Zabezpečená komunikácia klient server s využitím post-kvantových algoritmov

Autor: Ing. Jozef Šimko

Vedúci práce: prof. Ing. Miloš Drutarovský, CSc.

Technická univerzita v Košiciach, Fakulta elektrotechniky a informatiky

Motivácia

Všetky zariadenia pripojené k internetu, od serverov, cez stolné počítače až po IoT senzory, musia riešiť otázku bezpečnosti. Napriek tomu, že si to bežní používatelia neuvedomujú, tak všetky tieto zariadenia využívajú rôzne šifrovacie algoritmy na zabezpečenie autentizácie, dôvernosti a integrity dát. S nárastom výpočtového výkonu počítačov však vznikajú aj nové výzvy pre informačnú bezpečnosť. V posledných rokoch sa za hlavnú bezpečnostnú hrozbu považuje rozvoj kvantových počítačov.

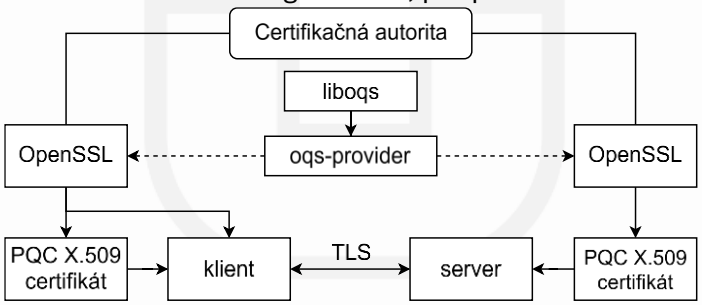
Post-kvantová kryptografia

Už v 90. rokoch vznikli teórie o kvantových algoritmoch, ktoré dokážu riešiť aj také matematické problémy, na ktorých je založená bezpečnosť aktuálne využívaných šifier. Medzi najvýznamnejšie patria Groverov algoritmus, na základe ktorého je potrebné zdvojnásobiť veľkosti kľúčov symetrických šifier ako je AES a tiež Shorov algoritmus, ktorého aplikáciou sa predpokladá prelomenie asymetrických šifier ako sú RSA alebo ECC. Napriek tomu, že kvantové počítače majú stále mnoho technických nedostatkov, tak ich vývoj napreduje a bezpečnostné riziko narastá. Post-kvantová kryptografia (PQC) sa zaoberá šifrovacími algoritmami založenými na matematických problémoch, ktoré budú odolné aj pri kryptoanalýze na kvantových počítačoch, pričom budú implementované v existujúcich protokoloch a hardvéri.

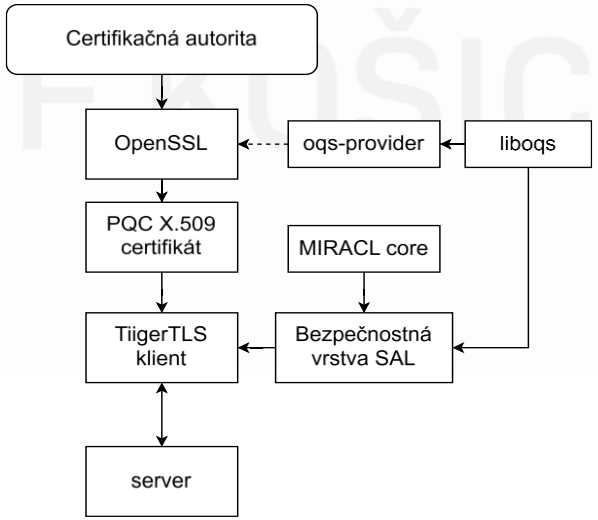
V roku 2016 vyhlásil americký NIST verejnú súťaž s cieľom zoskupiť, testovať a štandardizovať PQC algoritmy, konkrétne enkapsulačné algoritmy (KEM) na výmenu kľúčov a schémy digitálneho podpisu (DSA). Výsledkom tejto súťaže sú prvé oficiálne štandardy PQC algoritmov. FIPS 203 definuje KEM algoritmus ML-KEM odvodený od algoritmu CRYSTALS-Kyber. FIPS 204 a FIPS 205 sú DSA schémy, pričom ML-DSA je odvodený od algoritmu CRYSTALS-Dilithium a SLH-DSA je odvodený od algoritmu SPHINCS+. Štandardizácia však pokračuje, pretože okrem postupného zavádzania nových algoritmov do protokolov ako TLS, IPsec alebo IKE, bola v roku 2023 vyhlásená ďalšia súťaž s cieľom nájsť záložné algoritmy.

Integrácia PQC algoritmov do TLS

V rámci práce sme rozšírili OpenSSL funkciami pre PQC algoritmy z knižnice liboqs prostredníctvom knižnice oqs-provider. Získali sme rozhranie na testovanie TLS spojenia s využitím KEM algoritmov a PQC certifikátmi, ktoré sme mohli sami generovať, podpisovať a overovať.



Následne sme použili knižnicu TiigerTLS, optimalizovanú open-source C++ implementáciu TLS so šifrovacími algoritmami z knižnice MIRACL core. Doplnili sme podporu soketovej komunikácie pre Windows platformu a bezpečnostnú abstraktnú vrstvu (SAL) sme rozšírili funkciami knižnice liboqs.



Výsledná aplikácia klienta podporuje:

- 18 verzií PQC KEM algoritmov
- 11 verzií PQC DSA algoritmov

Experimentálne výsledky

- Testovanie spojenia s lokálnym OpenSSL serverom a verejným serverom *test.openquantumsafe.org*
- Meranie časov generovania kľúčov

	Verejný kľúč	Súkromný kľúč	Šifrovaný text	Generovanie kľúčov
X25519	32 B	32 B	32 B	0,13 ms
ML-KEM 1024	1568 B	3168 B	1568 B	0,09 ms

- Meranie doby overenia zreťazených certifikátov

	Verejný kľúč	Súkromný kľúč	Podpis	Overenie certifikátu
RSA-2048	256 B	256 B	256 B	0,56 ms
ML-DSA87	2592 B	4896 B	4627 B	1,11 ms

Merania ukázali porovnateľné výsledky PQC algoritmov s tými klasickými. Hlavným rozdielom je výrazný nárast veľkostí kľúčov, šifrovaného textu a podpisov.

Zhrnutie

- Šifrovacie algoritmy post-kvantovej kryptografie odolné aj voči útokom kvantových počítačov
- Rozšírená lightweight implementácia TLS klienta vhodná aj pre embedded systémy s možnosťami pre ďalšie testovanie
- Rozšírenie implementácie TLS klienta a servera v jazyku C, ktorá sa využíva na cvičeniach pri výučbe
- Veľkosť dátových štruktúr ako hlavná výzva pri používaní PQC algoritmov v zariadeniach s obmedzeným množstvom pamäte či v bezdrôtových sieťach
- Odborná publikácia prijatá na konferenciu ELMAR 2024 – *E. Kupcova, J. Simko, M. Drutarovský, M. Pleva, „Experimental Framework for Secure Post-Quantum TLS Client-Server Communication“*