Криптографічні алгоритми в мобільних додатках під управлінням iOS

Презентація до курсової роботи

Виконав студент МП КН-1 Сабадишин Максим
Науковий керівник
кандидат фізико-математичних наук, доцент Нагірна Алла Миколаївна

Вступ

- Мобільні пристрої мають стабільний ріст у кількості користувачів
- Все більше можливостей з’являється у розробників мобільних додатків, а тому і збільшується обсяги чутливих даних, що там зберігаються
- Це збільшує необхіндність в захищених даних та з’єднанні, а тому і в криптографії

Постановка задачі

- Проаналізувати
  - Криптографію в рамках розробки мобільних додатків
  - Актуальні алгоритми
  - Актуальні фреймворки для роботи з ними
- Дослідити
  - Проблеми, що криптографія вирішує
  - Існуючі додатки та сценарії використання алгоритмів
  - Прикладне використання

Результати роботи

- Криптографія - важливий аспект в розробці мобільних додатків
- Автентифікація, авторизація, цифрові підписи, та зберігання конфіденційності даних - основні проблеми, що вирішує криптографія на мобільних додатків
- CryptoKit та CryptoSwift - основні фреймворки для роботи з криптографічними алгоритмами
- Створено програмний застосунок, що демонструє підключення та роботу з бібліотеками алгоритмів

Результати роботи (2)

- Досліджено основні причини витоків даних - кібератаки та соціальна інженерія
- Проаналізовано тенденцію до створення захищених програмних продуктів - з 2005 року вона є позитивною
- Розглянуто відомі випадки та наслідки від витоків
- Проаналізовано роль криптографії та способи їм запобігти

Актуальні алгоритми в мобільній розробці. Хешування

- Сім’я алгоритмів SHA-2. Найпопулярніший SHA-256
- Можливість використання MD5 і SHA-1
- SHA-2 має кращу безпеку проте на 20% менш швидкий
- NeuralHash - алгоритм від Apple зі стійкою чутливістю до змін

Актуальні алгоритми в мобільній розробці. Симетричні шрифти

- AEAD - Authenticated Encryption with Associated Data як еталон
- AES-GCM та ChaCha20-Poly1305 як найпопулярніші представники
- ChaCha20-Poly1305 використовується частіше через відсутність переваг AES-GCM у швидкодії, які є у інших архітектур процесорів

Актуальні алгоритми в мобільній розробці. Асиметричні шрифти

- ECC алгоритми - основний вибір
- Алгоритми базовані на еліптичній криптографії
- Найчастіше вибір стоїть між реалізаціями P256/P384/P521 або Curve25519
- ECC алгоритми витіснили RSA з лідерів після своєї появи

Фреймворки для роботи з криптографічними аллгоритмами

- CryptoKit - випущений в 2019 році, розроблений Apple
  - Мінімальна підтримка iOS 13.0
- CryptoSwift - випущений сторонніми розробниками, має сильну підтримку спільноти
  - Мінімальна підтримка iOS 9.0

Результати роботи програмного застосунку

	SHA-256			ChaCha20/ChaChaPoly		
	min	avg	max	min	avg	max
CryptoKit	0.383	0.4	0.5	0.377	0.389	0.416
CryptoSwift	1.859	1.9	1.976	2.531	2.646	2.806

Таблиця 3.1 Результати аналізу швидкодії бібліотек

Дякую за увагу!