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

## Popis funkcionality systému

### 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).

## Používateľské požiadavky

### Funkcionálne požiadavky

Systém umožňuje používateľovi:

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

### Nefunkcionálne požiadavky

* Používateľsky prijateľné rozhranie.
* Jednoduchý webový systém

### Merateľné požiadavky

* Systému trvá šifrovanie 500MB súboru 10 sekúnd
* Maximálna veľkosť súboru na nahratie je 500MB

### Používateľská príručka

### Bezpečnostné odporúčania

# Systémová špecifikácia

## Use Case diagram

Obrázok - Use Case diagram

Obrázok - Use diagram webovej služby

## Použité technológie

* Jazyky:
  + Backend: Java
  + Frondend: JavaScript, HTML, CSS, JSP
* Šifrovacie knižnice:
  + javax.crypto.\*;
  + javax.crypto.spec.SecretKeySpec;
  + java.security.InvalidKeyException;
  + java.security.Key;
  + java.security.KeyPair;
  + java.security.KeyFactory;
  + java.security.NoSuchAlgorithmException;
  + java.security.PrivateKey;
  + java.security.spec.KeySpec;
  + java.security.spec.X509EncodedKeySpec;

## Šifrovanie

Postup šifrovania:

Po nahratí súboru na webstránku sa súbor odošle na backend. Tu sa súbor šifruje pomocou vygenerovaného symetrického secret key a ten sa následne asymetricky zašifruje pomocou public key. Táto šifra sa uloží do hlavičky súboru spolu s MAC. Public key a private key sa generuje na webstránke (pomocou algoritmu RSA).

Secret key sa šifruje algoritmom AES, ktorý je potom zašifrovaný public key-om cez RSA šifru.

Zašifrovaný súbor je vo formáte .enc

Výber šifrovacej funkcie a veľkosti kľúča:

* hľadiska rýchlosti:
  + AES symetrické šifrovanie súboru, je rýchlejšie ako šifrovanie pomocou RSA
  + šifrovane AES pomocou RSA asymetricky zvyšuje výkonnosť
* bezpečnosti:
  + asymetrické šifrovanie s RSA je dostatočne bezpečné pri zadaní vhodného kľúča
  + oproti iným asymetrickým šifrám je stabilnejšia spolu s AES

## Kompilácia a inštalácia

Pre správne otvorenie a kompilovanie kódu je potrebné nainštalovanie Apache Tomcat webserveru do cloudu. Do zložky webservera Tomcatu je potrebné nakopírovať .war súbor projektu.

Hlavná stránka sa nachádza na 147.175.121.137/upb