FYP15032

2015-2016

Chan Hai Ten Jacky
3035070107

Supervisor: Dr. Lucas Hui

DESIGN AND IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS IN PC AND MOBILE PHONE

PROJECT PLAN

Contents

Summary

Cryptography is well-developed on PC, but is still quite young on mobile. With more people handling sensitive data or transaction on mobile, mobile cryptography naturally become a concern. This project aims to create an application, which runs on both PC and Android, that is capable to encrypt and decrypt data using RSA, AES and SHA algorithm. If time allowed, Attribute-Based Encryption will also be added.

Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties[1]. It is one of the fundamental elements of secure communication – which powered a lot of online activities: online banking, e-Commerce etc.

With the increasing usage of smart phones, online transactions are no longer limited at home – people can trade anywhere at any time. Report of the Federal Reserve System shows that more than 50% of smart phone users in the U.S. also use mobile banking service[2]. With such popularity, security naturally becomes a major concern. However, a lot of such mobile apps are actually vulnerable to attackers[3], allowing them to obtain confidential information, like personal detail, or credit card number. It is quite obvious that more secure implementation can be done.

This project will focus on creating a mobile & PC application that can provide secure encryption and decryption service, base on different cryptographic algorithms, namely the AES, SHA, RSA, and also the Attribute-Based Encryption. All of the mentioned algorithms are extremely popular and reliable, and also frequently updated and evaluated.

Objective

The goal of this project is to create application(s) that can be used to encrypt & decrypt any form of input data with cryptographic algorithms. The objective can be sub-divided into the following:

1. **Create a Windows application which can encrypt & decrypt data with the choice of using AES, SHA-2 and RSA algorithm**

The basic part of this project. The part will be quite straight forward as PC tends to have good computational power and is error-tolerant. The main goal of this part will be familiarize with the algorithm & libraries.

2. **Port the above application onto Android phone**

The second part of the project is to convert the PC program into an android application. Unlike PC, on phone the computational power and heat-sinking is very limited. To create an efficient application, some structural change to the original program and maybe server-side computation will be needed. It is foreseeable that this will be a challenging task, but can be handled with testing and research.

3. **Implement Attribute-based Encryption into the application**

The last part of the project will involve implementing Attribute-based Encryption, a relatively recent and advanced encryption algorithm.

Methodology

What tools should be utilized in this project? The first step of development should always be evaluating resource available on The Internet, so that redundant effort can be avoided. The following tools are planned:

On Windows PC, C, together with OpenSSL Library will be used.

Why C & OpenSSL?

It is worth noticing that utilizing community-maintained tools is nearly always the better solution when working on a generic project. Again, there is no reason to reinvent a wheel. The libraries available online are robust, optimized and more bug-free. So the question will be which library to be used. Research[4] has shown that OpenSSL shows "high level of optimizations", and has "promising good performance" against other libraries. Therefore, OpenSSL will be used in this project. Since OpenSSL is only compatible with C, the program will be written with C as well.

On Android mobile, Java, together with Java Cryptography Extension (JCE) library will be used.

Why Java & JCE?

Unlike PC Platform, on android there exist a lot of constraints. For instance, everything on android is running Java, and it is impossible to develop an Android App not running Java. The programming language is fixed. Then it comes to library. Although there are again a lot of libraries available, JCE should be the one used. The point is native compatibility. JCE is developed and maintained by Oracle, and is natively packed inside JRE. This prevents users from installing additionally libraries, neglecting dependency concerns. As it is from Oracle, the company that owns Java, the computation speed should be acceptable. Thus JCE Library is used.

Schedule

Sep 2015	Research & Study
Oct 2015 – Dec 2015	Objective part 1 & 2 - RSA, AES and SHA-2 - PC & Android
Jan 2016	1st presentation Interim report
Feb 2016 – Apr 2016	Objective part 3 - Elliptic curve
Apr 2016 – May 2016	Final presentation and report

Reference

1. www.wikipedia.org [Internet].
   [cited 2015 Oct 4]. Available from:
   https://en.wikipedia.org/wiki/Cryptography.

2. Consumers and Mobile Financial Services 2014 (US).
   Board of Governors of the Federal Reserve System(US); 2014.

3. Lucky Onwuzurike, Emiliano De Cristofaro. Danger is My Middle Name:
   Experimenting with SSL Vulnerabilities in Android Apps. University College
   London; 2015.

4. Timo Bingmann. Speedtest and Comparsion of Open-Source Cryptography
   Libraries and Compiler Flags. [Internet].
   [updated 2008 Jul 14; cited 2015 Oct 4]. Available from:
   https://panthema.net/2008/0714-cryptography-speedtest-comparison