Úkol: Implementace SSL/TLS připojení k fit.cvut.cz

Vytvořte program v jazyce C, který naváže SSL/TLS připojení k serveru fit.cvut.cz na portu 443, získá informace o certifikátu serveru, pošle HTTP GET požadavek a uloží odpověď do souboru.

Zadání:

- Přeložení hostname: Implementujte funkci pro přeložení IPv4 adresy hostname fit.cvut.cz pomocí funkce getaddrinfo.
- Vytvoření TCP spojení: Vytvořte TCP spojení na přeloženou adresu na portu 443 pomocí funkcí socket a connect.
- Inicializace OpenSSL: Inicializujte knihovnu OpenSSL pomocí funkcí SSL_library_init, SSL_load_error_strings a OpenSSL_add_ssl_algorithms.
- Vytvoření SSL kontextu: Vytvořte nový SSL kontext pomocí funkce SSL_CTX_new a metody TLS_client_method. Zakažte zastaralé a zranitelné protokoly pomocí SSL_CTX_set_options.
- Vytvoření SSL struktury: Vytvořte SSL strukturu pomocí funkce SSL_new.
- Přiřazení spojení: Přiřaďte otevřené spojení k SSL struktuře pomocí funkce SSL_set_fd.
- Nastavení SNI: Nastavte jméno požadovaného serveru pro mechanizmus SNI pomocí funkce SSL_set_tlsext_host_name.
- Zahájení SSL komunikace: Zahajte SSL komunikaci pomocí funkce SSL_connect.
- Získání a zobrazení informací o certifikátu: Získejte a zobrazte informace o certifikátu serveru pomocí funkcí SSL_get_peer_certificate a X509_NAME_oneline.
- Odeslání HTTP GET požadavku: Odeslete HTTP GET požadavek na server a zpracujte odpověď pomocí funkcí SSL_write a SSL_read.
- Uložení odpovědi do souboru: Uložte odpověď serveru do souboru output.html.
- Ukončení SSL/TLS spojení a úklid:
- Ukončete SSL/TLS spojení a uvolněte všechny alokované zdroje.