Získanie prístupu k šifrovanej komunikácii

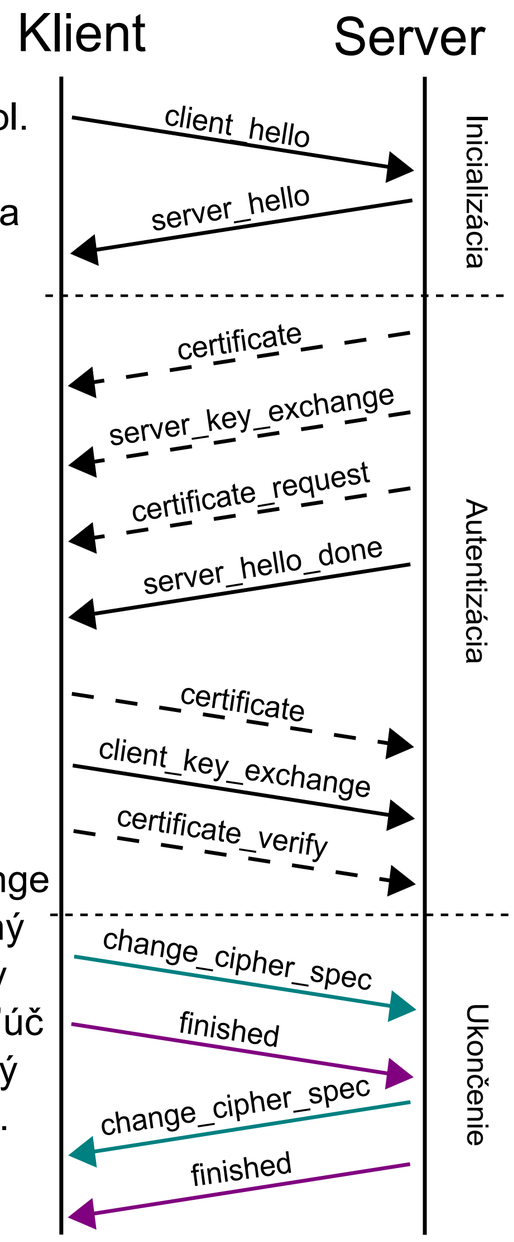
Nástroje rodiny Netfox vznikajú za účelom analýzy zachytenej komunikácie. Na rozdiel napríklad od nástroju Wireshark, ktorý sa používa na analýzu prevádzky na sieťovom rozhraní tak, ako chodí na sieti, nástroje tohto projektu sa snažia zo zachytenej komunikácie extrahovať aplikacné dáta a tie analyzovať a interpretovať. Doposiaľ projekt Netfox dešifrovanie neriešil. S využitím tohto modulu budú nástroje rodiny Netfox maťmožnosť analyzovať aj šifrované dáta.

Analýza protokolu SSL/TLS

Na vyjednanie parametrov šifrovanej relácie sa používa Handshake protokol. Handshake protokol môžeme rozdeliť na tri casti inicializacnú, autentizačnú a ukončenie handshaku.
Vyjednajú sa nasledujúce parametre:

- verzia protokolu,
- ID relácie,
- CipherSuite
  - metóda na výmenu kľúčov,
  - autentizačná metóda,
  - symetrická šifra,
  - message authentication code (MAC), na kontrolu integrity,
- kompresný algoritmus
- náhodné hodnoty

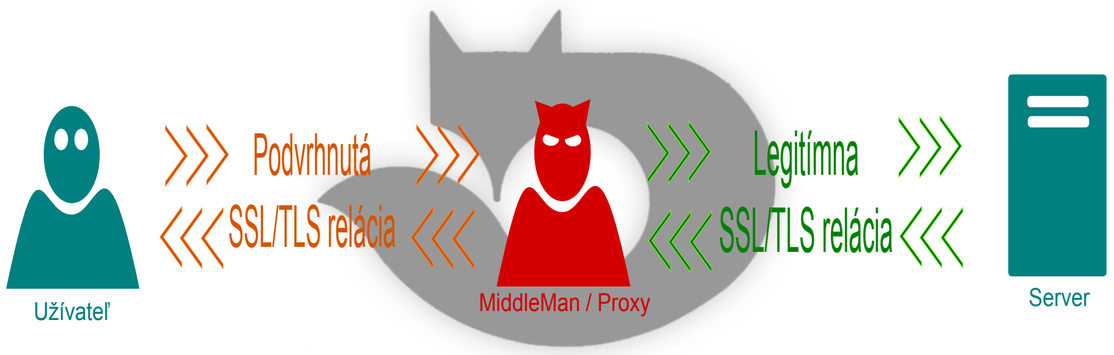
Pomocou hodnoty pre-master secret prenášaný správou Client Key Exchange sa vygeneruje master secret používaný na vypočítanie tzv. key material. Z key material sa potom časť použije ako kľúč symetrickej šifry, časť ako inicializačný vektor a časť ako kľúč HMAC funkcie.



Využitie v Netfox.Framework

Pred vstupom do modulov, ktoré analyzujú danú komunikáciu sa reassemblované PDU načítajú pomocou modifikovanej triedy System.IO.Stream. Trieda implementujúca dešifrovanie bude postavená na rovnaké miesto v spracovaní. Vstupom teda sú reassemblované L7 PDU, ktoré sú obsahom konverzácie.
A výstupom sú dešifrované dáta ako prúd bytov.

Výstupom práce je kompletný modul dešifrovania použitý v projekte Netfox. V prípade prístupu k privátnemu kľúču serveru dovoľuje Netfoxu extrakciu a analýzu šifrovaných dát. Keďže tento privátny kľúč nie je bežne dostupný, je možné pôvodnú SSL/TLS reláciu ukončiť na nejakom bode medzi klientom a serverom (proxy), nahradiť pôvodný privátny kľúč vlastným, a nadviazať novú SSL/TLS reláciu od proxy ku klientovy.



Excel@FIT

Netfox Detective
SSL/TLS Decryption

Dešifrovací modul

Vstupným bodom je metóda NewMessage() , ktorá pri každom zavolaní dešifruje jednu správu a pripraví ju na čítanie. Návratová hodnota metódy je True ak existuje ďalšia dešifrovaná správa na čítanie, False ak nebolo možné dešifrovať žiadnu ďalšiu správu.
Táto metóda implementuje konečný automat, aktuálne so štyrmi stavmi:

- Init - decrypter zatiaľ nie je nainicializovaný parametrami relácie,
- Negotiation - decrypter je nainicializovaný algoritmami, ale čaká sa na vyjednanie tajného kľúča (správa Client Key Exchange),
- Intermezzo - medzistav po inicializácii, v ktorom sa dešifruje prvá správa,
- Data Exchange - v tomto stave sa dešifrujú správy.

Ak bude potrebné zohľadniť autentizacnú časť, (napríklad pri implementácii statickej verzie algoritmu Diffie-Hellman) je možné pridať ďalší stav pred Intermezzo, v ktorom sa budú spracovávať požadované správy. V momentálnej implementácii je podporovaný algoritmus na výmenu kľúčov RSA, pri ktorom z hľadiska dešifrovania autentizačnú časť nie je potrebné riešiť.