


Security in the TCP/IP stack



HTTP	SMTP	FTP
TCP		
IP/IPSec		

Network layer

HTTP	SMTP	FTP
SSL, TLS		
TCP		
IP		


Transport Layers

	PGP	SET
Kerberos	SMTP	HTTP
UDP	TCP	
IP		

Application layer

SSL
09/05/2018
3

La suite di protocolli SSL



Applicazioni			
Protocollo Handshake	Protocollo Change Cipher	Protocollo Alert	HTTP
Protocollo Record			
TCP			
IP			

SSL
09/05/2018
4

References



- **Secure Socket Layer (SSL)**
 - Netscape
 - <http://wp.netscape.com/eng/ssl3/>
- **Transport Layer Security (TLS)**
 - Based on SSL v3.0
 - RFC 2246
 - <ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt>
 - Same design as SSL but different algorithms

SSL

09/05/2018

5

History of the protocol



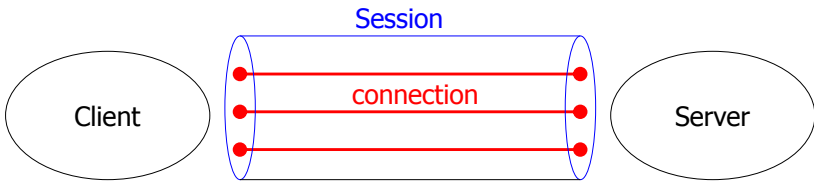
- **SSL**
 - Developed by Netscape in mid 1990s
 - SSLv1 broken at birth (never publicly released)
 - SSLv2 flawed, now IETF-deprecated (RFC 6176)
 - SSLv3 still widely supported (since 1996)
- **TLS**
 - IETF-standardized version of SSL.
 - TLS 1.0 in RFC 2246 (1999), based on SSLv3 but NOT interoperable
 - TLS 1.1 in RFC 4346 (2006).
 - TLS 1.2 in RFC 5246 (2008).

SSL

09/05/2018

6

Session vs connection

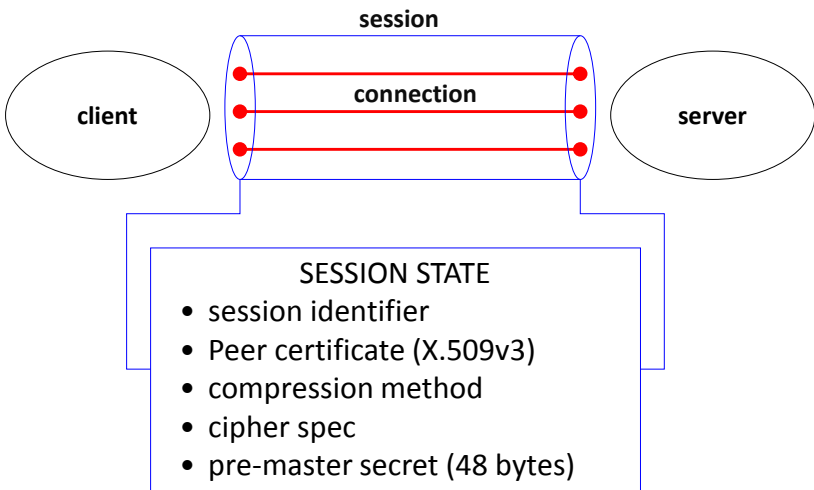


The diagram illustrates a 'Session' as a blue-outlined cylinder containing three red horizontal lines representing 'connections'. On the left end of the cylinder is a red dot, and on the right end are three red dots, one for each connection line. The cylinder is labeled 'Session' at the top. To the left of the cylinder is an oval labeled 'Client', and to the right is an oval labeled 'Server'.

- A **session** is a logical association between a Client and a Server
 - Created by the **Handshake protocol**
 - Define a set of **crypto pars** that can be shared by multiple connections
 - Avoid **expensive** negotiation of crypto pars for each connection

SSL 09/05/2018 7

Session vs connection



The diagram illustrates a 'Session' as a blue-outlined cylinder containing three red horizontal lines representing 'connections'. On the left end of the cylinder is a red dot, and on the right end are three red dots, one for each connection line. The cylinder is labeled 'session' at the top. To the left of the cylinder is an oval labeled 'client', and to the right is an oval labeled 'server'. Below the cylinder, a blue box labeled 'SESSION STATE' contains a list of items. Lines connect the top and bottom of the 'SESSION STATE' box to the bottom of the 'session' cylinder.

SESSION STATE

- session identifier
- Peer certificate (X.509v3)
- compression method
- cipher spec
- pre-master secret (48 bytes)

SSL 09/05/2018 8

Session vs connection

CONNECTION STATE

- Server random number (nonce)
- Client random number (nonce)
- Server write MAC secret
- Client write MAC secret
- Server write key
- Client write key
- Initialization vectors
- Sequence numbers

SSL 09/05/2018 9

The Record Protocol

Payload

Fragmentation
(max 2^{14} bytes)

Compression
max $2^{14} + 1024$ bytes

MAC

Encryption

Heading
(max $2^{14} + 2048$)

The Record Protocol encapsulates data from higher layers so guaranteeing confidentiality and integrity of communication

SSL 09/05/2018 10

The Record Protocol



- **Fragmentation** fragments application data in blocks whose size is $\leq 2^{14}$ -bytes
- **Compression** must be lossless and must not increase the block size more than 1024 bytes (default = null)
- MAC uses **the [Server|Client] write MAC key**, sequence number, compressed block, padding
- Encryption uses the **[Server|Client] write key**
 - Block and stream ciphers
 - Does not increase the content size more than 1024 bytes
- Total length of a fragment must be $\leq 2^{14} + 2048$ bytes

SSL

09/05/2018

11

The Record Protocol



Header


- **Payload type**
 - change cipher, alert, handshake, application_data
 - Application data is opaque to SSL
- **Major Version**
 - SSLv3 => 3
- **Minor Version**
 - SSLv3 => 0
- **Compressed length**
 - Fragment size $\leq 2^{14} + 2048$

SSL

09/05/2018

12


Payload types



<p>1byte</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td style="text-align: center;">1</td></tr> </table> <p>Protocollo Change Cipher</p>	1	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">1byte</td> <td style="width: 33%; text-align: center;">3byte</td> <td style="width: 33%; text-align: center;">≥0byte</td> </tr> <tr> <td style="border: 1px solid black; text-align: center;">tipo</td> <td style="border: 1px solid black; text-align: center;">lunghezza</td> <td style="border: 1px solid black; text-align: center;">contenuto</td> </tr> </table> <p>Protocollo Handshake</p>	1byte	3byte	≥0byte	tipo	lunghezza	contenuto
1								
1byte	3byte	≥0byte						
tipo	lunghezza	contenuto						
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">1byte</td> <td style="width: 50%; text-align: center;">1byte</td> </tr> <tr> <td style="border: 1px solid black; text-align: center;">livello</td> <td style="border: 1px solid black; text-align: center;">allarme</td> </tr> </table> <p>Protocollo Alert</p>	1byte	1byte	livello	allarme	<p style="text-align: center;">≥0byte</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td style="text-align: center;">Contenuto opaco</td></tr> </table> <p>Protocollo Applicativo (HTTP,...)</p>	Contenuto opaco		
1byte	1byte							
livello	allarme							
Contenuto opaco								

SSL **09/05/2018** **13**

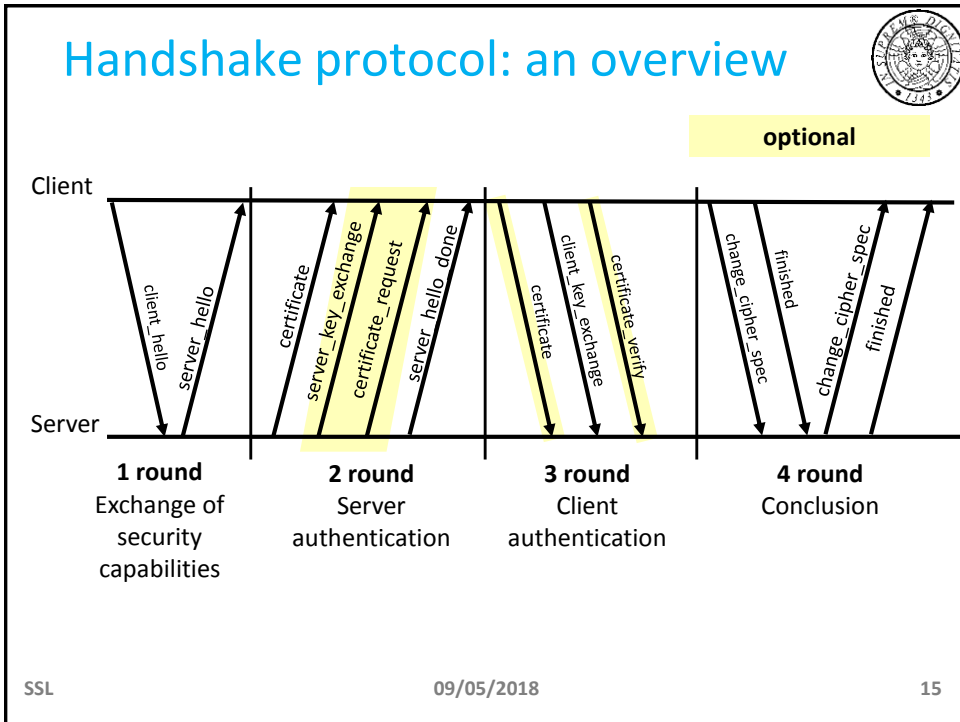
The other protocols in the SSL suite



- The **change cipher spec protocol** consists in one single message (cleartext) to make the negotiated crypto suite operational
- The **alert protocol** notifies alarms to peers

FATAL ALARMS unexpected_message bad_record_mac decompression_failure handshake_failure illegal_parameter	OTHER ALARMS no_certificate bad_certificate unsupported_certificate certificate_revoked certificate_expired certificate_unknown close_notify
--	--

SSL **09/05/2018** **14**



Set of messages

TIPO	CONTENUTO
<code>hello_request</code>	No pars
<code>client_hello</code>	version, nonce, session id, cipher suite, compression method
<code>server_hello</code>	version, nonce, session id, cipher suite, compression method
<code>certificate</code>	Certificate X.509v3
<code>server_key_exchange</code>	Pars, signature
<code>certificate_request</code>	Type, authority
<code>server_hello_done</code>	No pars
<code>certificate_verify</code>	signature
<code>client_key_exchange</code>	Pars, signature
<code>finished</code>	hash

SSL 09/05/2018 17

The Handshake Protocol



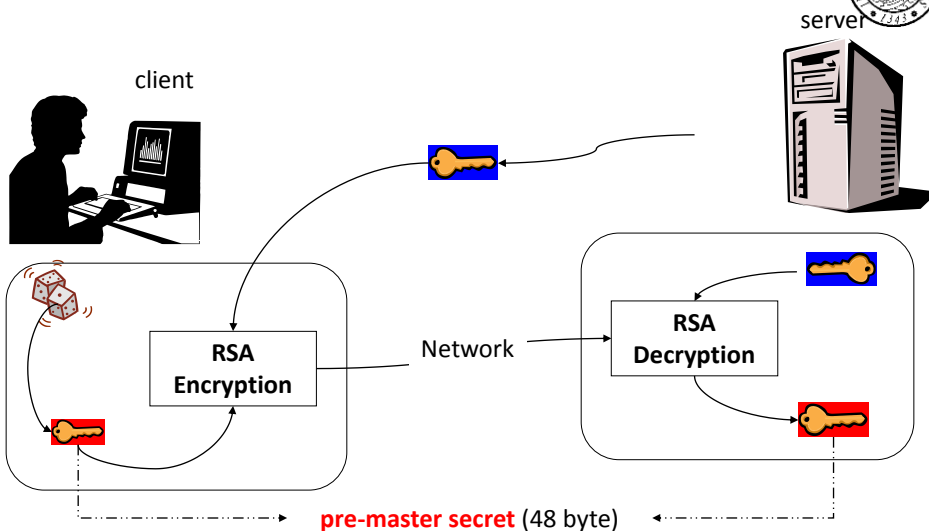
- Establish a secure session
 - Client and server authenticate each other
 - Client and server negotiate the cipher suite
 - Key establishment scheme;
 - Encryption scheme (used in the RP)
 - MAC (used in the RP)
 - Client and server establish a shared secret
 - E.g., pre-master secret
- Before any application data
- The most complex part of SSL

SSL

09/05/2018

18

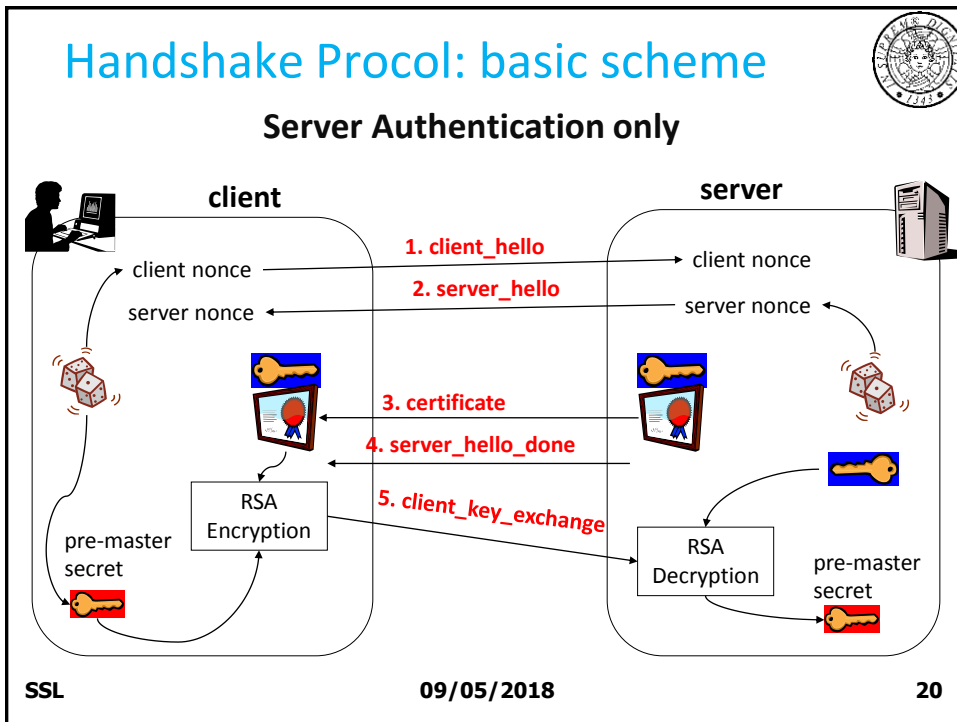
Handshake Protocol: basic scheme



SSL

09/05/2018

19





Hello message

- By means of **Hello** msgs, Client and Server tell each other what they are able to do
 - client_hello and server_hello
 - SSL version
 - Random: timestamp [32 bit] + random bytes[28]
 - Session id
 - Cipher suite
 - Compression method

SSL 09/05/2018 21



Cipher suite



- Cipher suite is a list of algorithm *tuples*
- A *tuple* specifies
 - Key establishment
 - cipher, cypher type, IV size, isExportable
 - MAC, hash size
 - key material
- Some tuples are standard
 - E.g., `SSL_RSA_WITH_3DES_EDE_CBC_SHA`

SSL 09/05/2018 22


Cipher suite



- Supported key establishment schemes
 - RSA (certified)
 - Fixed Diffie-Hellman (certified; fixed pub pars)
 - Ephemeral Diffie-Hellman (signed, dynamic pub pars)
 - Anonymous Diffie-Hellman (non authenticated)
- Supported ciphers
 - RC4, RC2, DES, 3DES, IDEA, ...
- Supported MAC
 - MD5, SHA-1

SSL 09/05/2018 23


Client_key_exchange message



- The message format depends on the chosen key establishment
 - **RSA** – pre-master secret
 - **Anonymous or ephemeral DH** – $(p, g, Y)_{\text{clnt}}$
 - **Fixed DH** – void payload, public pars will be sent in a **certificate** message

SSL 09/05/2018 24

Key generation



Server/client side

Pdefined data

pre-master secret

client nonce

server nonce

In the Hello msgs

Pre-master is an entropy source

Hash Multi-step

key block

Server write MAC secret

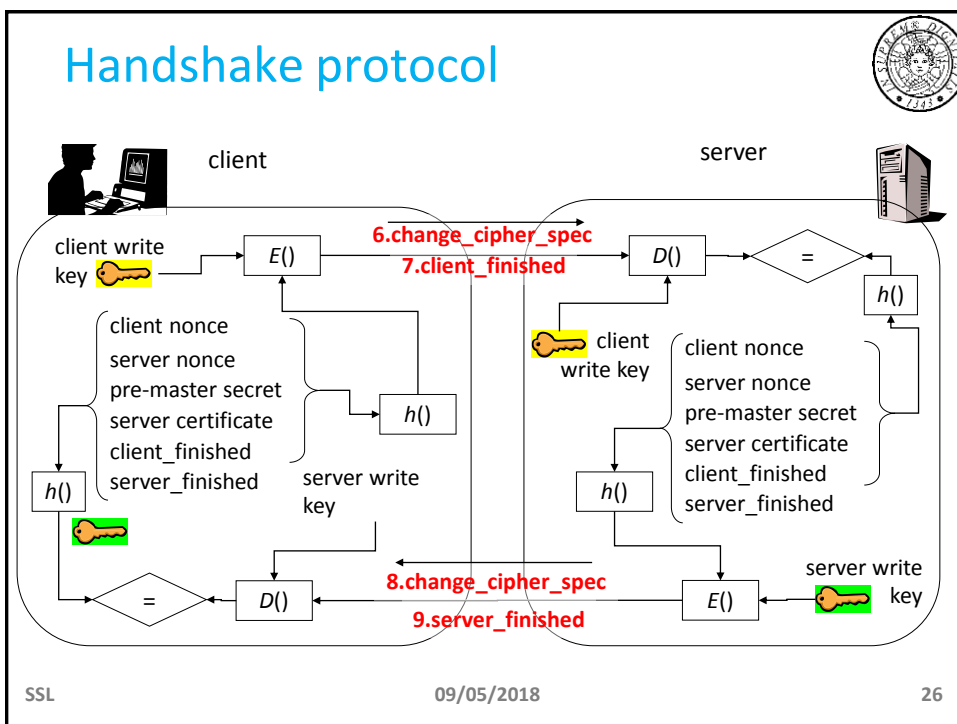
Client write MAC secret

Server write key

Client write key

altro...

SSL 09/05/2018 25



- ### Server_key_exchange message (opt)
- The optional message **server_key_exchange** is not necessary in the following cases:
 - **Fixed Diffie-Hellmann, RSA encryption**
 - **pubK** is in the **certificate** message
 - In contrast, it is necessary in the following cases:
 - **Anonymous DH** - p, g, Y_{svr}
 - **Ephemeral DH** - $p, g, Y_{svr}, S_{svr}(p||g||Y_{svr})$
 - **RSA (dig sig only)** - $tempPubK_{svr}, S_{svr}(tempPubK_{svr})$
- SSL 09/05/2018 27

certificate_request message



- Server may issue a **certificate_request** unless anonymous Diffie-Hellmann is used
- The message has two parameters
 - **Certificate_type**: type of digital signature and its use
 - (RSA | DSS) + (only signature | fixed Diffie-Hellmann | Ephemeral DH)
 - **Certificate_authorities**: acceptable certification authorities

SSL

09/05/2018

28

Client authentication

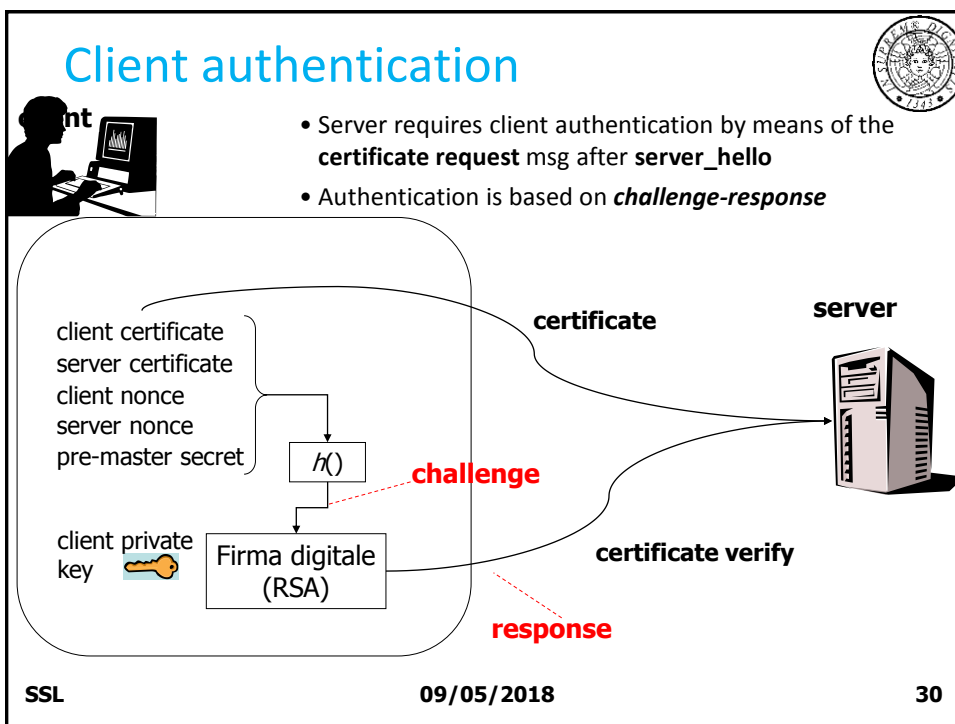


- \mathcal{CP} authenticates the server by default
- How can the client be authenticated?
 - Typically, the client is authenticated at the application level
 - password, credit card number (!!),...
- However, \mathcal{CP} also supports client authentication w.r.t. the server

SSL

09/05/2018

29



Security



- Handshake Protocol
 - Nonces in client hello and server hello
 - Nonces make it possible generate a fresh master secret and avoid replay attacks
 - Certificates
 - Avoid MIM
 - Random quantities
 - Pre-master secret and nonces must be unpredictable
- Record Protocol
 - A block is numbered, authenticated and encrypted
 - Avoid block replay, reordering and substitution
 - Cipher “protects” the MAC

SSL

09/05/2018

32

SSL: Pros and Cons



- Pros
 - SSL is a well-designed, robust and secure protocol
- Cons
 - SSL protects communication only
 - User has to check security parameters
 - SSL is vulnerable to name spoofing

SSL

09/05/2018

33



SSL

HISTORY: PITFALLS AND ATTACKS

SSL

09/05/2018

34

Random generator in SSL v2.0

(on the importance of a good SPRBG)



- Pseudo-Random Bit Generator
 - $\text{keystream} = H(\text{tod} || \text{pid} || \text{ppid})$
 - tod = time of day
 - pid = process id
 - ppid = parent process id
- Entropy of the triple is 47-bit => seed can be guessed in 25 s
- A more sophisticated attack based on system observation may be even more effective

SSL

09/05/2018

35

Most famous attacks



- **Browser Exploit Against SSL/TLS (BEAST) attack**
 - Weakness of CBC in TLS 1.0 (2011)
- **Compression Ratio Info-leak Made Easy (CRIME)**
 - Side-channel attack based on the compressed size of HTTP request (2012)
- **Lucky13 attack**
 - Timing side-channel attack with CBC (2013)
- **Heartbleed attack**
 - Buffer over-read attack (2014)

SSL

09/05/2018

36

SSL


ON USING SSL IN E-COMMERCE



SSL

09/05/2018

37



SSL in action

Sicurezza in ogni istante


Tutti i nostri siti internet utilizzano il **protocollo di comunicazione SSL/TLS**, che ti garantiscono una comunicazione cifrata in ogni istante.

Verifica sempre che l'indirizzo del sito inizi con https://... (si, con la "esse" finale).

Is it really true?

Cos'è il protocollo SSL (Secure Sockets Layer)
Scopri cos'è il protocollo di sicurezza SSL


Il protocollo SSL è attualmente lo standard di sicurezza per le transazioni via web utilizzato nelle connessioni utente-azienda di massima sicurezza e riservatezza quali le operazioni bancarie, i pagamenti, l'invio di dati sensibili. Inoltre, l'utente che si connette a un dominio con connessione SSL è in grado di verificare con assoluta certezza l'autenticità del webserver e quindi l'effettiva connessione al sito desiderato.



Il protocollo SSL fornisce le seguenti funzionalità di sicurezza:

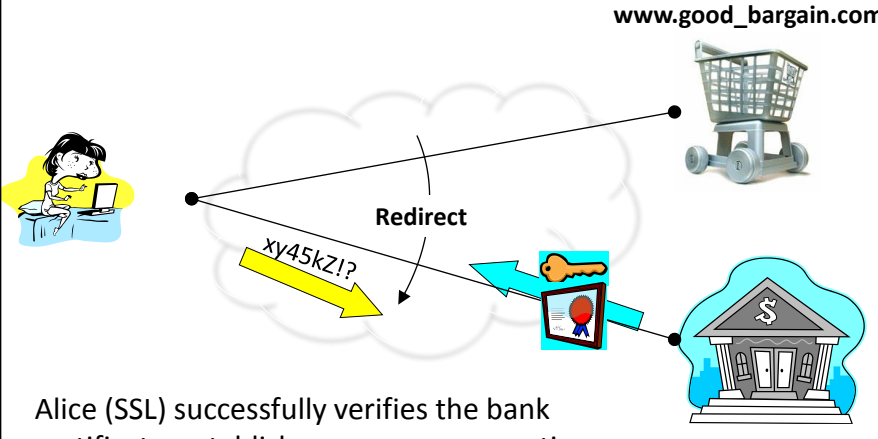
- riservatezza del messaggio scambiato nella comunicazione;
- integrità del contenuto del testo inviato durante la transazione;
- autenticazione del web server da parte dei browser più diffusi;
- autenticazione del browser, abbinando al certificato per web server l'uso di un certificato anche per il client.

SSL
09/05/2018
38



MIM with SSL (1/2)

www.good_bargain.com



Alice (SSL) successfully verifies the bank certificate, establishes a secure connection, and sends her pwd/PIN along the connection

www.bank.com

SSL
09/05/2018
39

MIM with SSL (2/2)

Alice is deceived by social engineering techniques

SSL

09/05/2018

40

Is it the right certificate?


- **SSL operates at the transport level rather than the application level**
- **Browser controls**
 - Browser warns user if the URL known to the browser is not equal to that in the certificate (**mismatch**)
 - Browser warns user whether a certificate is signed by an unknown CA (**self-signed certificates**)
 - The user has the last word
 - The **clickthrough** phenomenon
 - Does the user understand security?
 - Usability vs security
 - These controls may be not sufficient for all web applications
 - Browser have a largely variable behaviour in this respect(*)
 - What to warn; when to warn

SSL

09/05/2018

41


Risk allocation





- PIN/PWD is a shared secret
- In a home banking contract, the user commits himself to protect the PIN/PWD confidentiality
- In a fraud it is evident that the PIN/PWD confidentiality has been violated
- Who is liable for?

SSL 09/05/2018 42


E-payment by credit card







SSL

nr. 5490 1234 5678 valid thru 00/00



- Credit card number is **public**
- Is the sender Richard Cronwell?
 - How can the merchant discriminate between the two situations?



nr. 5490 1234 5678 valid thru 00/00

SSL 09/05/2018 43

E-payment by Credit Card



Decreto legislativo 22 maggio 1999, n. 185, di attuazione della direttiva 97/7/CE



Art. 8 - Pagamento mediante carta

1. Il consumatore può effettuare il pagamento mediante carta ove ciò sia previsto tra le modalità di pagamento, da comunicare al consumatore al sensi dell'articolo 3, comma 1, lettera e), del presente decreto legislativo.
2. L'istituto di emissione della carta di pagamento riaccredita al consumatore i pagamenti dei quali questi dimostri l'eccedenza rispetto al prezzo pattuito ovvero l'effettuazione mediante l'uso fraudolento della propria carta di pagamento da parte del fornitore o di un terzo, fatta salva l'applicazione dell'articolo 12 del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197. L'istituto di emissione della carta di pagamento ha diritto di addebitare al fornitore le somme riaccreditate al consumatore.

SSL

09/05/2018

44

E-payment by Credit Card



- **Gli istituti di emissione**, cui compete l'autorizzazione dell'operazione di pagamento, nonché i soggetti che rendono tecnicamente possibile la transazione on-line, **sono tenuti a controllare la correttezza del numero della carta e la data della sua scadenza ma non anche la corrispondenza tra il numero fornito e l'effettivo titolare**



- Gli istituti di emissione verificano la corrispondenza tra numero della carta di credito comunicato per effettuare una transazione on-line ed il nominativo fornito da colui che la effettua.

Ad esempio, l'**Address Verification Service (AVS)** verifica che l'indirizzo di consegna sia quello con cui il possessore della carta è registrato

- In Europa il grado di sicurezza nelle transazioni on-line è minore e quindi il commercio elettronico è destinato ad incontrare resistenze anche da parte dei fornitori di che sopportano rischi elevati

SSL

09/05/2018

45

E-payment by Credit Card: risk allocation



- Il fornitore di beni o servizi on-line è **tenuto ad accollarsi il rischio** della rivalsa degli istituti di emissione qualora, in caso di uso fraudolento della carta, questi riaccreditano le corrispondenti somme al legittimo titolare.
 - La legge **non consente** al fornitore di liberarsi dall'obbligo della restituzione delle somme agli istituti di emissione qualora dimostri
 1. di avere usato tutte le cautele necessarie e possibili ad evitare l'uso fraudolento della carta di credito
 2. che il fatto è stato causato dal caso fortuito.
 - I fornitori dovranno usare tutte le cautele del caso per potere, nel caso di uso fraudolento di carte di credito, perlomeno rintracciare l'illegittimo utilizzatore e rivalersi su questo.
- Le conseguenze derivanti dall'addebito delle somme riaccreditate al titolare della carta potrebbero poi essere annullate contraendo una **assicurazione** a copertura dei danni (economici) derivanti da tale circostanza.

SSL

09/05/2018

46

E-payment by Credit Card



Foglio informativo sulle operazioni e servizi offerti alla clientela (CariPrato)

Caratteristiche e rischi tipici

Struttura e funzione economica

CARTE DI DEBITO e CARTE DI CREDITO

Strumenti di pagamento rilasciabili a clienti della Banca che consentono:

- Acquisto di beni;
- Prestazione di servizio presso esercenti convenzionati.
- Ottenimento di contante presso sistemi automatici o sportelli bancari convenzionati.

Funzione Bancomat: è il servizio in forza del quale la banca (emittente), attraverso il rilascio di una Carta, consente al correntista (c.d. "titolare") di effettuare prelievi di denaro — entro massimali di utilizzo stabiliti dal contratto — presso sportelli automatici (ATM) contraddistinti dal marchio Bancomat, digitando un codice segreto (c.d. P.I.N., "Personal Identification Number").

Funzione PagoBANCOMAT: è il servizio in forza del quale il correntista può compiere acquisti di beni e servizi presso esercenti commerciali convenzionati che espongono il marchio "PagoBANCOMAT", digitando il citato codice segreto.

L'utilizzo del sistema di pagamento è consentito nei limiti giornaliero e mensile, entro limiti di importo contrattualmente previsti, determinato dal momento dell'emissione e dalla capienza di conto corrente al momento dell'addebito.

Principali rischi (generici e specifici)

Il rischio relativo ad eventuali utilizzi fraudolenti effettuati con le Carte di Pagamento è limitato a 130 € per evento se il Titolare ha ottemperato e rispettato quanto indicato dalla Raccomandazione della Commissione Europea del 30 giugno 1997 n. 97/459.

In sintesi il titolare è tenuto a:

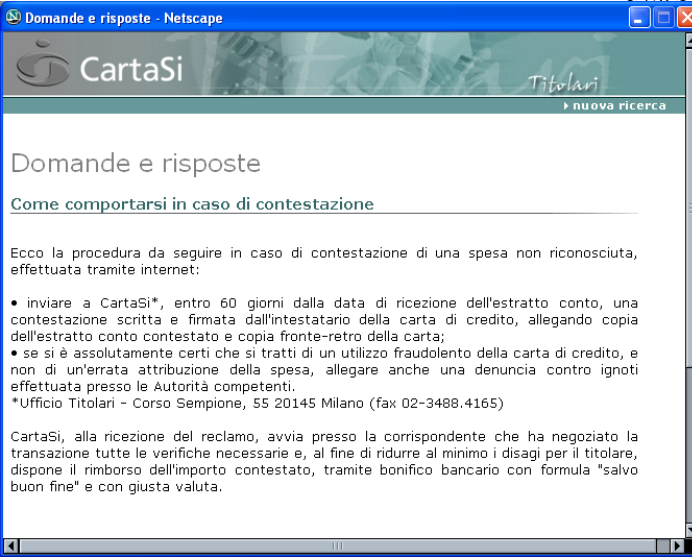
- Firmare la carta nel caso che la stessa sia munita di apposita banda di scrittura;
- Osservare la massima attenzione nella custodia della carta e PIN e la massima riservatezza nell'uso del medesimo;
- Bloccare la carta nel caso di furto, smarrimento o uso fraudolento della medesima, confermando l'evento con denuncia o dichiarazione di smarrimento.

SSL

09/05/2018

47

E-payment by Credit Card



Domande e risposte

Come comportarsi in caso di contestazione

Ecco la procedura da seguire in caso di contestazione di una spesa non riconosciuta, effettuata tramite internet:

- inviare a CartaSi*, entro 60 giorni dalla data di ricezione dell'estratto conto, una contestazione scritta e firmata dall'intestatario della carta di credito, allegando copia dell'estratto conto contestato e copia fronte-retro della carta;
- se si è assolutamente certi che si tratti di un utilizzo fraudolento della carta di credito, e non di un'errata attribuzione della spesa, allegare anche una denuncia contro ignoti effettuata presso le Autorità competenti.

*Ufficio Titolari - Corso Sempione, 55 20145 Milano (fax 02-3488.4165)

CartaSi, alla ricezione del reclamo, avvia presso la corrispondente che ha negoziato la transazione tutte le verifiche necessarie e, al fine di ridurre al minimo i disagi per il titolare, dispone il rimborso dell'importo contestato, tramite bonifico bancario con formula "salvo buon fine" e con giusta valuta.


SSL 09/05/2018 48

Secure Electronic Transactions

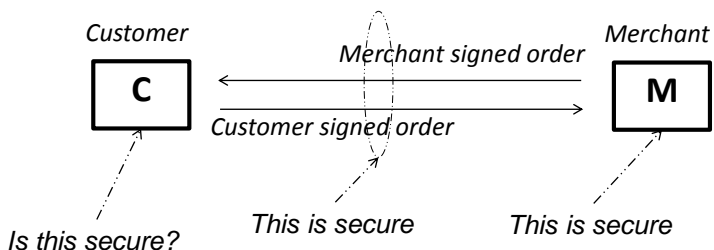
- SET was built to answer to these problems
- SET has been designed and implemented in the late 90's
 - Commissioned by Visa and Mastercard
 - Involves all (IBM, Microsoft,...)
- SET was a failure
 - Too "heavy"
 - Too expensive
 - Specifications takes more than 1000 pages (!)
- We are interested in the risk allocation

SSL 09/05/2018 49

Secure Electronic Transactions




- SET requires a PKI in place
- A (privK, pubK) pair is stored at M and C
- If an order is signed by your key you cannot repudiate it
 - The risk is allocated on the customer
- M and C are assumed trusted devices!
 - Stealing a privK is equivalent to stealing a file

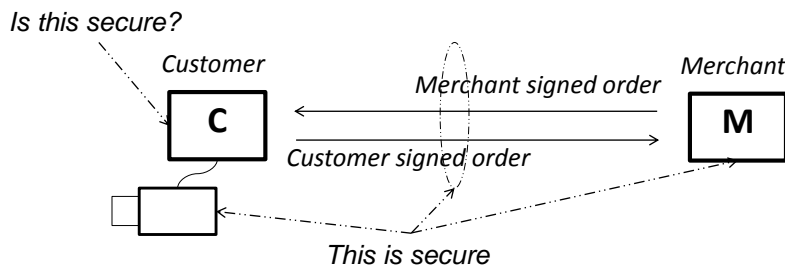


SSL 09/05/2018 50

Secure Electronic Transactions




- Do smart cards help?
 - Loosing a piece of plastic vs. loosing a file
 - Is what you see what you sign?



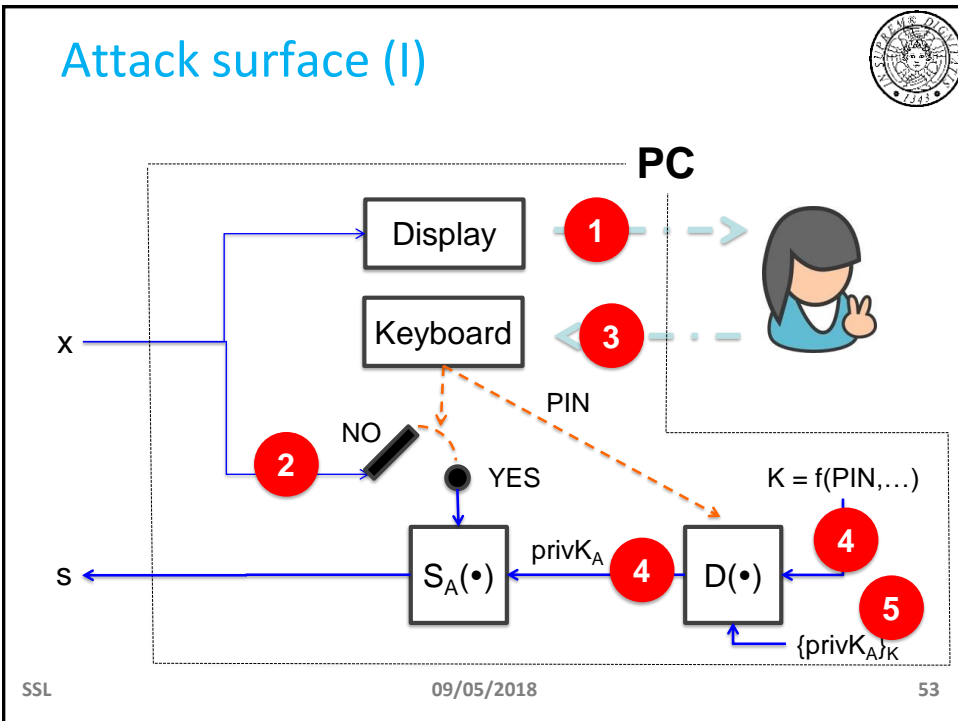
SSL 09/05/2018 51

Dancing on the cliff rim



1. The owner keeps secret the **privK**
2. If $V(\text{pubK}, s) == \text{True}$ then **s** was made by **privK**
3. A valid, unrevoked certificate links **pubK** to a name
4. Certification process links name to owner
5. Therefore the owner has generated signature **s** (and he is responsible of it)

SSL 09/05/2018 52



Attack surface (II)



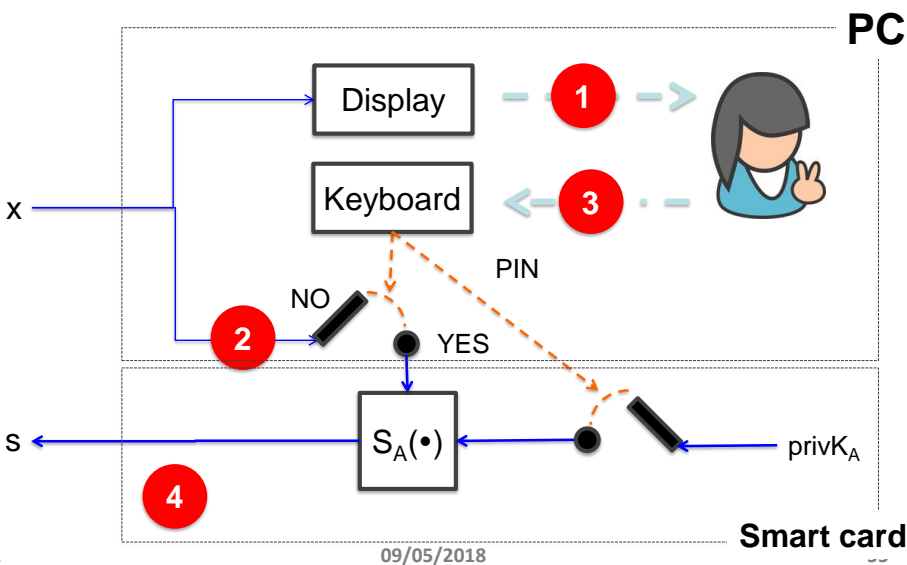
1. The attacker shows Alice x' instead of x
2. The attacker shows Alice x but signs x'
3. The attacker changes Alice's decision or steals Alice's PIN
4. The attacker steals the private key
5. The attacker steals the encrypted private key for an offline attack

SSL

09/05/2018

54

Attack surface (III)



SSL

09/05/2018

Smart card

Attack surface (IV)



1. The attacker shows Alice x' instead of x and trick Alice into signing x
2. The attacker replaces x with x'
3. The attacker changes Alice's decision or steals Alice's PIN
4. The attacker steals and attacks the smart card
 1. Physical attack
 2. Side-channel attack