

令和3年度 東邦大学理学部情報科学科 卒業研究

Android アプリケーションにおけるサード パーティー製APIでの暗号技術利用動向の 調査

学籍番号 5517097

山口千尋

金岡研究室

目次

1	はじめに	3
2	前提知識	4
2.1	Android	4
2.2	Operating System	4
2.3	APK	4
2.4	暗号 API	4
2.5	API	5
2.6	Android Developers	5
2.7	API ドキュメント	5
2.8	Linux とは	5
2.9	Ubuntu	5
2.10	シェル	5
2.11	シェルスクリプト	5
3	関連研究	6
3.1	河合らの調査	6
3.2	Y に関連した研究	6
4	提案手法のメインな部分	7
5	提案手法の試作みたいなものを書く部分	8
6	試作を用いて評価	9
7	まとめ	10

1 はじめに

2 前提知識

2.1 Android

Android とは、Google 社が 2007 年に開発した、スマートフォンやタブレット端末など携帯情報機器向けの Operating System のこと。主にスマートフォンの OS として広く普及しており、世界的に Apple 社の携帯機器向け iOS と市場を 2 分している。

2.2 Operating System

Operating System(以後 OS) とは、ソフトウェアの種類の一つで、機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェアのこと。

2.3 APK

Android Application Package の略であり、Android 向けのアプリケーションを Android 端末にインストールできる形式にパッケージにしたもの、もしくはそのファイルのこと。APK とは「.apk」という拡張子を持つ Android アプリケーションの本体ファイルのことである。ただし、apk ファイル自体は ZIP 形式で圧縮されており、その中にはアプリケーションの動作に必要なさまざまなファイルが納められている。apk のファイル形式でなければ Android 端末にアプリケーションをインストールすることができないため、Google Play など配信されているアプリケーションは、すべて apk ファイルとして公開されている。

2.4 暗号 API

- MD5 MD5(Message Digest algorithm 5) MD5 は、ハッシュ値を計算するためのハッシュ関数のひとつで、RSA 暗号の開発者のひとり、ロン・リベスト氏らによって開発された。IPsec や、POP before SMTP など、さまざまなセキュリティプロトコルで使われている一方、最近になって脆弱性も指摘されている。
- SHA-1 SHA-1 (シャーン) とは Secure Hash Algorithm 1 の略で、入力データを一定の手順で計算を行い、入力値のデータの長さに関わらず決まった長さの文字列を出力するハッシュ関数の一つ。生成された値は「ハッシュ値」(hash value) と呼ばれる。SHA-1 は NSA (米国家安全保障局) が考案し、1995 年に NIST (米国標準技術局) によって連邦情報処理標準の一つ (FIPS 180-1) として標準化された。2005 年頃から効率的に攻撃する手法がいくつか発見され十分な安全性が保たれなくなったため、近年では 2001 年に制定された後継の SHA-2 規格への移行が進んでいる。
- SHA-2 SHA-2 はハッシュ関数の計算手順 (アルゴリズム) を定義しており、どんな長さのデータからも常に同じ長さのハッシュ値を生成する。同じ原文からは必ず同じ値が得られる一方、少しでも異なる原文からはまったく違う値が得られる。データの伝送や複製を行なう際に、入力側と出力側でハッシュ値を求め一致すれば、途中で改ざんや欠落などが起こっていないことを確認することができる。また、暗号や認証、デジタル署名などの要素技術として様々な場面で利用されている。

2.5 API

API とは Application Programming Interface の略であり、あるコンピュータプログラム（ソフトウェア）の機能や管理するデータなどを、外部の他のプログラムから呼び出して利用するための手順やデータ形式などを定めた規約のこと。

- 公式 API Android の開発者向け公式 Web サイトである Android Developers の API リファレンスに記載されている
- サードパーティー製 API サードパーティーという意味は、サードパーティとは、特定のハードウェア、OS、ソフトウェア、あるいはサービスなどを対象として、それに対応する（プラットフォーム上で動作する、もしくは互換性のある）製品を販売・提供している、ただし、その対象となっている製品自体の開発元・販売元ではない企業のことで企業が提供しているものや、開発者が提供しているものがあるサードパーティー製 Google 社の tink(ティンク) や Facebook 社の Concealn(コンシール) がある。
- 独自実装等の API API 開発者が既存の API を利用せずに独自に実装した API や、先述 2 つに含まれないものを独自実装等の API とします。

2.6 Android Developers

公式ドキュメントといった場合 Android Developers を指す。Android Developers とは、Android アプリケーション開発者向けの Android 公式 Web サイトである。Android の詳細やドキュメントが提供されている。

2.7 API ドキュメント

API リファレンスとも呼ばれる。API による開発方法やクラス内のメソッドの使用方法を解説した説明書のこと

2.8 Linux とは

Linux とは OS の一種で、パソコンを動かすのに必要な基本ソフトウェアの 1 つです。

2.9 Ubuntu

Ubuntu は Linux 系の OS。

2.10 シェル

コンピュータの OS を構成するソフトウェアの 1 つで、利用者からの操作の受付や、利用者への情報の提示などを担当するもの。

2.11 シェルスクリプト

OS を操作するためのシェル上で実行 (スクリプト言語)。また、そのような言語によって書かれた、複数の OS コマンドや制御文などを組み合わせた簡易なプログラム。一般的には UNIX 系 OS のシェルで実行できるものを指す

3 関連研究

本研究における関連研究を紹介する。

3.1 河合らの調査

河合による調査は [] は、

3.2 Yに関連した研究

あああああ

- まずは
- この章のなかで書くことを
- 箇条書きで書き出してみる
- ことから始めましょう

4 提案手法のメインな部分

あああああ

あああああ

- まずは
- この章のなかで書くことを
- 箇条書きで書き出してみる
- ことから始めましょう

5 提案手法の試作みたいなのを書く部分

あああああ

あああああ

- まずは
- この章のなかで書くことを
- 箇条書きで書き出してみる
- ことから始めましょう

6 試作を用いて評価

あああああ

あああああ

- まずは
- この章のなかで書くことを
- 箇条書きで書き出してみる
- ことから始めましょう

7 まとめ

あああああ

あああああ

- まずは
- この章のなかで書くことを
- 箇条書きで書き出してみる
- ことから始めましょう

参考文献

- [1] だれだれ, "文献 1", 年度
- [2] だれだれ, "文献 2", 年度
- [3] だれだれ, "文献 3", 年度
- [4] だれだれ, "文献 4", 年度
- [5] だれだれ, "文献 5", 年度
- [6] だれだれ, "文献 6", 年度
- [7] だれだれ, "文献 7", 年度
- [8] だれだれ, "文献 8", 年度
- [9] だれだれ, "文献 9", 年度
- [10] だれだれ, "文献 10", 年度