Programowanie Sieciowe
Projekt
Sprawozdanie wstępne

Radosława Żukowska - Lider Zespołu
Aleksandra Szczypawka
Małgorzata Grzanka

31.12.2025 r.
Wersja sprawozdania: 1

Opis zadania

Celem projektu jest zaprojektowanie oraz implementacja szyfrowanego protokołu opartego na protokole TCP, tzw. mini TLS

Opis rozwiązania

Struktura wiadomości

ClientHello

- typ wiadomości (flaga: CLH)
- publiczny klucz klienta

ServerHello

- typ wiadomości (flaga: SVH)
- publiczny klucz serwera

EndSession

- typ wiadomości (flaga: END)

Szyfrowane wiadomości

- typ wiadomości (flaga: MSG)
- tekst

Wykorzystane algorytmy

Ustalenie kluczy

Początkowo klient i serwer generują swoje klucze publiczne i prywatne. Do ustalenia klucza sesji jest wykorzystywany algorytm *Diffie-Hellman key exchange*.

Szyfrowanie/odszyfrowanie wiadomości

Do szyfrowania użyta jest metoda OTP: na każdym bajcie wiadomości jest przeprowadzana operacja XOR z kolejnymi bajtami klucza sesyjnego, powielonego w razie potrzeby.

Scenariusz użycia

Nawiązanie połączenia TLS

1. Klient nawiązuje połączenie TCP z serwerem.
2. Klient wysyła wiadomość typu CLK - Client Hello.
3. Serwer odbiera wiadomość od klienta i wysyła wiadomość typu SVH - Server Hello.
4. Klient odbiera wiadomość od serwera.
5. Klient i serwer obliczają wspólny klucz sesyjny.
6. Klient i serwer wyprowadzają klucz MAC (na podstawie poprzedniego klucza) do obliczania kodu MAC.

Przesłanie wiadomości teskstowej

1. Nadawca przygotowuje wiadomość z flagą MSG.
2. Wiadomość jest szyfrowana metodą OTP: każdy bajt plaintextu jest XORowany z kolejnymi bajtami klucza sesyjnego (powielonego, jeśli potrzeba).
3. Na zaszyfrowanym tekście obliczany jest kod MAC (zgodnie z mechanizmem encrytpt-then-mac) i dopisywany do zaszyfrowanej wiadomości.
4. Przygotowana wiadomość wraz z MAC jest wysyłana do odbiorcy.
5. Odbiorca otrzymuje wiadomość, sprawdza jej integralność i autentyczność, oraz odszyfrowuje, jeśli MAC się zgadza.

Zakończenie połączenia

1. Klient lub serwer przygotowuje wiadomość z flagą END.
2. Wiadomość jest szyfrowana i wysyłana, a następnie odszyfrowywana, jak opisano w punkcie *Przesyłanie wiadomości tekstowej*
3. Nadawca wiadomości usuwa klucze oraz zamyka gniazdo.
4. Odbiorca wiadomości usuwa klucze oraz zamyka gniazdo.

Mechanizm integralności i autentyczności dla szyfrowanych wiadomości

Jako mechanizm integralności i autentyczności wykorzystano mechanizm *encrypt-then-mac* dla wysyłanych szyfrowanych wiadomości.

- Do obliczenia wartości MAC wykorzystujemy funkcję hashującą, zaszyfrowany tekst i klucz MAC (wyprowadzony z klucza sesyjnego)