



Android端末デバッグ セキュリティオプションのご紹介

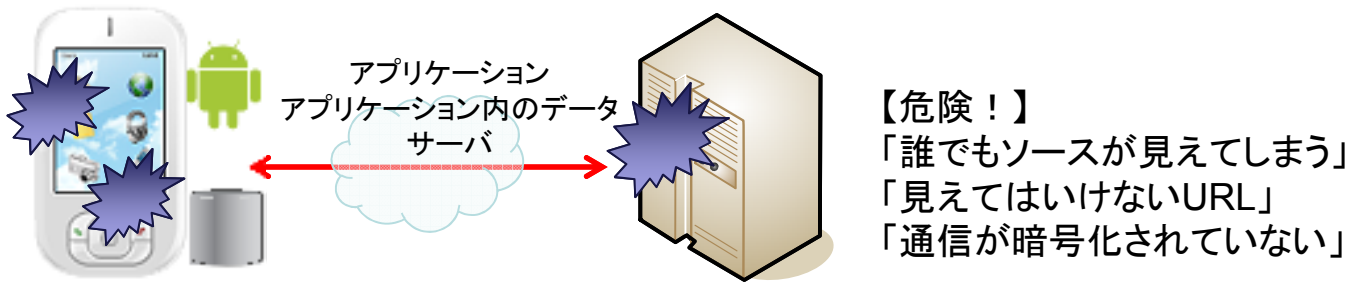


■はじめに

Google端末をはじめ、多くの機種不正利用に関する情報がネット上に流れています。
その情報を利用すれば、端末で保護されていたアプリケーションが解析されて、アプリケーションとサーバ間の通信、アプリケーション内のデータなどの機密情報が奪取される可能性があります。

必須!?

Free & OpenなAndroid端末には、
セキュリティ制御が無効化される事を前提に、安全性を確保すること



保護対象	Root権限を奪取された場合の危険性
アプリケーション	アプリケーションのリバースエンジニアリング→アプリケーションの改変・サーバ側データの流出
アプリケーション内のデータ	ユーザデータの奪取 各変数名の暴露 → サーバ側データの流出
サーバ	サーバ内アプリケーションの破壊 サーバ内機密データの流出

■セキュリティオプションの種類

	“Essentials”	“Basic”	“Advanced”
対象範囲			
	検査深度		

- ← 【実動サーバ側アプリの確認】
様々な方法でサーバ側の安全性を確認します。
- ← 【実機端末アプリの確認】
全体的な懸念事項を実機端末にて再現確認をします。
- ← 【設計仕様による確認】
ご準備頂いた資料よりセキュリティの懸念事項をご提示します。



Android端末デバッグ セキュリティオプションの作業内容

■ Essentialsの作業内容

■ リバースエンジニアリングの可否

① 難読化確認

root化された端末での、対象apkファイル移動、解凍、変換→ソース閲覧という手順で、平文で書かれているかどうかを確認します。

② 閲覧できたソースの難読化実施状態確認

この際に、URL及びデータ変数の難読化状況を確認します。

■ 機密データの閲覧可否

① 外部リソースへのアクセス状況確認

ソース内URLが可読できる場合に、全URLをリストアップします。一般には隠されているURLが平文で読めたり、想定していないURLの存在をリストから確認することが出来ます。

② 設定情報確認

Shared Preferenceなど、実機で動作させた後に保存される設定ファイルを確認して、機密情報が保管されていないかどうかを確認します。

(例: 認証情報(ID及びパスワード)の平文保存など)

■ 通信秘匿性強度

① アプリからサーバに通信する場合の認証方式

仕様書及び(可能な場合)実機で認証方式を確認し、その安全性を確認します。また、仕様書で1次取得したデータをキャッシュする場所を確認し、保存場所・方法の安全性を確認します。

② 端末・サーバ間の暗号化通信の強度

仕様書で暗号化の強度(鍵長)などを確認します。

■ Basicの作業内容

実施内容	具体例
端末の不正利用等によるアプリケーションの不正使用	アプリケーション内データへの不正アクセス、アプリケーションのリバースエンジニアリングの可否(Javaコードの難読化の有無)、Wifiルータを介した通信の奪取
UIからの擬似攻撃	入力項目に対する不正コマンド稼働可否等 (SQLインジェクション等の主要な脆弱性カテゴリの可能性の有無※)
上記の仕様確認による懸念点調査	認証方式の確認等

■ Advancedの作業内容

実施内容	具体例
サーバ側の安全性確認	データの秘匿性の確認、個人識別認証の確認
ソースコード診断	静的解析(Fortify360を使用)で問題の洗い出し
疑似攻撃診断	エージェント偽装によるブラックボックス診断で問題の洗い出し
個別端末確認	公に認知されている端末・OSによる脆弱性の悪用によるアプリケーション・端末の情報流出の可能性

詳しくは営業担当へお問い合わせ下さい。TEL:03-3379-2072(営業部直通)