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

概要文みてかくといいかも

2　前提知識

2.1　Android

Android とは、Googel 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、また Android OS が搭載された端末のことである。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である。

2.3　Android アプリケーション

Java というプログラミング言語で作成されている。Java プログラムをコンパイルして機械語に変換し、画像などのリソースと合わせて apk というパッケージにすることで Android にインストールできるアプリである。

2.4　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である。APK とは”.apk”という拡張子を持つが、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 などで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。

2.5　APK ストア

APK ストアとは、Android アプリケーション開発者の作成した Android アプリケーションの配信を代行するサービス、およびそれを行っている Web サイトのことである。Android の公式 APK ストアは、Android の公式 APK ストアである GooglePlay[10]1 つのみであり, 非公式の APK ストアは数多く存在する。

2.6　Android Developers

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

2.7 smali ファイル

smali とは、Android の Dalvik 仮想マシンで使用されるアセンブリ言語 Smali で書かれた開発者ファイルである。通常、Android アプリケーションに含まれている実行可能ファイルである。DEX（Dalvik 実行可能）ファイル（.apk ファイル）を逆コンパイルすることによって作成される。Apktool や Baksmali を使って app ファイルを展開するとプログラム部分の classes.dex が展開され smali ファイルに分かれる。つまり、smali ファイルとは Java をコンパイルした後の機械語の状態のファイルである。これは Android アプリ（.APK ファイル）に含まれる実行ファイルである。

2.8 暗号技術

2.8.1 MD5

MD5 は、Message Digest algorithm 5 の略であり、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ー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。

2.8.2 SHA-1

SHA-1（シャーワン）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。

2.8.3 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、途中で改竄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。

2.9 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である。これは、3 種類に分けられる。

2.9.1 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 API である。

2.9.2 サードパーティー製 API

サードパーティーとは、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・提供しているという意味である。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 API という。Google 社の tink(ティンク) や Facebook 社の Concealn(コンシール) がある。

2.9.3 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 とする。

2.10 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である。

2.11 Liux

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。

2.12 Ubuntu

Ubuntu は Linux 系の OS。

2.13 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。

2.14 シェルスプリクト

OS を操作するためのシェル上で実行 (スプリクト言語)。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、Android アプリケーションを調査対象とし、Android アプリケーションの暗号技術利用に関する現状を明らかにするために暗号で用いられるメソッド名や特徴のある用語によるフィルタリングアルゴリズムが指定可能な代表的箇所の抽出や API の利用傾向分析をしていた。ていた。しかし、河合の研究では And 公式 API のみの調査しか行われていない。

3.2　Y に関連した研究

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　残課題

サードパーティー製 API

8　まとめ

まとめえええええええええええええええええええ

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