Introduzione

Nel corso degli ultimi anni è divenuto possibile effettuare pagamenti anche *senza* disporre di denaro contante (basta pensare, ad esempio all'uso di carte di credito e bancomat). In questo contesto, anche il world wide web è divenuto, oltre ad un efficiente mezzo di divulgazione di notizie e informazioni, anche un utile strumento per effettuare transazioni commerciali. Con l'avvento e il successivo affermarsi del commercio elettronico, il l'aspetto della sicurezza delle transazioni è diventato sempre più importante, soprattutto su Internet.

Il Commercio Elettronico

Le parti coinvolte nel meccanismo di transazioni commerciali di tipo elettronico sono:

- *Compratore* e *Venditore*
- *Fornitore*: chi fornisce gli strumenti di pagamento elettronico (es. carta di credito) al Compratore e garantisce il pagamento delle transazioni avvenute tramite tali strumenti al venditore.
- *Acquirente*: è l'intermediario tra il compratore ed il venditore. Autorizza ed accetta i pagamenti al venditore

Tipicamente è possibile identificare nel Fornitore la banca del compratore e nell'acquirente la banca del venditore.

Ovviamente nessuna delle parti in causa vorrà esporsi finanziariamente prima che il pagamento sia esplicitamente autorizzato. Pertanto ogni transazione elettronica dovrà soddisfare i requisiti fondamentali di:

- *Integrità*
- *Autenticazione*

L'autenticazione in particolare si basa sull'*identificazione* dell'utente e sulla *verifica* dei requisiti dell'utente che si è appena identificato. Nel processo di autorizzazione possono essere usati tre fattori al fine di identificare univocamente una persona:

- Conoscenza (qualcosa che la persona sa)
- Possesso (qualcosa che la persona ha)
- Caratteristiche fisiche (v. Appendice A: biometrie)

Molti sistemi di identificazione usano almeno due di questi fattori; ad esempio l'autorizzazione all'uso di una carta di credito si basa sui requisiti del possesso (l'utente deve avere la carta) e della caratteristica (la firma). Analogamente il bancomat si basa sui requisiti di possesso (del bancomat) e della conoscenza (è richiesto un codice PIN).

Internet ed E-commerce

Il commercio digitale attraverso Internet sembrerebbe una pratica rischiosa: basta pensare a cosa accadrebbe, ad esempio, se qualcuno riuscisse a "copiare" il nostro numero di carta di credito o di conto corrente mentre stiamo eseguendo un acquisto attraverso Internet!

Oppure, limitandoci a casi meno gravi e meno dannosi, ci potrebbe capitare che tutte le nostre transazioni vengano tracciate e monitorate da "snoopers"...

Eppure ogni giorno vengono effettuate milioni di transazioni di questo tipo: come è possibile farlo in modo sicuro?

Un primo possibile tipo di approccio, il cliente riempie una Web form per prenotare un servizio o acquistare un bene; in questa form lascia, assieme ai dati personali, il proprio numero di telefono. La società o l'azienda a cui la form è destinata userà il numero di telefono del cliente per contattarlo ad una specifica ora del giorno, in modo che il cliente stesso possa comunicare, ad esempio, il numero di carta di credito per via telefonica. Ovviamente uno schema di questo tipo è sicuro e conveniente né più né meno quanto il commercio telefonico...

Un secondo tpo di approccio prevede invece l'uso di un *Internet Commerce Broker* (ICB), ovvero un "mediatore" tra il venditore ed il compartore. Lo schema ICB prevede l'uso di Internet con il supporto di comunicazioni telefoniche, seguendo il seguente algoritmo:

1. Il cliente si registra telefonicamente all'ICB e fornisce i propri dati, fra i quali quelli relativi alla carta di credito. L'ICB assegna al cliente un identificatore numerico.
2. Ad ogni transazione, il cliente fornisce al venditore il proprio numero di identificazione.
3. Il venditore presenta la richiesta di acquisto all'ICB.
4. Il venditore confronta il numero identificativo del cliente presso l'ICB prima (o dopo) portare a termine la transazione (cioè, ad esempio prima di recapitare il bene acquistato).
5. Il venditore invia al cliente il bene che questi ha acquistato. Se il bene acquistato è un documento, può essere spedito anche tramite posta elettronica.
6. L'ICB chiede al cliente di confermare l'acquisto. Tipicamente anche questa operazione avviene tramite e-mail.
7. Il cliente da' la conferma via e-mail
8. L'ICB usa i dati relativi alla carta di credito dell'utente (inseriti al momento dell'iscrizione all'ICB) per eseguire il pagamento.

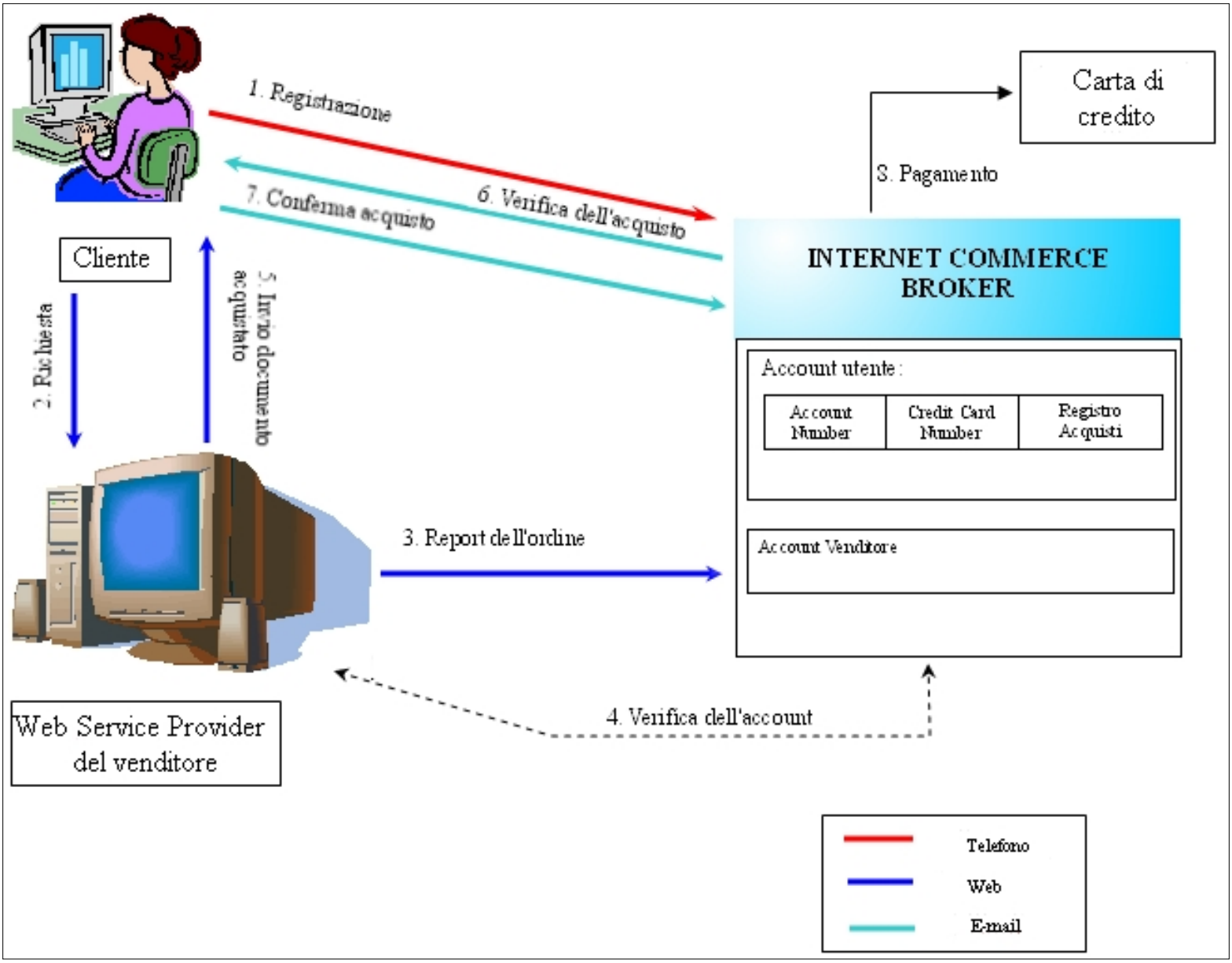

fig.1 : schema dell' Internet Commerce Broker

Con questo sistema si assume che le comunicazioni via telefono e via e-mail siano sicure ed affidabili; in realtà queste condizioni non sono sempre verificate.

Inoltre entrambi gli schemi visti finora hanno la grande limitazione di essere poco convenienti per il cliente e non offrono quelle che sono alcune delle caratteristiche salienti del commercio elettronico: sicurezza e spontaneità delle transazioni via Web.

Requisiti essenziali per l' E-commerce

Fino a questo momento abbiamo visto quali sono gli aspetti primari e secondari che un utente cerca all'interno di un servizio di e-commerce. Gli esempi di approcci possibili per realizzare un servizio di commercio elettronico che

abbiamo esaminato in precedenza, non riuscivano a soddisfare tutte le richieste che il cliente desidera: questi schemi sono infatti superati da modelli più efficienti ed in grado di rispondere alle esigenze primarie e secondarie del cliente. Tali esigenze possono essere schematicamente individuate in:

Requisiti primari:

1. *Confidenzialità:* Il servizio Web deve assicurare che la transazione non possa essere intercettata e letta da estranei. Nessuno deve essere in grado di catturare, ad esempio, il nostro numero di carta di credito e, successivamente, fare acquisti col nostro nome!
2. *Autenticità:* Il servizio Web deve assicurare che "siamo chi diciamo di essere". Entrambe le parti devono essere sicure dell'identità dell'altro. Senza questa assicurazione potremmo incautamente fornire il nostro numero di carta di credito ad un malfattore che si finge, ad esempio, una azienda produttrice di Software (vedi attacchi di tipo "man in the middle")!
3. *Integrità del messaggio:* Il servizio Web deve assicurare che il messaggio ricevuto è esattamente quello inviato. Non deve essere possibile intercettare e alterare il nostro ordine (o parte di esso) mentre viaggia sulla rete.

Requisiti nono strettamente necessari, ma di grande importanza:

1. *Spontaneità delle transazioni:* per un cliente è preferibile poter effettuare un acquisto in modo sicuro dove e quando vuole, piuttosto che effettuare un'iscrizione e ottenere un account per ogni Web che offre servizi a cui è potenzialmente interessato.
2. *Transazioni anonime:* è importante che i nostri acquisti non vengano tracciati e loggati, poichè altrimenti sarebbe facile per un calcolatore reperire una grande quantità di informazioni sul nostro conto.

Possibili minacce ai sistemi di E-Commerce

E' facile rendersi conto che un sistema che offre servizi di commercio elettronico sia potenzialmente soggetto ad attacchi da parte di malfattori che, cercando un tornaconto personale, tenteranno di violare la sicurezza del sistema. Nel seguito vedremo alcuni tipi di attacchi, suddividendoli in tre categorie.

Minacce "Low-Tech"

Nell'immaginario collettivo, chi riesce a violare un sistema protetto (come appunto un sistema per l'E-commerce) si avvale di tecnologie d'avanguardia che gli permettono di penetrare nel sistema e attingere a informazioni riservate. In realtà, studi sulla sicurezza dei sistemi ATM (usati anche per i bancomat) hanno scoperto che la causa più frequente di avvenute violazioni sono:

1. Bugs nel Software del sistema
2. Furto del PIN
3. Violazioni da parte del personale delle banche

Sebbene questi dati facciano riferimento ai sistemi ATM, il concetto può essere esteso anche ai sistemi Web. In particolare possiamo costruire tre classi di problematiche che possono dar luogo ad attacchi "a bassa tecnologia":

- **Mancanza di preparazione** da parte degli utenti e dell'amministratore. Gli utenti devono capire l'importanza di un uso corretto della password (e della scelta di una buona password), mentre gli amministratori dovrebbero sapere come implementare e configurare correttamente un sistema che sia sicuro.
- **Personale corrotto**: le probabilità di accedere ad un sistema protetto aumentano proporzionalmente con l'aumentare delle persone addette alla manutenzione dei sistemi di cifratura o in possesso di permessi privilegiati.
- **Bugs del Software**: è stato stimato che lo 0,01% degli errori in una transazione ATM (ad esempio denaro destinato ad un account sbagliato) è dovuto ad errori del Software. Se pensiamo che 1 errore ogni 10.000 transazioni sia una cifra accettabile, dobbiamo però considerare che ogni giorno avvengono milioni di transazioni, perciò quotidianamente ci sono centinaia di errori! Transazioni commerciali che usano il Web hanno, senza dubbio, la stessa percentuale di errore.

Denial-of-Service

Si ha un attacco di tipo *Denial-of-Service* quando qualcuno (probabilmente un concorrente) "inonda" di richieste il server Web al punto che il server non riesce più a gestire le altre richieste in tempi ragionevoli. In condizioni del genere i *veri* clienti attendono inutilmente che le loro richieste vengano soddisfatte fino a quando, spazientiti, lasciano il server.

Attacchi di questo tipo sono possibili in tutti i sistemi network-based e sono spesso indistinguibili da situazioni non malevole, come un crash del sistema. Il protocollo HTTP in particolare è molto sensibile ad attacchi Denial-of-Service.

Attualmente, tutto ciò che un amministratore di sistema può fare, è monitorare costantemente il server cercando di discriminare le connessioni dei clienti da quelle effettuate con intenzioni malevole.

Man in the middle

Immaginiamo di installare un finto sportello bancomat in un centro commerciale per raccogliere i PIN dei bancomat degli ignari utenti: le informazioni così ottenute possono essere usate per appropriarsi criminosamente del denaro di quegli utenti prelevandolo direttamente dal loro *vero* conto corrente.

Un ragionamento analogo può essere applicato anche al commercio elettronico attraverso il Web: in questo caso, attacchi di questo tipo vengono chiamati "*man in the middle*". Il nome deriva proprio dal fatto che "l'uomo-nel-mezzo" si frappone tra il client ed il server, fingendo di essere il vero Web server e ottenere informazioni riservate (come il numero di carta di credito) direttamente dal cliente.

Questo tipo di attacco può essere prevenuto se il browser richiede al server una autenticazione attraverso, ad esempio, lo schema della firma digitale.

Servizi Web Sicuri

Per risolvere i problemi discussi nel paragrafo precedente sono stati introdotti due protocolli per garantire che le operazioni che avvengono tramite web e, in particolare, le transazioni economiche avvengano in modo sicuro. Questi protocolli sono *Secure Socket Layer* (SSL) e *Secure HTTP* (S-HTTP).

SSL è un protocollo sviluppato da Netscape Communications Corp. e può essere usato in molte applicazioni di rete, come la posta elettronica, ma è usato soprattutto per aumentare la sicurezza di Http. Un URL, in accordo con lo standard SSL, può essere specificato con la seguente sintassi:

```
https://www.myurl.com/mySSL_page.html
```

Anche Microsoft ha sviluppato un protocollo chiamato Private Communication Tecnology (PCT), ma è pressochè identico al protocollo SSL, tranne poche eccezioni.

Secure Http è un protocollo sviluppato da CommerceNet. Un URL destinato ad individuare un servizio web che implementa S-HTTP ha la seguente sintassi:

```
shttp://www.myurl.com/myS-HTTP_page.html
```

Secure Socket Layer

SSL è un protocollo progettato per fornire la cifratura e l'autenticazione tra un client ed un server web. SSL viene implementato come un nuovo metodo di accesso all'URL (https://...) al quale è stata assegnata la porta 443. Ciò significa che lo stesso server può trattare sia un server HTTP insicuro (sulla porta 80) che un server HTTPS sicuro. SSL è un protocollo a livelli che deve interfacciarsi a livello più basso con un livello di trasporto affidabile come il TCP ed a livello superiore con un protocollo applicazione (v. figura 1).

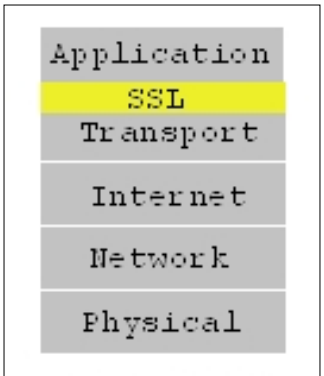

fig.1: SSL nella layerizzazione OSI

Il protocollo SSL fornisce le seguenti caratteristiche:

- **Autenticazione del server SSL**, in modo che un utente possa confermare l'identità del server. Questo è reso possibile dal fatto che un browser SSL-compatibile mantiene un elenco dove sono memorizzate le *Certification-Authority* (CA) fidate, con le relative chiavi pubbliche. Il browser ottiene dal server SSL un certificato contenente la sua chiave pubblica; tale certificato è firmato proprio da una CA che compare nell'elenco delle CA fidate. In questo modo il browser può verificare l'identità del server, prima che l'utente

inoltri, ad esempio, il numero di carta di credito.

- **Autenticazione del client SSL**, in modo che il server possa autenticare il client. Sebbene questa caratteristica di SSL sia solo opzionale, è molto importante specialmente in casi in cui il server è una banca che vuole autenticare il cliente prima di mandargli informazioni professionali. L'autenticazione del client avviene in modo analogo a quella del server: anche il client infatti può utilizzare dei certificati rilasciati dalle Certification Authority.
- **Sessione SSL cifrata**: le informazioni inviate fra il browser ed il server vengono cifrate in fase di spedizione e decifrate in fase di ricezione. Inoltre SSL fornisce un meccanismo per rilevare eventuali contraffazioni delle informazioni da parte di un intruso.

Il protocollo inizia con una fase di handshake tra il client ed il server SSL, durante la quale vengono negoziati i parametri che verranno usati durante la comunicazione (*Negotiation of Crypto-options*). Il client deve infatti accordarsi col server su unalgoritmo di cifratura, un algoritmo di integrità e un algoritmo per la cifratura a chiave privata; in caso contrario non viene garantita la sicurezza del canale di comunicazione la richiesta verrà scartata. La negoziazione delle Crypto-options avviene automaticamente, senza che l'utente debba intervenire. A questo punto può iniziare la trasmissione dei dati, e questi sono cifrati con la chiave concordata durante la fase di handshake.

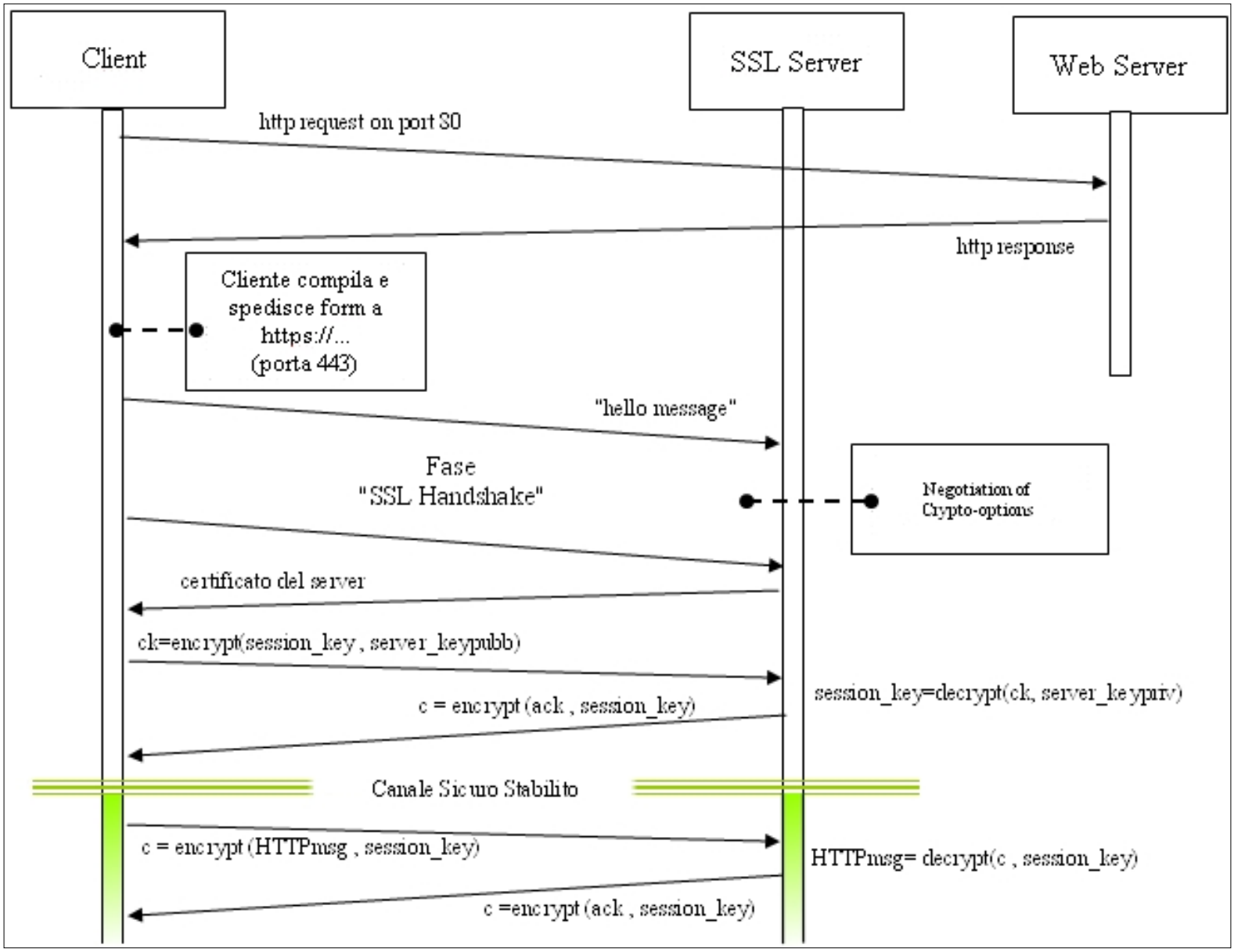

fig. 2: apertura di una connessione SSL

SSL è una tecnologia ormai largamente utilizzata e compresa in quasi tutti i web server e browser. SSL2 supporta solo l'autenticazione del server, SSL3 supporta anche l'autenticazione del client.

Secure HTTP

Un protocollo alternativo a SSL è Secure-HTTP: la forza di questo protocollo è nella sua flessibilità e nel fatto che da anni sta continuamente evolvendo attraverso dei miglioramenti e rifiniture. SSL è più generico e non rivolto alle applicazioni poiché lo standard SSL vuole diventare un protocollo che offre servizi a livello più basso; SHTTP è invece un estensione dell' HyperText Transfer Protocol (HTTP) ed è stato progettato da E. Rescorla e A. Schiffman della EIT (Enterprise Integrated Technologic Inc.) per realizzare connessioni HTTP sicure. S-HTTP fornisce servizi sicuri applicabili per:

- transazioni confidenziali;
- autenticazione e integrità dei dati;
- non ripudiabilità dell'originale.

Il protocollo lascia massima flessibilità nella scelta dei meccanismi di gestione della chiave, politiche di sicurezza e algoritmi di crittografia, permettendo la scelta di queste opzioni direttamente da parte dell'utente. Non è richiesta la chiave pubblica per il client. Un pacchetto S-HTTP "contiene" HTTP, poichè permette ai messaggi di essere incapsulati in vari modi.

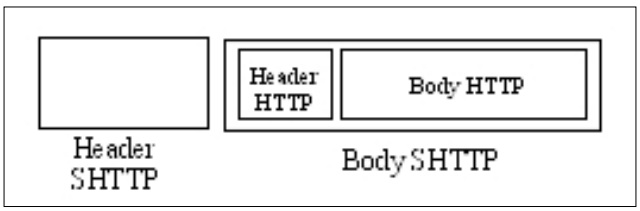

fig. 3 : Incapsulamento di un pacchetto Http in SHTTP

Per poter creare pagine web sicure compatibili con S-HTTP, è necessario definire alcune nuove estensioni al linguaggio HTML, poichè è necessario rendere sicuri i collegamenti. Se ad esempio vogliamo creare una form che possa essere spedita ad un server S-HTTP, il codice HTML dovrà essere del tipo:

```
<header>
    <CERTS FMT=PKCS7> PEG5T835GJ54HJ6425G43HG43HGHOLG434...
    </CERTS>
</header>
```

Fra i tag <CERTS> </CERTS> è racchiuso il certificato del server.

Nella porzione di codice seguente invece sono specificate informazioni relative al certificato e le crypto-options:

```
<form action="shttp://..."
    DN= ... ",    OU= ... ,     O= RSA Data Security ,        C=US"
    CRYPTOPTS=" ... ">

/* ... */

</form>
```

In particolare DN specifica il nome della società, OU è il tipo di certificato, O è il nome della Certification Authority (es. RSA Data Security) e C rappresenta lo stato (es. United States).

Le cryptopts servono per specificare quale algoritmo di crittografia (es. RSA) e quale algoritmo di Hashing (es. MD5) verranno usati per realizzare la firma digitale.

Appena il cliente compila la form e la spedisce attraverso l'hyperlink al server S-HTTP, ha inizio la fase di negoziazione degli algoritmi di crittografia. Il browser S-HTTP riesce a ricavare la chiave pubblica del server dal certificato incluso nell'header della pagina che conteneva la form; in questo modo il browser può generare una chiave di sessione con la quale cifrare il corpo del messaggio HTTP (il contenuto della form). La chiave di sessione viene cifrata con la chiave pubblica del server ed è contenuta nell'header S-HTTP. Il messaggio S-HTTP, che sostituisce il messaggio HTTP, è composto da una linea di richiesta, da un header (secondo le specifiche RFC-822) ed infine dal corpo (cifrato) del messaggio:

```
Secure-HTTP/1.1  200  OK

Content-Transfer-Encoding: base64
Content-type: application/http
Prearranged-Key-Info: des-ecb, 87tyhd94736kjkpu4 // chiave sessione
cifrata
                                    //con chiave pubblica del server
Content-Privacy-Domain: PKCS-7

-- BEGIN PRIVACY ENHANCED MESSAGE --
    // Corpo del messaggio cifrato e firmato
-- END PRIVACY ENHANCED MESSAGE --
```

Il messaggio viene ricevuto dal server che lo decifra in accordo a quanto specificato nell'header. In prticolare usa la sua chiave privata per decifrare la chiave di sessione e poi, con quest'ultima, decifra il corpo del messaggio. Infine il

server manda un avviso (anch'esso cifrato e firmato) di avvenuta ricezione al client.

Il browser che riceve il messaggio di notifica dal server usa nuovamente la chiave di sessione per decifrarlo e infine controlla la firma digitale ricevuta con la notifica.

A questo punto la transazione può dirsi completata.

Mentre prepariamo o leggiamo un messaggio sicuro, il browser visualizza tramite icone lo stato della transazione sicura, cosi come quando si legge una firma o un messaggio cifrato il browser indica l'identità di chi firma.

APPENDICE A: Biometrie

L'identificazione di un utente, necessaria al fine di controllare e monitorare gli accessi ad un sistema, può essere realizzata mediante l'uso di tecniche biometriche. In particolate le tecniche di riconoscimento tramite biometrie possono essere *statiche* (misurazioni) o *dinamiche* (riconoscimento calligrafico, analisi della voce ecc.). In ogni caso un sistema di identificazione, e in particolare un sistema di identificazione basato su tecniche biometriche, deve essere:

- resistente alla contraffazione
- affidabile
- di facile utilizzo e accettabile dall'utente. E' importante che gli utenti si sentano a proprio agio con il sistema di identificazione. I tempi di risposta del sistema devono essere molto brevi.
- Accurato. L'accuratezza è spesso misurata tramite due fattori: FAR (False Accept Rate, utenti che accedono al sistema senza essere autorizzati) e FRR (False Reject Rate, utenti che sono rifiutati dal sistema pur essendo autorizzati).

Nel seguito vedremo alcune delle tecniche di riconoscimento basate su biometrie attualmente utilizzate. Nella valutazione di queste tecniche dovremo tener conto dei seguenti parametri: tempi di riconoscimento, costi dell'attrezzatura, fattore psicologico, FAR e FRR.

Impronte digitali

L'utente pone il proprio dito su una apposita superficie in grado di campionare l'impronta. Poiché la posizione del dito (e quindi dell'impronta) può variare di volta in volta è necessario che il dispositivo di scansione permetta all'immagine acquisita di effettuare piccoli angoli di rotazione. Nell'immagine acquisita vengono inoltre isolati i tratti particolari dell'impronta e ne viene individuata la posizione; questi dati verranno poi confrontati con quelli dal database contenente le impronte degli utenti autorizzati.

Gli svantaggi di un sistema di autenticazione basato sul riconoscimento delle impronte digitali stanno, per prima cosa, nel elevato costo del sistema stesso. Inoltre molti sistemi di questo tipo hanno difficoltà nel riconoscere ed autenticare utenti che si sono procurati ferite alle dita (il FRR aumenta). Bisogna infine considerare che molti utenti spesso manifestano una certa riluttanza, a livello psicologico, nel fornire le proprie impronte digitali, associando la procedura di autenticazione alla schedatura dei criminali!

Geometria della mano

Si basa sulla misurazione delle caratteristiche fisiche della mano per verificare l'identità di un utente. Tipicamente vengono misurate la lunghezza e lo spessore delle dita e l'ampiezza della mano. Generalmente un sistema di identificazione di questo tipo è ben accettato dagli utenti, ma la sicurezza che esso offre è fonte di discussione.

Analisi dell'iride

Concettualmente è simile alla scansione delle impronte digitali, ma la campionatura viene effettuata sui tratti principali dell'iride, tramite un apposito scanner retinico. Le informazioni raccolte con questo metodo sono molto più precise rispetto alla analisi delle impronte digitali e possono essere fino a sei volte più numerose.

Riconoscimento vocale

Il dispositivo che esegue il riconoscimento vocale confronta le caratteristiche del suono con i dati di relativi al campionamento vocale di ogni utente, presenti in un database. E' importante creare le condizioni giuste per un corretto riconoscimento, eliminando possibili interferenze e disturbi ambientali. Generalmente i sistemi basati su riconoscimento vocale presentano lo svantaggio di spendere troppo tempo nella fase di interazione con l'utente e anche il processo di analisi e riconoscimento della voce è spesso molto lento. Inoltre la voce è spesso condizionata dallo stato fisico della persona e persino particolari stati emotivi possono influenzare la qualità della voce costringendo il sistema a chiedere la ripetizione della procedura di autenticazione: tutto ciò contribuisce a diminuire il troughput e causare stress nell'utente.

Altri sistemi di identificazione biometrica sono:

- riconoscimento della firma
- riconoscimento della calligrafia
- caratteristiche di battitura
- riconoscimento del volto