Kryptoanaliza stosowana 2025

Lista zadań nr 7: programowanie usług sieciowych z TLS

Na zajęcia 8 grudnia 2025

Protokół WSPAK/1.0 jest tekstowym protokołem warstwy aplikacji wykorzystującym transport TCP. Działa domyślnie na porcie `7777`. Zakładamy, że znaki tekstu są kodowane zgodnie ze standardem 7-bit US-ASCII. Komunikacja klienta z serwerem jest podzielona na wiersze, jak wszędzie w Internecie zakończone parą znaków `CR LF` (kody ASCII `0x0D`, `0x0A`). Po odebraniu każdego wiersza serwer odsyła do klienta wiersz zawierający znaki odebranego wiersza w odwrotnej kolejności, np. jeśli klient prześle wiersz `"Ala ma kota\r\n"`, to serwer odeśle wiersz `"atok am alA\r\n"`. Standard przewiduje, że wiersz nie może być dłuższy niż 65535 znaków (włączając znaki końca wiersza). Wysłanie pustego wiersza oznacza żądanie zakończenia połączenia przez serwer (klient może też po prostu zamknąć połączenie).

Protokół WSPAKs, to wersja protokołu WSPAK/1.0 zabezpieczona za pomocą protokołu TLS. Domyślnie działa na porcie 2024.

Zadanie 1 (5 pkt). Zaprogramuj w C serwer protokołu WSPAK/1.0. Serwer powinien nasłuchiwać na domyślnym porcie `7777` i w razie nawiązania połączenia z klientem stworzyć proces potomny, który powinien obsłużyć klienta i zakończyć działanie. W roli klienta możesz wykorzystać programy `telnet(1)` lub `nc(1)`.

Zaprogramuj następnie serwer protokołu WSPAKs. Użyj wybranej przez siebie biblioteki implementującej protokół TLS (OpenSSL, LibreSSL, GnuTLS itp.). W roli klienta możesz wykorzystać program `openssl(1)` z opcją `s_client(1)` (program `openssl` przyda się też do wygenerowania klucza prywatnego i certyfikatu serwera), `gnutls-cli(1)` itp.

Zadanie 2 (5 pkt). Zaprogramuj w C klienta łączącego się z dowolnym serwerem implementującym protokół tekstowy zabezpieczony protokołem TLS (coś na wzór `openssl s_client`). Po ustanowieniu połączenia TLS program powinien wypisywać przychodzące od serwera wiersze tekstu (7-bit US-ASCII zakończone znakami `CR LF`) i wysyłać do serwera wiersze wprowadzane z klawiatury. Do edycji wysyłanego wiersza możesz wykorzystać np. biblioteki GNU Readline i GNU History. Argumentami programu powinny być: certyfikat główny serwera, adres IP i port TCP.