SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Úvod do počítačovej bezpečnosti

Používateľská dokumentácia

Selepová Adriána

Ličaková Barbora

Chalupková Zuzana

Matúš Klement

Pavol Šantavý

# Používateľská špecifikácia

## Stručný úvod do problematiky

### Úloha 1

Vytvorenie web aplikácie, ktorá umožní používateľovi šifrovať a dešifrovať súbory symetrickým kľúčom K, náhodne vygenerovaným a uloženým niekde mimo zašifrovaného súboru. Použitie

symetrickej kryptografie. Na riešenie zadania využitie hotového kryptografického API. Užívateľ nahrá svoj súbor na web server a web server vykoná šifrovanie súboru a poskytne ho užívateľovi na stiahnutie. Podobne si užívateľ dokáže súbor pomocou web servera aj dešifrovať.

### Úloha 2

Pridanie uloženému súboru informáciu na kontrolu integrity, či prostredníctvom MAC alebo AEAD módu. Malo by byť schopné overiť či došlo k modifikácii uloženého súboru.

### Úloha 3

Rozšírenie vytvorenej aplikácie tak, že vygenerovaný symetrický kľúč K sa zašifruje asymetricky a pripojí k zašifrovanému súboru v rámci hlavičky/päty súboru s metadátami potrebnými k dešifrovaniu. Dbanie na to, aby bolo možné skontrolovať aj integritu zašifrovaného súboru. Web aplikácia pred šifrovaním súboru požiada o nahratie verejného kľúča (použitého pri šifrovaní symetrického kľúča) a v prípade dešifrovania požiada o nahratie privátneho kľúča (potrebného pre dešifrovanie symetrického šifrovacieho kľúča). Tiež ponúkne možnosť vygenerovania nového verejného a privátneho kľúča a jeho uchovania na serveri (a jeho následné stiahnutie).

Pre náročnejšieho užívateľa vytvorte aplikáciu na dešifrovanie web serverom šifrovaných súborov ktorý by bolo možné užívateľom si stiahnuť z web servera v prípade ak by užívateľ nechcel odosielať svoj privatný kľúč na web server pre dešifrovanie súborov. Ako vstup pre aplikáciu by bol zašifrovaný súbor (stiahnutý z web servera) a privatný kľúč uživateľa. Výužitím asymetrickej kryptografie je takto možné zabezpečiť aby použitý symetrický kľúč nebol ukladaný na servery.

## Používateľské požiadavky

### Funkcionálne požiadavky

Systém umožňuje role Používateľ:

* nahrať súbor na server
* stiahnuť odšifrovaný súbor zo servera
* vygenerovať private key

### Nefunkcionálne požiadavky

* Používateľsky prijateľné rozhranie.
* Jednoduchý webový systém

### Merateľné požiadavky

Systému trvá šifrovanie 1GB súboru

### Použitie

### Bezpečnostné odporúčania

# Systémová špecifikácia

## Použité technológie

* Jazyky:
  + Backend: Java
  + Frondend: JavaScript, HTML, CSS
* Šifrovacie knižnice:
  + javax.crypto.\*;
  + javax.crypto.spec.SecretKeySpec;
  + java.security.InvalidKeyException;
  + java.security.Key;
  + java.security.KeyPair;
* Zdroje:

### Šifrovanie

Formát zašifrovaného súboru je .

Postup šifrovania:

Výber šifrovacej funkcie a veľkosti kľúča z hľadiska rýchlosti a bezpečnosti

### Kompilácia/Inštalácia