invio*]

  Questo comando si riferisce ai due esempi precedenti e si mostra l'estrazione del secondo file di informazioni (generando il file '`testo-bis.txt`'). Si osservi che la selezione si ottiene solo

in base alla scelta della parola d'ordine corretta e l'opzione '**-k**' rimane in forma minuscola:

```
Reading danza-steg.jpg....
Extracting usable bits:   17882 bits
Steg retrieve: seed: 111, len: 55
```

44.9.3 Stegdetect

«

Stegdetect[24] è un programma realizzato dallo stesso autore di Outguess, con lo scopo di cercare di individuare la presenza di informazioni steganografiche all'interno di file che apparentemente contengono solo un'immagine.

Il programma è in grado, teoricamente, di individuare la presenza di diversi tipi di algoritmi steganografici, ma non si può contare che l'analisi sia attendibile; soprattutto, non si può contare sul fatto che sia rivelato alcunché, anche quando l'informazione nascosta esiste veramente.

```
stegdetect [opzioni] [file] ...
```

Il programma '**stegdetect**', viene usato normalmente senza opzioni, indicando nella riga di comando l'elenco dei file da controllare; se questa indicazione manca, '**stegdetect**' attende il nome dei file da controllare dallo standard input. Ecco un esempio molto semplice di utilizzo:

```
$ stegdetect *.jpg [Invio]
```

```
...
000001.jpg : negative
000002.jpg : jphide(*)
000003.jpg : skipped (false positive likely)
000004.jpg : jphide(***)
000005.jpg : outguess(**)
000007.jpg : negative
...
```

Come si può intuire, gli asterischi vengono usati per indicare la probabilità con la quale è da ritenere che esista effettivamente un'informazione steganografata con l'algoritmo indicato.

Il pacchetto di Stegdetect include anche il programma '**stegbreak**', con il quale si può tentare di estrarre l'informazione contenuta nella portante, tentando di scoprire la parola d'ordine usata per cifrare i dati:

```
stegbreak [opzioni] [file] ...
```

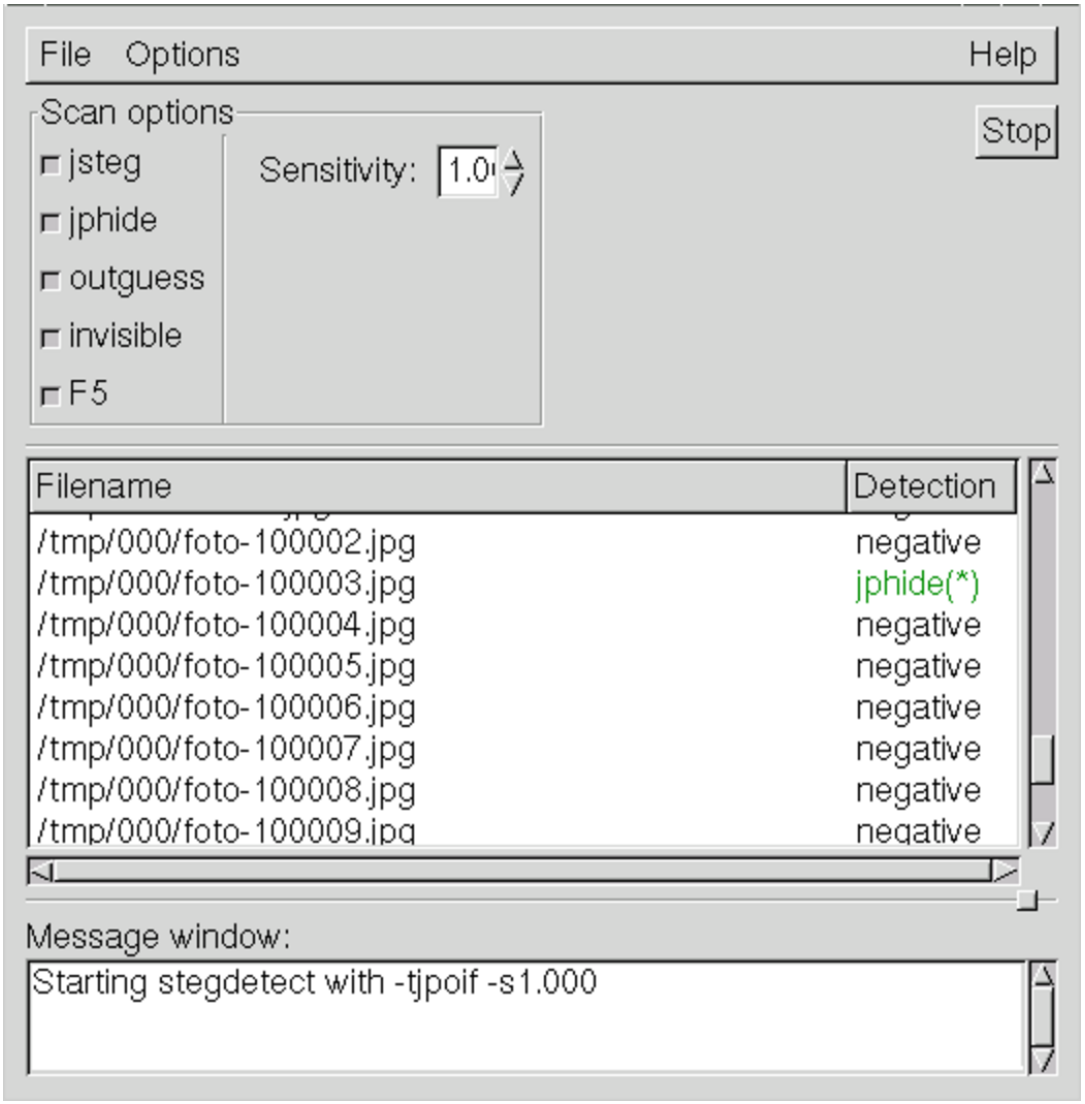
L'utilizzo del programma avviene nello stesso modo di '**stegdetect**', con la differenza che, se l'analisi ha successo, il rapporto generato restituisce, con il nome del file, la parola d'ordine scoperta.

Di solito, assieme a questi programmi si trova anche '**xsteg**'[25] (che eventualmente può essere distribuito con un pacchetto separato), il quale consente l'uso di '**stegdetect**' attraverso un pannello grafico.

```
xsteg
```

Il programma non richiede opzioni e comunque offre funzionalità limitate.

Figura 44.143. Xsteg durante il funzionamento.



Per ulteriori dettagli, si vedano le pagine di manuale *stegdetect(1)*, *stegbreak(1)* e *xsteg(1)*.

44.9.4 Steghide

«

Steghide[26] è un programma per la steganografia, utilizzando formati grafici (JPEG e BMP) e formati audio non compressi (WAV-RIFF e AU). La sintassi per l'uso del programma prevede un argomento iniziale che dichiara l'azione, seguito dalle opzioni relative:

```
steghide azione [opzioni]
```

L'azione viene dichiarata attraverso un nome che eventualmente può essere preceduto da due trattini ('**--**').

Tabella 44.144. Alcune azioni.

Azione	Descrizione
`embed` `--embed`	Richiede l'inserimento di un'informazione all'interno di un file portante che si vuole steganografare.
`extract` `--extract`	Richiede l'estrazione di un'informazione da un file steganografato in precedenza.
`info` `--info`	Richiede informazioni su un file da steganografare o già steganografato.

Segue la descrizione di alcune opzioni. Si osservi che le opzioni utilizzabili effettivamente dipendono dall'azione dichiarata all'inizio della riga di comando.

Tabella 44.145. Alcune opzioni.

Opzione	Descrizione
`-ef` ***file*** `--embedfile` ***file***	Specifica un file da inserire all'interno di un altro, attraverso la steganografia (quando si usa l'azione '**embed**').

Opzione	Descrizione
`-cf` ***file*** `--coverfile` ***file***	Specifica un file portante, da steganografare.
`-sf` ***file*** `--stegofile` ***file***	Specifica il nome del file steganografato da generare (quando si usa l'azione '**`embed`**').
`-xf` ***file*** `--extractfile` ***file***	Specifica il nome del file da generare con il contenuto di quanto inserito in precedenza in un file steganografato (si usa con l'azione '**`extract`**').
`-p` ***parola_d'ordine*** `--passphrase` ***parola_d'ordine***	Specifica, già nella riga di comando, la parola d'ordine da usare per cifrare o per decifrare un'informazione segreta.

In condizioni normali, Steghide comprime e cifra le informazioni prima di procedere alla steganografia; attraverso delle opzioni che non sono state elencate, è possibile specificare il livello di compressione e l'algoritmo da usare per la cifratura. Il sistema crittografico è simmetrico, ovvero a chiave segreta, costituita da una parola d'ordine. Segue la descrizione di alcuni esempi.

- `$` **`steghide info prova.jpg`**[*Invio*]

  Richiede informazioni sul file '`prova.jpg`' che in questo caso consente di inserire circa 2,9 Kibyte:

```
"prova.jpg":
  format: jpeg
  capacity: 2.9 KB
```

Il programma propone di verificare l'esistenza di un contenuto steganografico, ma in questo caso si rinuncia:

```
Try to get information about embedded data? (y/n) n[Invio]
```

- `$ steghide embed -ef messaggio.txt -cf prova.jpg ↩`
  `↪ -sf prova-steg.jpg`[*Invio*]

  Si richiede di utilizzare il file '`prova.jpg`' per incorporare il contenuto del file '`messaggio.txt`', generando il file steganografato '`prova-steg.jpg`'. Mancando l'opzione '**`-p`**', viene richiesto di specificare la parola d'ordine:

  ```
  Enter passphrase: digitazione_all'oscuro [Invio]

  Re-Enter passphrase: digitazione_all'oscuro [Invio]

    embedding "messaggio.txt" in "prova.jpg"... done
    writing stego file "prova-steg.jpg"... done
  ```

- `$ steghide extract -sf prova-steg.jpg`[*Invio*]

  Si richiede di estrarre il contenuto di '`prova-steg.jpg`':

  ```
  Enter passphrase: digitazione_all'oscuro [Invio]

    wrote extracted data to "messaggio.txt".
  ```

- `$ steghide extract -sf prova-steg.jpg -xf segreto.txt`[*Invio*]

  Si richiede di estrarre il contenuto di '`prova-steg.jpg`', specificando che il nome da usare per il file da creare deve essere '`segreto.txt`':

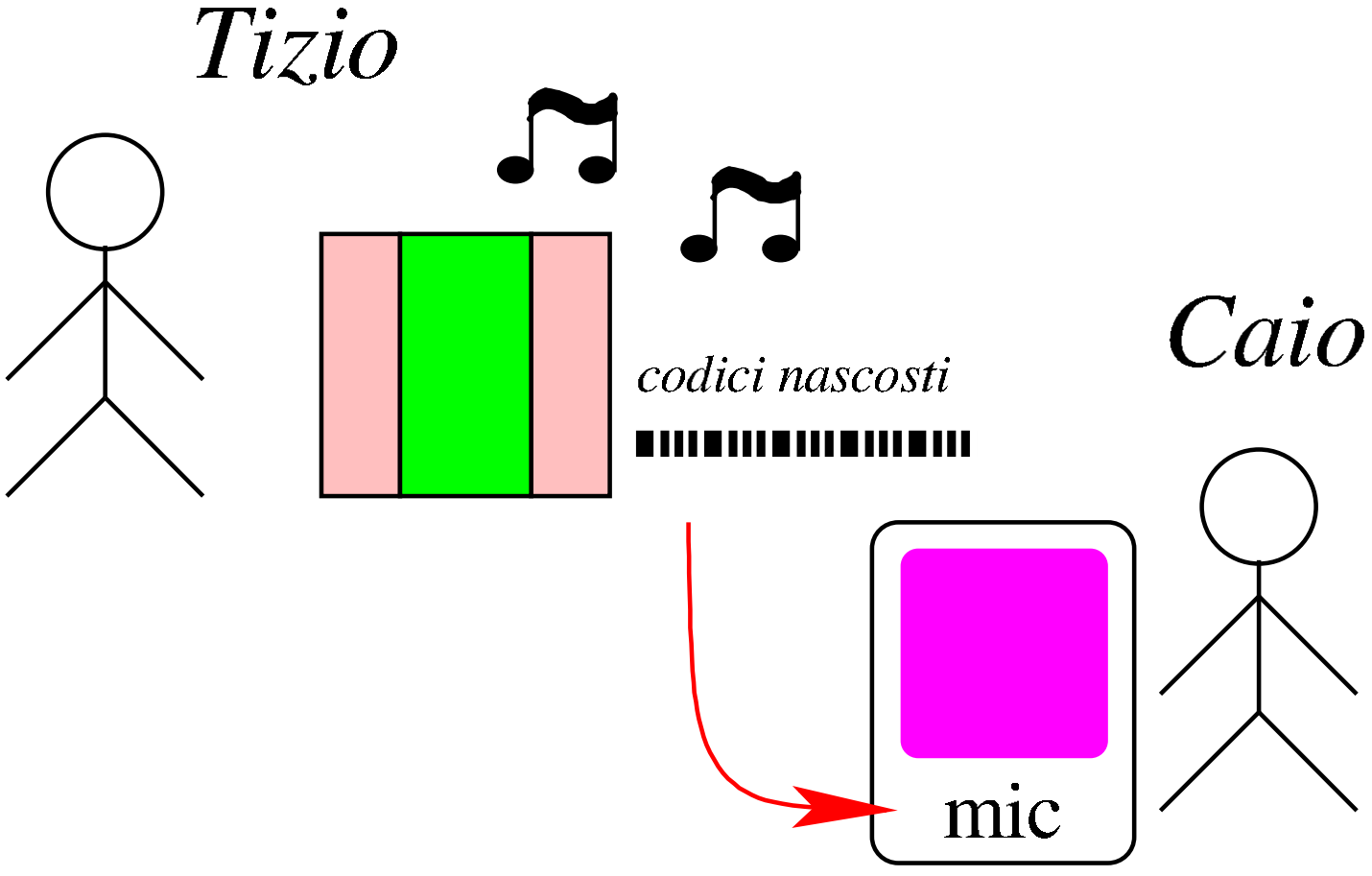
  ```
  Enter passphrase: digitazione_all'oscuro [Invio]
  ```

```
wrote extracted data to "segreto.txt".
```

44.9.5 Codici audio

«

L'inserimento di filigrane audio ha delle implicazioni importanti, le quali comportano la possibilità di controllare dove viene ascoltata una certa fonte sonora. Il principio si basa sul fatto che le filigrane non risultino udibili, per l'orecchio umano, ma possano essere captate da un microfono di un telefono mobile, nel quale sia stata installata un'applicazione adatta. Tale applicazione avrebbe lo scopo di raccogliere costantemente l'audio proveniente dal microfono, alla ricerca di codici audio riconoscibili, da trasmettere successivamente a qualche destinazione.



La figura mostra Tizio che sta riproducendo una fonte sonora di qualunque tipo. In tale fonte sonora sono nascosti dei codici che non si riconoscono a orecchio, ma lì vicino c'è Caio, con un telefono mobile connesso a Internet, nel quale c'è in funzione un'applicazione in grado di intercettare tali codici audio, trasmettendoli da qualche parte. Si possono ipotizzare diverse situazioni, per esempio questi due casi:

- la fonte sonora proviene da una stazione radio (o televisiva) e il meccanismo di intercettazione dei codici permette di ottenere delle statistiche molto precise sugli ascolti, eventualmente con un dettaglio sull'efficacia della pubblicità trasmessa;
- la fonte sonora proviene da una copia di una canzone acquistata da Sempronio, nella quale è stato inserito un codice univoco per individuarla, copia che però Sempronio ha diffuso incautamente a degli amici, così si scopre che quella copia particolare di quella canzone viene ascoltata in luoghi molto differenti e che Sempronio non ha rispettato i termini della licenza di quell'acquisto.

44.10 Riferimenti

«

- Andrea Colombo, *Le nuove tecnologie di crittografia*, http://impresa-stato.mi.camcom.it/im_43/colo.htm
- *The GNU Privacy Handbook*, 1999, http://www.gnupg.org/gph/en/manual.html
- Tony Sale, *Codes and Ciphers in the Second World War*, *The history, science and engineering of cryptanalysis in World War II*, http://www.codesandciphers.org.uk/

- *The GNU Privacy Handbook*, 1999, http://www.gnupg.org/
- Bert-Jaap Koops, *Crypto law survey*, http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm (non più disponibile)
- Kille S., *RFC 1779, A String Representation of Distinguished Names*, 1995, http://www.ietf.org/rfc/rfc1779.txt
- *Introduction to SSL*, http://docs.sun.com/source/816-6156-10/contents.htm
- *OpenSSL*, http://www.openssl.org
- R. Housley, W. Ford, W. Polk, D. Solo, *RFC 2459: Internet X.509 Public Key Infrastructure -- Certificate and CRL Profile* 1999, http://www.ietf.org/rfc/rfc2459.txt
- *OpenSSH*, http://www.openssh.com/
- Pagine di riferimenti a lavori attorno al protocollo SSH, http://www.openssh.org/
- Ulrich Flegel, *The interaction between SSH and X11, thoughts on the security of the Secure Shell*, 1997, http://wayback.archive.org/web/2002/http://p.ulh.as/docs/
- OpenVPN Technologies, *OpenVPN*, http://openvpn.net/
- *Hostizzle: Free OpenVPN–for real!*, http://hostizzle.com
- Enrico Pagliarini, *2024, 28/01/2012, La firma elettronica*, http://www.radio24.ilsole24or24e.com/main.php?articolo=firmare-senza-carta-codici-sonori-udibili-privacy-digitale-documenti , da 00:16 fino a 00:25 viene trattata la questione dei codici sonori, mentre da 00:25 in poi viene trattato l'argomento della firma elettronica, ovvero di quella che si ottiene con un pennino usato sopra una superficie sensibile.

[1] La firma elettronica è un concetto diverso dalla firma digitale, dove la firma avviene come su carta, attraverso un pennino e uno schermo sensibile, in grado di registrare sia il tratto, sia la pressione con cui questo è stato ottenuto.

[2] Nella terminologia normale che riguarda i sistemi di cifratura dei messaggi, questo codice di controllo è conosciuto come «hash».

[3] Qui si intende il furto di una chiave privata che non sia stata cifrata, o della quale sia stata scoperta la parola d'ordine necessaria per decifrarla.

[4] L'affermazione va intesa nel senso che l'autore non è in grado di dare un'indicazione precisa al riguardo.

[5] **GnuPG** GNU GPL

[6] In questo contesto, il comando è un'opzione che ha un ruolo particolare.

[7] **Gnome PGP** GNU GPL

[8] Si comprende l'importanza di avere un orologio del sistema funzionante e configurato in modo corretto.

[9] Anche se l'autenticazione del servente fallisce, di solito il programma cliente offre all'utente la possibilità di accettare ugualmente il certificato del servente, in modo da poter instaurare la connessione cifrata.

[10] Ciò spiega il motivo per cui, in questi casi, nel campo ***CN*** del nome distintivo di un certificato X.509 viene indicato il nome a dominio del servente.

[11] La difficoltà maggiore nella realizzazione di software libero di questo tipo sta nei problemi legali dovuti all'uso di questo o quel-

l'algoritmo crittografico, che potrebbe essere brevettato, oppure potrebbe non essere ammesso dalle leggi del proprio paese.

[12] Se si vuole mantenere la possibilità di utilizzare un sistema di autenticazione RHOST+RSA, in cui l'utente non debba intervenire in alcun modo, è necessario che la sua chiave privata non sia protetta da parola d'ordine. Ma è già stato spiegato che si tratta di un modo molto poco sicuro di gestire tale tipo di comunicazione.

[13] **OpenSSL** licenza speciale + SSLeay

[14] È importante ribadire che se questo file contiene il valore n, l'ultimo certificato che è stato creato è quello corrispondente al numero $n-1$.

[15] Qui si intende un proxy che non conosca il protocollo utilizzato effettivamente dal servizio che viene ridiretto, a parte la gestione TCP pura e semplice.

[16] **Telnet-SSL** UCB BSD

[17] **SSLwrap** GNU GPL

[18] Soprattutto nel caso di servizi che per loro natura non si lasciano gestire semplicemente in questo modo, come avviene per il protocollo FTP.

[19] **Stunnel** GNU GPL

[20] **OpenSSH** licenza speciale

[21] Si deve fare attenzione al fatto che tra il nome del nodo e il nome dell'utente ci deve essere uno spazio.

[22] **OpenVPN** GNU GPL

[23] **Outguess** licenza speciale BSD

[24] **Stegdetect** licenza speciale BSD

[25] **Xsteg** licenza speciale BSD

[26] **Steghide** GNU GPL