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。

サードパーティ製のAPIの分析ではまずAPIのリスト化を行う必要があるが、サードパーティー製APIは公式APIとは違いドキュメントが作成されていないものがある。存在しない場合はサードパーティ製のAPIのソースコードを解析し、APIのドキュメントを作成してからAPIのリストの作成を行う。APKを取得し、APKからsmaliファイルを展開し、展開したsmaliファイルと調査対象のAPIのリストとのマッチングを行う。マッチング結果を各APKごとに利用したメソッドをCSV形式でファイルに記述し、現状どの程度暗号技術が利用されているのか、その時のアルゴリズムはどのようなものが多く利用されているのか探っていく。現在は、Android OSとAPKの関係性、Javaと Androidアプリの関係性を理解し、 知識を付けるために河合の論文を読み、Javaの暗号APIとはどんなものか理解するためにAES暗号とRSA暗号を使い暗号化するプログラムを作成した。

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.[1]

[2] Android Developers. https://developer.android.com/index.html?hl=ja, 参照 2020-11-25. [2]