TLS pro SIP server

Jakub Mareček

PV177 - Laboratoř pokročilých síťových technologií

22. října 2009

Původní text: Jan Růžička

Úvod

- pro IP telefonii přes SIP používáno většinou UDP místo TCP
- autentizace pro SIP je realizována přes HTTP Digest
  - používán pro autentizaci uživatelů i pro komunikaci mezi servery
  - málo bezpečné
  - heslo posíláno ve formě hashe (MD5)
  - používá se nonce - jednorázový identifikátor sekvence
  - server nevyžaduje všechny hodnoty - snadné podvrhnout MitM
- jedním z řešení je použití TLS - Transport Layer Security
  - kryptografický protokol nahrazující SSL
  - zabraňuje odposlouchávání a falšování zpráv
  - typicky autentizován pouze server
  - autentizace obou stran - vzájemná autentizace

Ukázka hlavičky pro HTTP Digest

```
GET /dir/index.html HTTP/1.0 Host: localhost
Authorization: Digest username="Mufasa",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
uri="/dir/index.html", qop=auth, nc=00000001,
cnonce="0a4f113b",
response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

TLS - jak funguje

ClientHello první zpráva od klienta (verzi TLS, náhodné číslo seznam šifrovacích sad a kompresí)

ServerHello první odpověď serveru (zvolený protokol, šífrovací sadu a kompresi, náhodné číslo)

Certificate server posílá certifikát

CertificateRequest nepovinný - pouze pokud server vyžaduje vzájemnou autentizaci

ServerHelloDone server ukončil domluvu na autentizačních metodách

ClientKeyExchange klient pošle buď klíč nebo je prázdná (dle šifry)

TLS - jak funguje 2

Master Secret server i klient jej počítají z PreMasterSecret, k dalším klíčům

ChangeCipherSpec zpráva od klienta, že všechna data jsou odteď šifrována

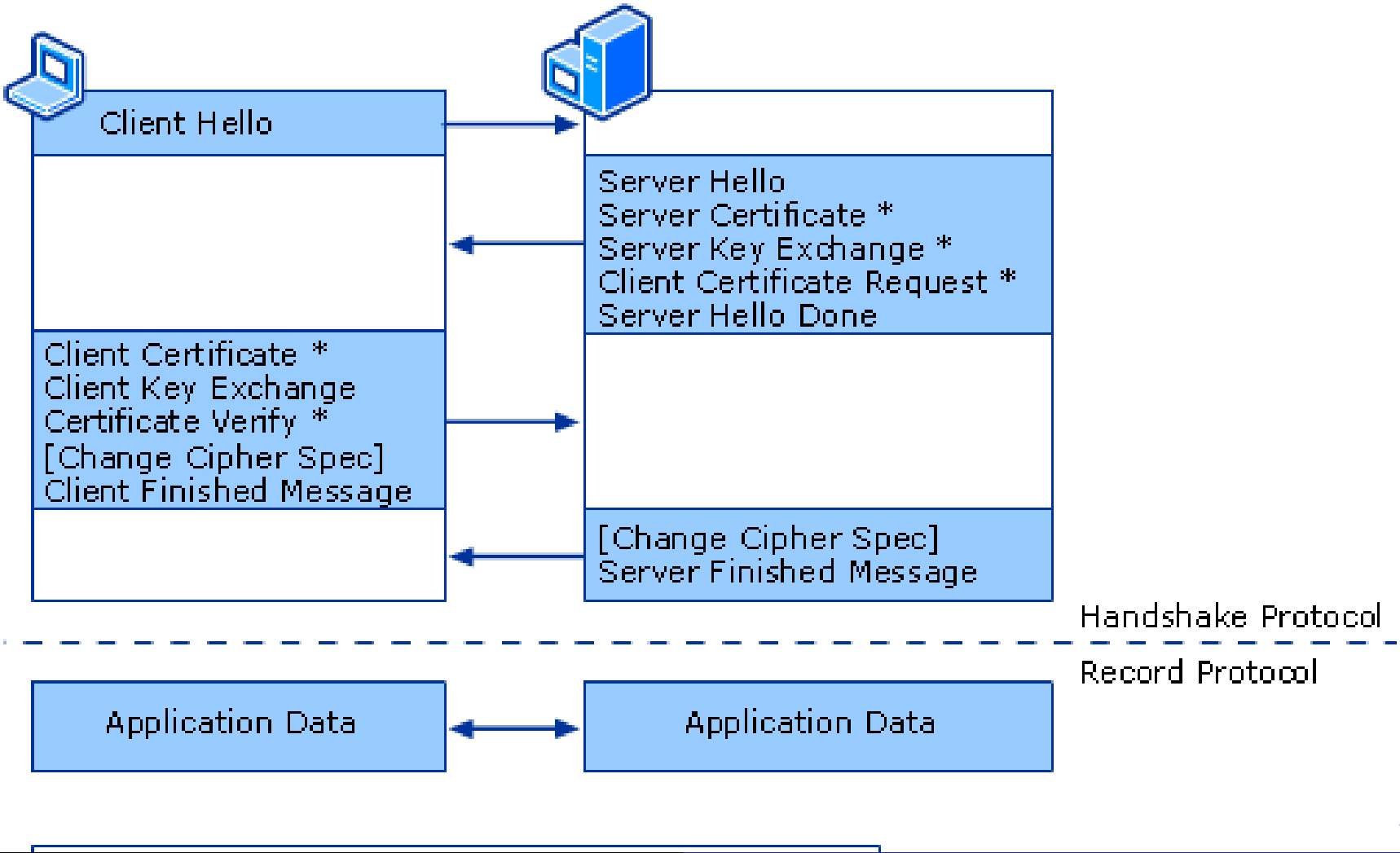
Finished od klienta, šifrovaná, obsahuje hash předchozích zpráv

server dešifruje Finished

ChangeCipherSpec server klientovi, ten zkouší dešifrovat

Odteď jsou všechny zprávy šifrovány

TLS - obrázek


Client Hello
Server Hello
Server Certificate *
Server Key Exchange *
Client Certificate Request *
Server Hello Done
Client Certificate *
Client Key Exchange
Certificate Verify *
[Change Cipher Spec]
Client Finished Message
[Change Cipher Spec]
Server Finished Message
Handshake Protocol
Record Protocol
Application Data
Application Data

Požadavky

- SIP server
  - OpenSER nebo SER
  - oba nenáročné na hardware, ale musí zvládat větší počet síťových připojení
  - SIP server musí být zkompilován s TLS podporou (OpenSSL-dev balíček)
- DNS
  - musí být nastaveny SRV a NAPTR záznamy
  - SRV - Service Record - obsahuje upřesňující záznamy o dostupných službách
  - NAPTR - Name Authority Pointer - doplňující DNS záznamy pomocí nichž jsou rozlišovány služby a jejich adresy
  - umožňují nastavit chování serveru pro různé požadavky

Příklad SRV a NAPTR záznamu

SRV:

```
_sip._udp.ten.cz 86400 IN SRV 100 1 5060 sipx.ten.cz.
```

- Záznam ukazuje na server `sipx.ten.cz`, poslouchá na standardním SIP portu 5060, prioritu má 100, váhu 1 86400 je standardní TimeToLive pro DNS
- Váha a priorita určují, který záznam bude použit v případě nedostupnosti toho s nejnižší prioritou a váhou.

NAPTR:

```
IN NAPTR record 100 0 "s" "SIP+D2U" "" _sip._udp.ten.cz
```

- pomocí NAPTR záznamů a jejich priorit (100) je možné řídit, která služba bude použita jako první, SIPS $\Rightarrow$ SIP $\Rightarrow$ mail

Certifikáty a klienti

- Vyžadován certifikát alespoň pro SIP server
  - certifikát od autority - Verisign, CESNET CA
  - certifikát opatřený vlastní podpisem - nevhodné pro ostrý provoz
- TLS musí podporovat také klient
  - testování probíhalo na CounterPath EyeBeam 1.5 na Widows
  - ani EyeBeam neumí klientské certifikáty
  - free klienti nepodporují TLS vůbec (nebo se tím nechlubí)

Konfigurace serveru pro TLS

- nutný certifikát - zachovat celý řetěz certifikátů
- povolení TLS, nastavení adresy a portu a načtení certifikátu
- povolení NAPTR záznamů a nastavení jejich preference
- nastavení certifikátů a cest jejich uložení
- zvolení způsobu ověřování, parametry Require a Verify
  - Require = 0 a Verify = 0 - nejslabší, pouze šifrovaný tunel
  - Require = 0 a Verify = 1 - běžné nastavení, když klient předloží certifikát, je ověřen
  - Require = 1 a Verify = 1 - nejsilnější ochrana, bez platného certifikátu je klient odmítnut

Konfigurace serveru pro TLS

- nastavení ověřovací metody
  - TLSv1 - novější, ale není zpětně kompatibilní
  - SSLv23 - kompatibilní se staršími protokoly SSL
- možnost nastavit různé množiny parametrů dle portu (t_relay)
- nastavení formátu systémových záznamů přes `syslog` (xlog modul v SIP serveru)

Testování

- spojení Eyebeam a SIP serveru
- i bez certifikatu by melo byt mozne se pripojit
- v případě špatného certifikátu spojení zamítnuto
- v případě úspěchu bude spojení viditelné pomocí `netstat` příkazu
- možné vyzkoušet propojení 2 serverů s využitím TLS - jeden SIP server může působit jako TLS klient i jako TLS server zároveň

Závěr

- popsána konfigurace a případy, které mohou nastat při testování
- TLS pracuje na Hop-By-Hop principu - nevyžadovány ověření o přenosech
- SIP kleinti nepodporují vzájemnou autentizaci se serverem
- mezi servery je možné využít TLS oboustraně
- i přes problémy je využití TLS v SIP použitelné

Děkuji za pozornost!

Děkuji za pozornost!

- Dotazy? Odpovědi?