Protokol SSL

Petr Dvořák

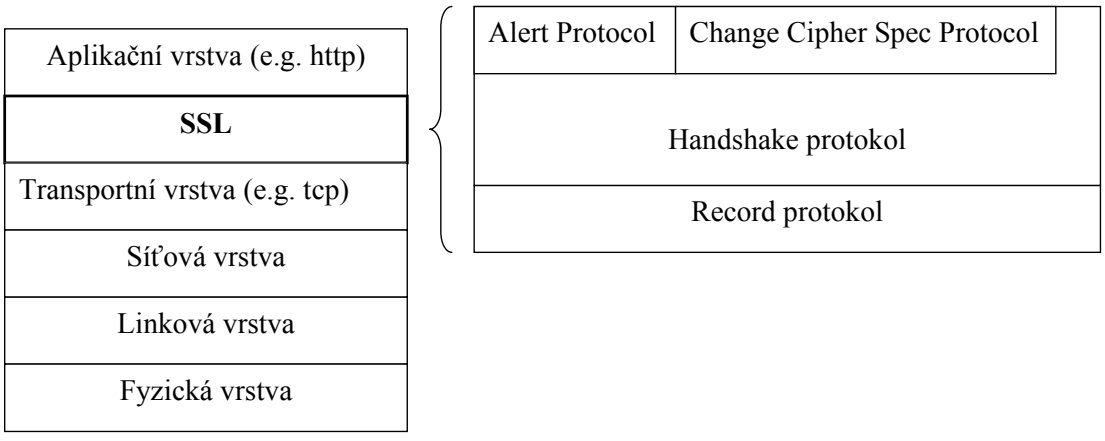
Obsah prezentace

- Co je SSL
- Popis protokolu
- Ukázka
- Použití v praxi

Co je SSL

- SSL zajišťuje bezpečnou komunikaci
- SSL specifikuje, jak kombinovat jiné protokoly pro:
  - autentizaci
  - šifrování
  - kompresi

Protokolový zásobník



Record protokol

K čemu slouží

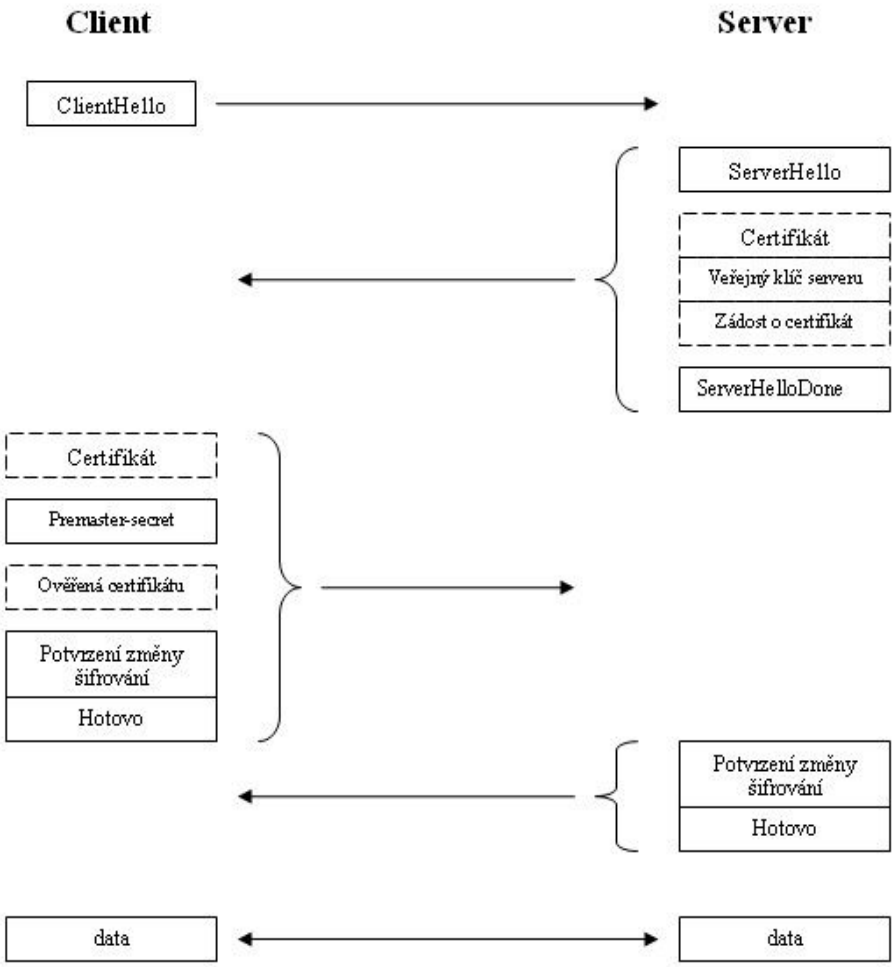
- Příprava pro odeslání
  - rozděluje data do bloků - fragmentace
  - volitelně data zakomprimuje
  - vypočte zabezpečovací informaci (MAC)
  - šifruje
  - předá nižší vrstvě
- Zpracování přijatých dat

Handshake protokol

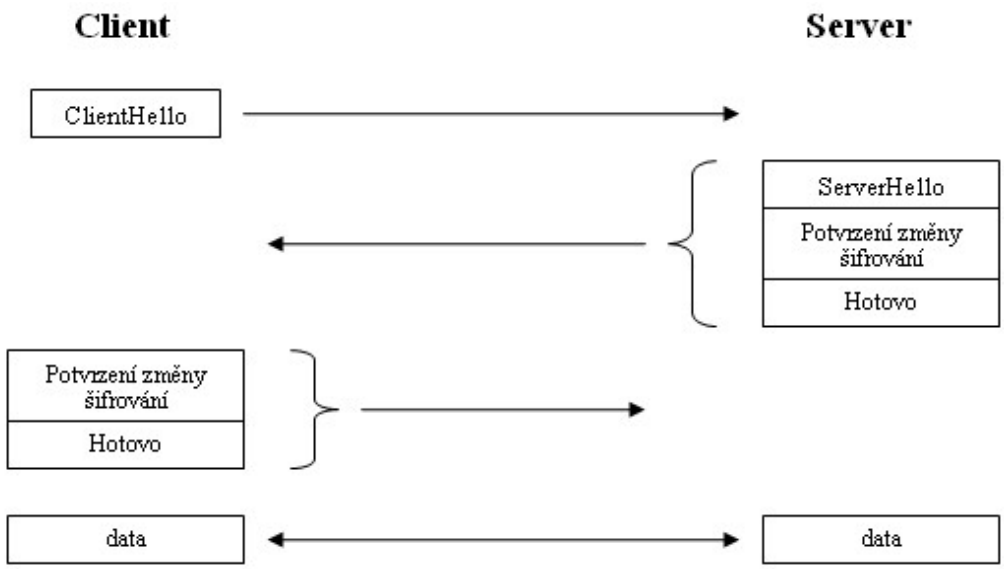
- navázání spojení
- vyjednání parametrů
- identifikace komunikujících
- subprotokoly
  - Alert
    - fatální chyby
    - ostatní
  - Change Cipher Spec

Handshake protokol

- Přenášené informace
  - identifikátor spojení
  - certifikát počítače, s nímž se komunikuje
  - způsob komprese dat
  - algoritmy pro šifrování a hešování
  - master secret
  - lze vytvořit další spojení?
  - …
- Plný handshake
- Zjednodušený handshake



Zjednodušený handshake



Autentizace a výměna klíčů

- DH
- DHE – přechodná DH
- RSA

Modely důvěry

- O co jde?
- Typy
  - Hierarchický
    - Certifikační autorita
    - Známá serveru i klientovi
  - Distribuovaný
    - peer-to-peer
- Výhody/nevýhody

Šifrování dat

- Blokové šifry
  - RC2
  - DES
  - 3DES
  - IDEA
  - AES
- Proudové šifry
  - RC4

Hešování

- Co se hešuje
- Algoritmy
  - MD5
  - SHA-1

Zachycení komunikace

- Jpcap
  - http://netresearch.ics.uci.edu/kfujii/jpcap/doc/index.html

SSL knihovny

- OpenSSL
- GnuTLS
- NSS
- JSSE

OpenSSL server/klient

- Instalace OpenSSL
- Vygenerování klíčů (RSA, délka 1024):

```
openssl req -newkey rsa:1024 -nodes -keyout server.key -out server.req
```

- Vygenerování certifikátu (X.509):

```
openssl x509 -req -signkey server.key -in server.req -out server.pem
```

Srovnání s SSL a TLS

- Jiný algoritmus výpočtu MAC
- V TLS není Fortrezza
- Do Alert protokolu bylo přidáno mnoho nových zpráv.
- V TLS není nutné znát všechny certifikáty až ke kořenové certifikační autoritě. Stačí použít některou mezilehlou
- Padding blokových šifer v modu CBC je proměnný
- SSL se jako standard již nerozvíjí
- TLS je mnohem striktnější
- + další drobné rozdíly

Shrnutí

- TLS zajišťuje bezpečnou komunikaci
- TLS spravuje informace pro bezpečné spojení mezi klientem a serverem
- TLS specifikuje, jak kombinovat jiné protokoly pro:
  - autentizaci
  - šifrování
  - kompresi

Závěr

- http://webcity.wz.cz/psi/ssl.zip
- dotazy