Validace certifikátu

Kontrola probíhá proti lokálnímu úložišti certifikátů a navíc přidává vlastní certifikační autoritu (CRoCS FI MU).
Program využívá možností `SSL_get_verify_result()`, takže validuje veškeré chyby které indikuje tato funkce, z nich si navíc vybírá, jako jedinou méně závažnou chybu `X509_V_ERR_CERT_HAS_EXPIRED`. Všechny ostatní považuje za závažné.
Dále je využita kontrola veřejného klíče certifikátu, kdy se ověřuje použitý algoritmus a jeho síla. Vychází se ze specifikace od společnosti Mozzila (viz Zdroje), která doporučuje používat pouze RSA o síle 2048 bitů nebo lepší či eliptických křivek s 256 bitovým parametrem, či větším.

Hodnocení důvěry

1	Vše je v pořádku
2	Certifikát má prošlou platnost
3	Použita slabá nebo nepodporovaná šifra (RSA < 2048b, EC < 256b)
4	Jiná chyba (neplatný CN, self signed, chybějící CA, porušen řetězec důvěry...)

Hodnocení OpenSSL API a předchozí zkušenosti

1 (nikdy) až 5 (velmi často)

1	Používali jste již někdy před tímto úkolem OpenSSL API?

1 (rozhodně ne) až 5 (rozhodně ano)

1	Chci používat OpenSSL API často
5	OpenSSL API je zbytečně složité
2	OpenSSL API bylo snadné použít
2	Potřebuji podporu více zkušeného vývojáře, aby mohl používat OpenSSL API
3	Funkce v OpenSSL API byly dobře integrovány.
5	Vnímám v OpenSSL API příliš mnoho nekonzistence.
4	Většina vývojářů se naučí používat OpenSSL API velmi rychle.
3	OpenSSL API má velmi těžkopádné k použití.
1	Cítil jsem se velmi jistý při použití OpenSSL API.
3	Před použitím OpenSSL API jsem se potřeboval naučit spoustu věcí.

Bylo to mé první setkání s C/C++ API knihovny OpenSSL, myslím, že jejím největším problémem je nepřehledná dokumentace. Nikde není vysvětleno, proč potřebuji SSL_CTX, BIO atd… Je vždy uvedeno pouze pár příkladům, ale možnost zjistit širší souvislosti chybi.

Zdroje

Pro samotné nastudování OpenSSL knihovny jsem se snažil využí převážně následující zdroje:

- man stránky, které jsou velmi nepřehledné a málo detailní
- https://wiki.openssl.org/index.php/Main_Page
- https://github.com/openssl/openssl, (protože obsah struktur, certifikátu není jinde k nalezenení)

Dále pro identifikaci podpory jednotlivých typů šifrování a podporované délky klíčů bylo nutné sáhnout k tabulkám pro samotné TLS a podporu ve webových prohlížečích:

- https://en.wikipedia.org/wiki/Transport_Layer_Security#Cipher
- https://en.wikipedia.org/wiki/Transport_Layer_Security#cite_note-ciphers-56
- https://wiki.mozilla.org/Security/Server_Side_TLS