卒業研究中間発表概要

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。

他の研究では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つに含まれないものを独自実装等のAPIが存在する。

そこで、より網羅的な調査のために他のライブラリやAPKのデータ規模を拡大し調査の幅を広げていく。

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]、Twitter社のGeduldig[5] がある。この中でもTinkは、AndroidOS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ので本研究の調査対象とする。

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。このドキュメントから、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[6] のデータセットより411,486個のAPKから展開に成功した401,971個の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”[7] 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ので、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。以上より、Tinkはあまり使用されていないことがわかった。

理由としては、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調査が必要であると考えられる。

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] Geduldig, ”Geduldig”, https://github.com/geduldig, （参照 2021-01-25）

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

[7] ZapZap, ”ZapZap ”,https://www.zapzapwallet.com/, （参照 2021-01-25）