Dokumentácia k projektu 2 z predmetu Kryptografie

Timotej Ponek, xponek00@stud.fit.vutbr.cz

Algoritmus pre vytvorenie paddingu

Pre padding som sa nesnažil vytvárať nejako kryptograficky bezpečné riešenie. Inšpiroval som PKCS 1.5 paddingom, u ktorého bolo preukázané, že nie je bezpečný. Moje riešenie funguje tak, že klient vždy pri posielaní správy (ako druhú správu, prvá je správa je dĺžka správy v bajtoch + 16 bajtov nonce pre AES šifru) pošle serveru náhodne vygenerované zakódované číslo v rozsahu <0,240), ktoré reprezentuje počet bajtov použitých ako padding napravo od skutočnej prenášanej hodnoty. Schéma je teda:
<1-239 bajtov random padding > <16 bajtov hash> <0-239 bajtov random padding>
Ak je hodnota po paddingu nevyhovujúca - vyššia ako verejný modulus n, padding sa generuje znova.

Implementácia klienta

Klient v smyčke čaká na vstupnú správu, po jej zadaní vykonáva úkony tak ako vyžaduje zadanie projektu a vypisuje výsledky jednotlivých úkonov. Serveru najskôr pošle dĺžku správy v bajtoch, potom veľkosť paddingu napravo od rozumnej hodnoty (hashu) a následne celú správu (zašifrovanú správu + hash a zašifrovaný AES kľúč) skrz volania funkcie `sendall()`. Medzi jednotlivými volaniami `sendall()` mám miniatúrny `sleep()`, pretože sa na strane serveru mohli prijať naraz dĺžka správy s veľkosťou random paddingu, čo nie je žiadané, a nijako inak som to nevedel vyriešiť. Potom čaká na odpoveď od serveru. Ak od serveru dostane odpoveď, ktorá značí že integrita správy bola narušená, posiela správa znova a znova, dokiaľ nie je správa v poriadku doručená. Až po správnom doručení správy klient čaká na zadanie novej správy.

Implementácia serveru

Server pri štarte čaká na pripojenie od klienta. Akonáhle sa klient pripojí, čaká od neho na správu. Najskôr príjme v prvej správe veľkosť dát a 16 bajtov nonce pre AES šifru, následne veľkosť random paddingu, a potom celú šifrovanú správu. Tú následne dešifruje a výsledky vypisuje v súlade s popisom v zadaní. Ak server zistil, že bola narušená integrita správy (vygenerovaný hash správy sa nerovnal dešifrovanému hashu), server o tom informuje klienta a čaká na ďalšiu správu. Keďže ako bolo spomenuté vyššie, klient posiela serveru správu až dokiaľ nedostane od serveru odpoveď, že správa bola prijatá bez porušenia integrity, server v realite v tomto momente čaká na znovuzaslanie správy od klienta.

Bezpečnosť riešenia

Hybridné šifrovanie je jedno z najbezpečnejších riešení pre šifrovanie správ. Hoci v mojom projekte používam niektoré veci, ktoré nezvyšujú kryptografickú bezpečnosť (posielanie

nešifrovanej dĺžky správy a veľkosti paddingu zo strany klienta na server), tieto nedokonalosti vo všeobecnosti neznižujú bezpečnosť hybridného šifrovania.

Poznámky k riešeniu

Na šifrovanie pomocou AES používam mód EAX mód, pretože nevyžaduje padding správy. Implementácia znovuzasielania správy v prípade že integrita správy bola narušená je funkčná (bola otestovaná počas nesprávne kontrolovania dešifrovaného a novo vygenerovaného hashu, a fungovala).