[Work in Progress] 研究報告

SSL/TLS証明書情報を用いた悪性Webサーバの検出

大室 高帆[1]　新城 靖[†1]　三宮 秀次[†1]　佐藤 聡[†1]

The Detection of Malicious Web Server by using SSL/TLS Certification

インターネットが世界中で利用されている現在において、情報の機密性を確保することは必須である。Web コンテンツの送受信においては従来の HTTP に SSL/TLS による暗号・認証機能を付与した HTTPS が用いられることが増えてきた。HTTPS では通信内容が暗号化されており、通信内容を監査してサイバーセキュリティ攻撃を検知する侵入検知装置等が正常に機能しなくなる可能性がある。特にマルウェアも HTTPS を使うようになるとマルウェアが悪性サイトに情報を流出させることを阻止できなくなる。このような事態を防ぐために、機微な情報を送信する前に通信相手の信頼性を確認することが重要となる。

本研究では HTTPS 通信において、第三者に通信相手に関する情報を送信することなく、機微情報を送信する前に通信相手の信頼性を判断する手法の開発を目的とする。目的の実現のために、あらかじめ良性・悪性と判明している対象サーバに対し TLS ネゴシエーションを行い、証明書情報などを収集する。これらのデータを用い教師あり学習を行い、ルールを生成することにより、良性・悪性の判別を行える手法を開発する。目標は接続先情報を秘匿したままローカル環境で当該サーバの安全性を確かめることができることである。

収集する情報に関しては、あらかじめ良性・悪性であると判明しているサーバ群のリストを入手し、それぞれからデータを収集する。今回、良性サーバは Cisco 社が無料で提供している Top 1 million[1] のリストおよびそれに類似するものと定義し、悪性サーバに関しては malwaresite.com[2] に掲載されている各種マルウェアサイトのリストおよびこれに類似するものと定義する。収集するデータは証明書情報、プロトコルスイート 、ネゴシエーション時のパケットである。まずはじめに、調査対象サーバの FQDN が指し示す全ての IP アドレスを調査できるように IP アドレスの取得に際し getaddrinfo を用い、出力であるアドレスのリストの全てに関して情報を収集した。次に、調査対象サーバの IP に複数 FQDN が割り振られている場合には対象の FQDN を適切に調査するために、ClientHello における SNI の servername フィールドに目的のドメインを明示した。最後に調査対象となるサーバの HTTPS に関する設定情報を可能な限り収集した。具体的には HTTPS ではクライアントとの間で暗号のプロトコルスイートのネゴシエーションを行うが、サーバ側ではどのプロトコルスイートを優先するかの設定があるので、これらの情報も取得を試みた。

収集に際しては、C 言語で作成したクライアントで対象サーバに接続し、ハンドシェイクの間にやり取りされたパケットを tcpdump で収集するという形式をとった。クライアントについては OpenSSL のライブラリを使用しており、C 言語で実装を行なった。プロトコルスイートに関しては、まずスイートを指定せずに接続を行いサーバ側で採用されたものを序列一位のスイートとして記録した。次に、一位以外のスイートでの接続を要求し、採用されたスイートを序列二位とする。以下これを繰り返し、サーバのプロトコルスイートの優先順位を取得した。同時に tcpdump を用いて clienthello, serverhello パケットを収集することにより、ネゴシエーションがうまくいかない場合の理由の分析も行える。

収集によって得られた情報を教師として学習を行い、良性・悪性のサーバを分類するルールの生成を目指す。方針としては、悪性と良性の二種に分類を行うか、あるいは悪性の度合いを計る指標を準備しその値で評価を行う方法を考えている。学習に際しては、プロトコルスイート 、部分木などはカテゴリ要素として扱い、python の scikit-learn 等を用いて学習を行う。

参考文献

[1] Cisco, Cisco Popularity List Top 1 million, Cisco Umbrella 1 Million, http://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip (accessed Oct 26, 2018)
[2] RiskAnalytics, BH DNS Files, DNS-BH Malware Domain Blocklist by RiskAnalytics, http://malware-domains.com/files/domains.zip (accessed Oct 26, 2018)

[1] 筑波大学情報科学類
University of Tsukuba College of Information Science
[†1] 現在，筑波大学
Presently with University of Tsukuba