卒業論文要旨

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

5517097
山口千尋

開発者向けユーザブルセキュリティ、ユーザブルプライバシーの研究分野においてソフトウェア開発者の暗号技術の利用に関する研究が活発になっている。それらの研究により、暗号技術の利用が適切にされておらず脆弱性が存在するソフトウェアが多数あることが判明している。

これまでの研究は、SSL/TLS や DES、AES など特定の暗号技術に限った調査だけであり、暗号技術全般の網羅的な調査が行われていない。これに対し、河合による先行研究 [1] では、Java で開発された 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。

しかし、河合の研究では Android の開発者向け公式 Web サイトである Android Developers[2] の API リファレンスに記載されている公式 API のみの調査しか行われていない。その他の API としては、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、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 つに含まれない独自実装等の API が存在する。

独自実装等の API はドキュメントが公開されている可能性が低いため API のリスト化が困難である。これは、RSA や ECC、Crypto といった暗号、セキュリティに関するキーワードを API のリストの代わりとし検索する必要があるため APK の網羅的調査を行う上で困難である。比較して、サードパーティー製 API ではドキュメントが公開されているものもあるのでリスト化の困難性が少ない。そこで、本研究では特にサードパーティー製 API を分析対象とする。

サードパーティ製 API の例としては、Google 社の Tink[3] や Facebook 社の Conceal[4] がある。この中でも Tink は、Android OS を提供している Google 社によるサードパーティ製 API であるため、Android アプリケーション開発者にも利用されている可能性は高いと考えられる。本研究では Tink を調査対象とした。

Tink は現在、AEAD(関連データを備えた認証付き暗号)、MAC(メッセージ認証コード)、PublicKeySign と PublicKeyVerify(ディジタル署名)、HybridEncrypt と HybridDecrypt(ハイブリッド暗号化) の 4 つのプリミティブを使用して実装された暗号化操作を提供している。また、Tink はドキュメントが公開されている。このドキュメントの全クラスのページから 705 個の Method 部分のリスト化を行った。

APK において利用される API のマッチング調査の対象として、AndroZoo[5] のデータセットより取得した 316,277 個の APK を展開した smali ファイルを使用する。

調査の結果、Tink を利用しているのはパッケージ名が”mobi.zapzap” の APK だけであった。この APK では、AndroidKeysetManager クラスとそのメソッドが使用されている。このアプリケーション名は、”ZapZap - Mobile Wallet”[6] であり日本ではサービスしていない Android 版モバイルアプリケーションである。使用されている API の分析から設定値を保存する SharedPreferences へのアクセスに Tink 上の AndroidKeysetManager クラスとそのメソッドを使用しているため、暗号技術そのものとして Tink は使用されていないと考えられる。

Tink 利用が Android 公式 API よりも大幅に少ない理由として、Tink1.0.0 のリリース開始が 2017 年 9 月と最近である点と、Android では公式 API の利用が中心的である点が考えられる。

今後は、より詳しい API での暗号技術利用傾向を

知るために他のサードパーティ製 API や、独自実装等の API に調査の幅を広げる必要があると考えられる。

参考文献

[1] 河合惇丞.”Android アプリケーションにおける暗号技術利用動向の網羅的調査”.2020.

[2] Android Developers, ”Android Developers”, https://developer.android.com/index.html?hl=ja,（参照 2021-01-25）

[3] Tink, ”Tink”, https://github.com/google/tink,（参照 2021-01-25）

[4] Conceal, ”Conceal”, https://github.com/facebookarchive/conceal,（参照 2021-01-25）

[5] Université du Luxembourg, ”AndroZoo”, https://androzoo.uni.lu/,（参照 2021-01-25）

[6] Wonderwill Limited, ”ZapZap - Mobile Wallet”,https://www.zapzapwallet.com/,（参照 2021-01-25）