SSLサーバ証明書の認証レベルに着目した悪性Androidアプリ検知手法

情報工学科　笹瀬研究室　加藤広野、春田秀一郎、笹瀬巌

研究背景

端末から個人情報を取得し、ユーザの意図とは関係なく外部サーバに送信する悪性Androidアプリが横行

└ 近年、パケット解析を困難にするために暗号化を用いる悪性アプリが増加傾向

従来方式

良性と悪性アプリ間でネットワークトラフィックのパターンに差異が生じる事に着目し機械学習により検知

└ パケット解析なしで特徴を取得可能なため暗号化を用いる悪性アプリに対応可能

問題点

単なる統計的な特徴であるため、各特徴が悪性の通信であるかの判定は不可能であり正確な検知には不十分

攻撃者が利用せざるを得ない要素を基に悪性の通信をより正確に特徴に反映することが必要

提案方式

- 悪性アプリは暗号化パケットを送信するために信頼性の低いサーバと通信を行う傾向（図１）
- サーバの信頼性は通信の暗号化に必須なSSLサーバ証明書の認証レベルにより判別可能

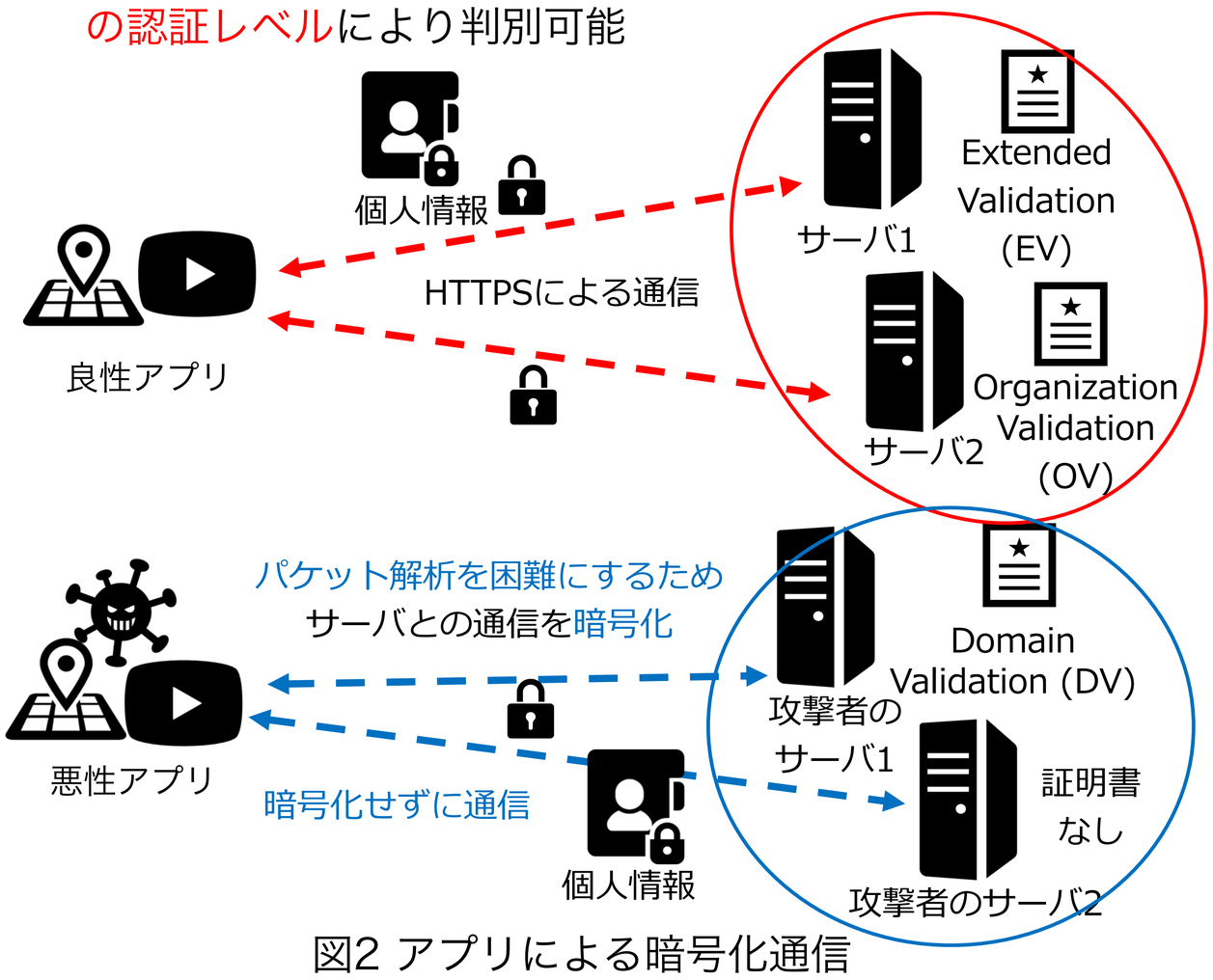

図2 アプリによる暗号化通信

- 宛先サーバに着目しているため、暗号化に対応可能
- DVおよび証明書のないサーバとの通信のみから特徴を取得
- さらに正確な特徴を取得するため、要求する権限（端末情報などの取得に必須）を基にした重みを導入
- 取得した特徴を用いて機械学習により検知

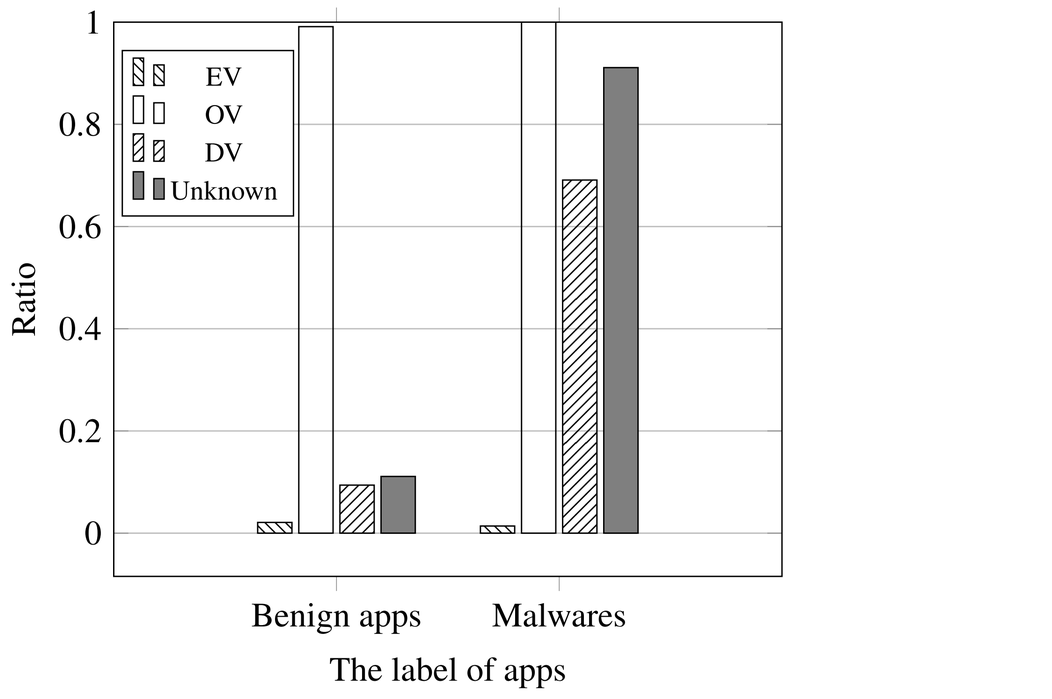

図1 宛先サーバのSSL証明書の認証レベルに関する検証結果

特性評価

良性アプリ：801個
悪性アプリ：884個 に対して
正解率、TPR (True Positive Rate)およびFPR (False Positive Rate)を比較

表1 検知性能の評価結果

	正解率(%)	TPR(%)	FPR(%)
従来方式	88.2	88.2	11.7
提案方式	92.7	93.8	8.48

提案方式は正解率、TPRおよびFPRを改善

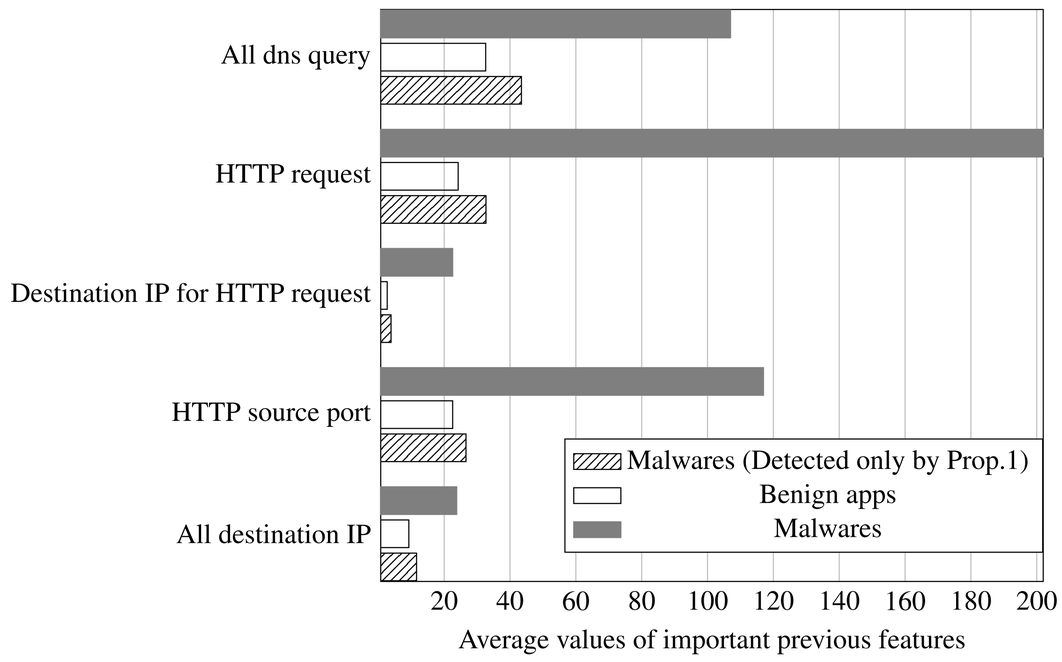

図3 提案方式でのみ検知可能な悪性アプリに関する評価

提案方式は、従来方式において重要度の高い特徴が良性と類似するため検知できない悪性アプリを検知可能

結論

本研究では、SSLサーバ証明書の認証レベルに着目した悪性Androidアプリ検知手法を提案し、従来方式の検知精度を改善可能であることを示した.

本研究に関する業績

[1] Hiroya Kato, Shuichiro Haruta and Iwao Sasase, " Android Malware Detection Scheme Based on Level of SSL Server Certificate, " IEICE Transactions on Information and Systems Vol.E103-D, No.02, pp.379-389, Feb. 2020.
[2] Hiroya Kato, Shuichiro Haruta and Iwao Sasase, "Android Malware Detection Scheme Based on Level of SSL Server Certificate," IEEE GLOBECOM 2019, Waikoloa, HI, USA, 9-13 December 2019.
[3] 加藤 広野, 春田 秀一郎, 笹瀬 巌, “SSLサーバ証明書の認証レベルに着目した悪性Androidアプリ検知手法,” 通信方式研究会, CS2019 -15 pp.13 -18, 2019 年 7 月 4日.