

Projekt do PB173
Bezpečné videokonferenční architektura

Tučňáci kolektiv

12. října 2013

Obsah

1	Motivace:	2
2	Použité technologie:	2
3	Náš přístup k řešení:	2
4	Naše API:	3

1 Motivace:

Jak už bylo naznačeno, dnes je člověk odposloucháván všude. Co si programátor sám nenapiše, to nemá zabezpečené. A pokud se jako programátoři máme domluvit na hacknutí cele NSA, musíme se domlouvat na šifrovaném kanálu bez možnosti odposlechu ze strany NSA. Za vedlejší cíle se dá považovat cvičení implementace kryptografických metod v "praxi" (ve vlastním kódu C/C++) a rozvinutí schopnosti spolupráce na větším projektu v kolektivu.

2 Použité technologie:

C/C++ s knihovnou PolarSSL, v našem případě většinou C++, ale jelikož je PolarSSL psána v C, tak sekce kolem šifrování nemohou používat mechanismy C++ (např. použití pole znaků místo objektu typu String). Dále planujeme použít knihovny pro práci se sockety/HTTPS, knihovnu pro vlákna a události. Pro zpracování obrazu a zvuku využijeme doporučené knihovny ze cvičení.

Konkrétněji ke kryptografii: pro zajištění důvěrnosti, integrity i soukromí využijeme šifrovacího schématu encrypt-then-mac v podobě otevřené implementace Galois/Counter Mode (GCM), která je dostupná v PolarSSL. Jako hashovací funkci budeme používat SHA-512, symetrickou šifrovací funkcí bude AES v již zmíněném módu GCM a pro ustanovení komunikace použijeme asymetrické kryptografie v podobě RSA.

3 Náš přístup k řešení:

V projektu vystupují tři komponenty, mezi kterými je ustanovena komunikace.

Certifikační autorita Certifikační autorita (CA) je komponentou, která zajišťuje ověřování a distribuci certifikátů veřejných klíčů potřebných pro navázání asymetricky šifrované komunikace mezi klienty. Certifikační autorita přijímá certifikáty od nově přichozích klientů, a na žádost vydává veřejné certifikáty klientů. Pro komunikaci s CA je zřízen jeden pár veřejného a soukromého klíče, který je používán CA. Veřejný klíč je pro klienta známý. Komunikace je ustavena klientem, který po CA požaduje ověření veřejného klíče jiného klienta. Na tento dotaz CA odpovídá dohledáním příslušného veřejného klíče ve své databázi a odesláním certifikátu tohoto klíče.

Server Server je komponentou zaštiťující ustanovení komunikace mezi klienty. Komunikace probíhá pomocí jednosměrně šifrované komunikace od klienta k serveru. Server přijímá od klienta požadavky na přihlášení do systému a odesílá ostatním připojeným klientům jeho dostupnost. Následně očekává požadavky na spojení. Nakonec po odpojení odešle všem klientům požadavek na smazání klienta. Server přijme požadavek na spojení od klienta ke klientu. Tento požadavek propaguje k cílovému klientovi společně s údaji pro navázání komunikace se zdrojovým klientem. V případě přijetí pozitivní odpovědi odešle komunikační údaje cílového klienta zdrojovému a označí oba klienty za nedostupné. Pokud některý z klientů ukončí komunikaci odešle tuto informaci serveru a ten označí oba klienty za dostupné.

Klient Komponenta klient zajišťuje rozhraní pro přímou komunikaci dvou klientů, navázání komunikace a získávání veřejných klíčů vystupujících v komunikaci. Klient se připojí k serveru a přijme seznam připojených klientů.

Klient požaduje připojení ke klientovi: Klient požaduje připojení ke klientovi: Iniciální klient (IK) si vyžádá od CA veřejný klíč cílového klienta (CK) a zašle serveru požadavek na spojení. Po kladné odpovědi serveru a přijetí komunikačních údajů o CK. Následně navazuje komunikaci s CK. Odešle požadavek společně s náhodně vygenerovaným klíčem a inicializačním vektorem pro symetrickou kryptografii zašifrovaný a podepsaný pomocí asymetrické kryptografie k CK. Pokud CK odpoví kladně, přijme a zpracuje symetrický klíč a inicializační vektor pro komunikaci od CK a IK je schopen pomocí veřejného klíče CK ověřit autenticitu. Nakonec navazuje a přijímá komunikaci k resp. od CK šifrovanou pomocí symetrické kryptografie.

Klient přijímá požadavek na komunikaci od serveru: CK přijme od serveru požadavek a informace o IK. Od CA si vyžádá certifikát veřejného klíče IK a odpoví na požadavek. Následně přijímá požadavek přímo od IK, které ověří pomocí jeho veřejného certifikátu. Přijme klíč pro komunikaci od IK, vygeneruje a odešle klíč pro komunikaci mezi CK a IK. Nakonec přijímá a otevírá přímé spojení mezi IK a CK.

4 Naše API:

Viz hlavičkové soubory na GitHubu včetně dokumentace v repozitáři po názvem PB173_tucnaci dostupný zde: https://github.com/LukeMcNemee/PB173_tucnaci