色相を利用して自動的に検知範囲を拡大可能なフィッシングサイト検知法

慶應義塾大学　春田秀一郎，山崎史貴，朝比奈啓，笹瀬巌

研究背景

ユーザの個人情報を狙うフィッシングサイト(PWS:Phishing Website)の検知が急務，
視覚情報を用いた検知方式に注目

従来方式（シグネチャベース検知）

PWSは標的サイトを模倣して作成されるため，標的サイト，同一の標的を持つPWS間でレイアウトや色の位置などの視覚情報が類似
➡視覚情報を「シグネチャ」と呼ばれる特徴マップに記述，データベースに格納し，これに類似するシグネチャを持つサイトをPWSと判定（図1）

問題点

従来方式のシグネチャはPWSの亜種間の類似度の差異が大きいため(図2)，多くのタイプのPWSを検知するためには人力による多くのシグネチャの登録が必要 ➡ ゼロデイ攻撃が発生しやすい
・シグネチャを自動的に追加していく機構が必要

提案方式

PWSは標的サイトおよび他の亜種を元に作られ，それらの亜種間では類似した色相が用いられる(図3)ため，色相の類似する亜種を追跡することで多くの亜種が検知可能 ➡ データベースに登録されている検知済みPWSと似た色相を持つサイトを登録済みのPWSの亜種として検知し，データベースに自動的に追加することで，検知範囲を拡大

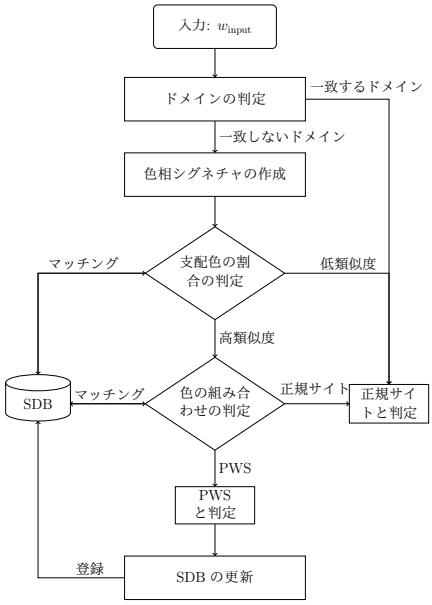


図4 提案方式の検知フロー

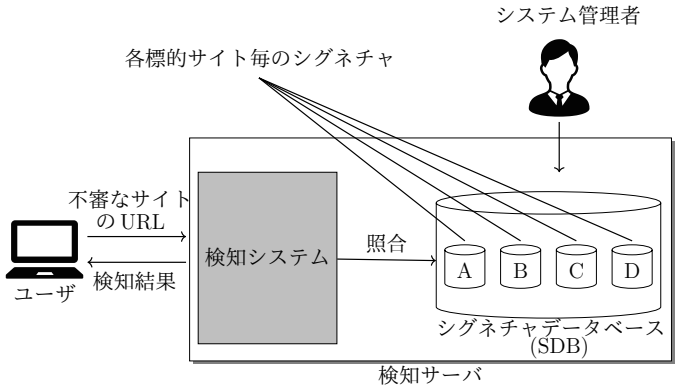


図1 検知システム

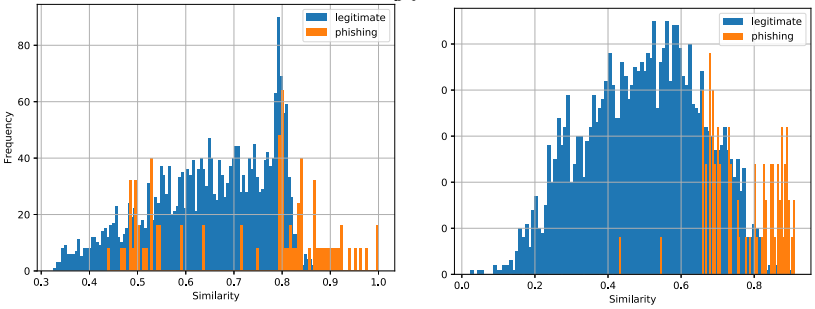
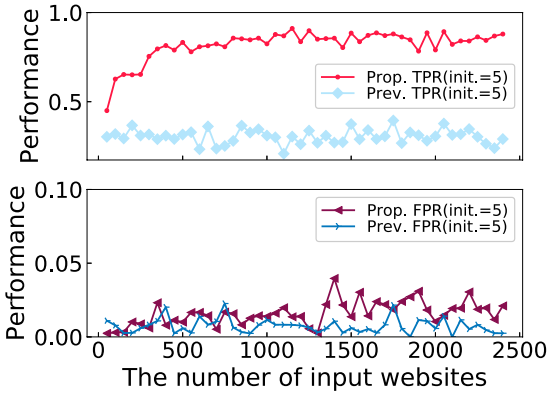


図2, 3 従来，提案におけるPWSの亜種の類似度の分布 (Facebookデータセット)

特性評価

正規サイト:1800件
FacebookのPWS : 656件



・FPR(False Positive Rate) を低く抑制しつつ
・TPR(True Positive Rate)は入力サイト数増加に伴い上昇

結論

本研究では，色相を利用して自動的に検知範囲を拡大可能なフィッシングサイト検知法を提案した．
シミュレーションにより，提案した色相シグネチャを自動更新と共に用いることで検知範囲を描くだ可能であることを示した．

本研究の業績

[1] S. Haruta, H. Asahina, F. Yanazaki, and I. Sasase, “Hue Signature Auto Update System for Visual Similarity-based Phishing Detection with Tolerance to Zero- day Attack, ” IEICE Trans. on Information and Systems Vol.E102-D, No.12, pp.2461-2471, Dec. 2019
[2] S. Haruta, F. Yamazaki, H. Asahina, and I. Sasase, “A Novel Visual Similarity- based Phishing Detection Scheme using Hue Information with Auto Updating Database, ” in IEEE APCC, Ho Chi Minh city, Vietnam, Nov. 6-8, 2019.
[3] 春田秀一郎, 山崎史貴, 朝比奈啓, 笹瀬巌, “色相を利用して自動的に検知範 囲を拡大可能なフィッシングサイト検知法,” 電子情報通信学会通信方式研 究会、CS2019-14, pp.7-12, 2019 年 7 月 4 日.

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

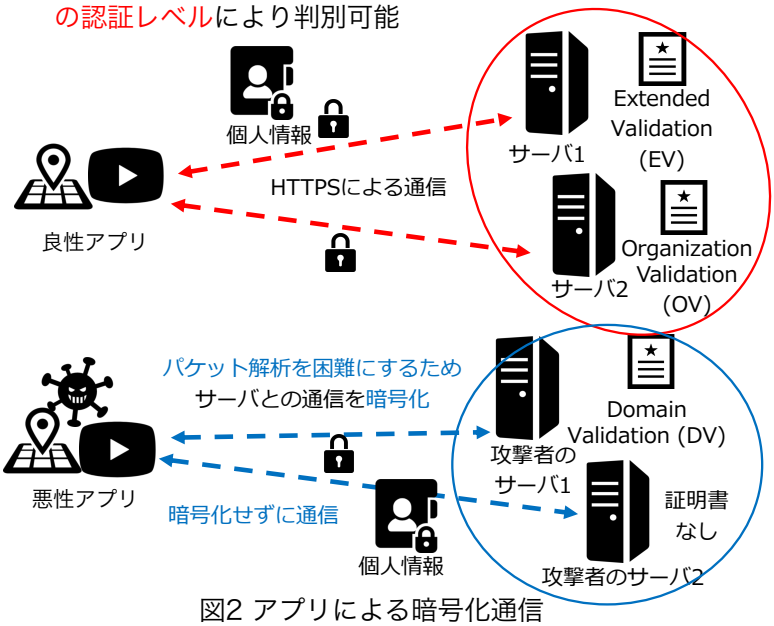


図2 アプリによる暗号化通信

- 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

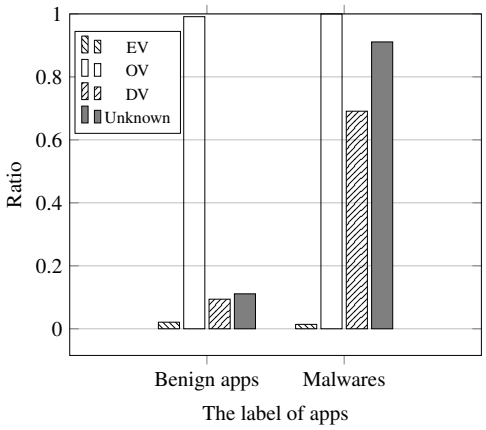


図1 宛先サーバのSSL証明書の認証レベルに関する検証結果

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

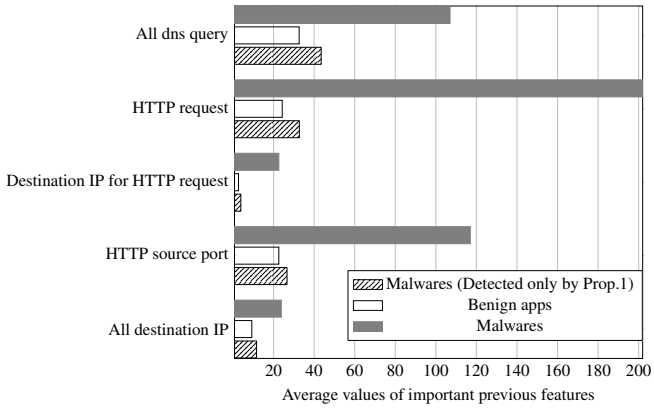


図3 提案方式でのみ検知可能な悪性アプリに関する評価

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.-, 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.