[ポスター発表] 研究報告

SSL/TLSハンドシェイク時に取得可能な情報を用いたWebサーバの信用度算定に関する検討

大室 高帆[1]　新城 靖[2]　中井 央[3,4]　三宮 秀次[2,4]　佐藤 聡[2,4]

The Study about Calculation Method of Web Server's Credibility by Using Information of SSL/TLS Handshake.

1. はじめに

インターネットが世界中で利用されている現代において, 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 がほとんどの場合用いられている. HTTPS 通信は比較的安全だが, 機密情報を送信する前に通信相手の見極めを行うことは重要である. Virustotal などのサービスを利用することで既存のドメインの安全性は確認できる. しかし, 未知のサーバの信頼性を見極める有効な手段は確立されていない.

本研究は任意のドメインを精査できる環境を実現し, より安全な HTTPS 通信を行うことを目的とする. 手法としては, 任意のサーバに対し TLS ネゴシエーションを行い, 終了時点までに得られる情報のみを用いて当該サーバの信用度を算定することを提案する. 具体的には, 各サーバとの TLS ネゴシエーションで得られる証明書情報, 暗号スイートの設定情報及びドメイン情報 (以下, ネゴシエーション情報とする）を収集する. ネゴシエーション情報から抽出された特徴量の出現確率を用い, ベイジアンフィルタを作成しカテゴリ分類を行う. 作成したフィルタはクロスバリデーションで評価する.

1 筑波大学大学院博士前期課程システム情報工学研究科コンピュータサイエンス専攻
Master's Program in Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba
2 筑波大学システム情報系
Faculty of Engineering, Information and Systems, University of Tsukuba
3 筑波大学図書館情報メディア系
Faculty of Library, Information and Media Science, University of Tsukuba
4 筑波大学学術情報メディアセンター
Academic Computing & Communications Center, University of Tsukuba

2. ベイジアンフィルタの使用

ベイジアンフィルタとは, ベイズ理論を応用した文書等の学習フィルタである [2]. 学習量と精度が向上する性質を利用し, メールのスパム判定などに用いられている [1]. 今回はネゴシエーション情報から特徴量を抽出し, 各特徴量における特定の値の出現確率を使用して調査対象サーバ x について信用できないサーバ群 (以下, 悪性サーバ群とする)M とそれ以外のサーバ群 (以下, 良性サーバ群とする)N へとベイジアンフィルタにより分類する. 各サーバのネゴシエーション情報から n 種類の特徴量 $p_1, ..., p_n$ が得られ, 調査対象サーバ x における特徴量の値が $p_{1_x}, ..., p_{n_x}$ であるとき, x が M に分類される確率を求める手順を示す.

(1) カテゴリ出現率の計算
既知のサーバのうち M となるサーバの総数を M_n, 既知のサーバのうち N となるサーバ総数を N_n とする. この時, 全てのサーバに対して M と分類されるサーバの割合 P(M) および N と分類されるサーバの割合 P(N) を以下のように定める.

$$\begin{aligned} P(M) &= M_n/(M_n + N_n) \\ P(N) &= N_n/(M_n + N_n) \end{aligned} \tag{1}$$

(2) 各カテゴリで調査対象が出現する確率の計算
M に属するサーバにおいて特徴量 p_1 が p_{1_x} になる確率を $P(p_1 = p_{1_x}|M)$ とし, この確率を $p_{1_x}, ..., p_{n_x}$ 全てについて求める. このとき, M において x が出現する確率 $P_M(x)$ を以下のように定める.

$$P_M(x) = \prod_{k=1}^{n} P(p_k = p_{k_x}|M) \tag{2}$$

(3) 調査対象サーバ x が M に分類される確率 $P_x(M)$
(1) と (2) を用い以下の様に計算する.

$$P_x(M) = P(M)P_M(x) \tag{3}$$

表 1 予備実験において収集した事項

大項目	小項目	良性サーバにおける考慮点
証明書	ルート認証局	安定化のため信頼できる認証局を利用する
	有効期間	運用・保守の観点から短すぎない適切な期間を取る
ドメイン情報	レジストラ名	信頼できるレジストラを利用する
	初回登録年月日	(良いサービスほど長く利用される)
	有効期間	運用・保守の観点から短すぎない適切な期間を取る
暗号スイート	暗号スイートの設定	様々な端末でアクセス可能とする, セキュリティを強化する

表 2 データが収集できた割合

属性名	対象 サイト数	収集できた サイト数	収集できた 割合 (%)
良性	23,000	18,175	79.0
悪性	23,000	5,958	25.9

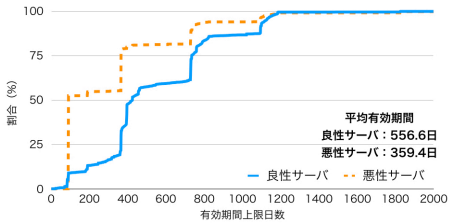

図 1 証明書の有効期間に関する累積相対度数分布グラフ

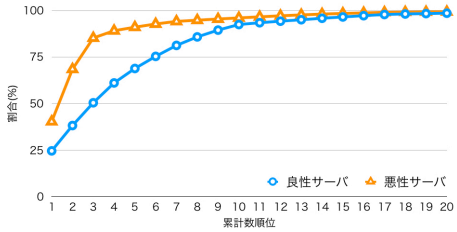

図 2 証明書のルート認証局に関する累積相対度数分布グラフ

同様に N に分類される確率も計算し, $P_x(M) > P_x(N)$ なら x を M に分類する.

3. 予備実験の結果

HTTPS サーバからネゴシエーション情報を収集する予備実験を行なった. 予備実験では, Cisco 社が無料で提供している Top 1 million のリスト [3] に含まれるものを良性サーバ群, DNS-BH Malware Domain Blocklist に掲載されている各種マルウェアサイトのリスト [4] に含まれるものを悪性サーバ群と定義した. 調査では表 1 に示した情報を良性サーバ群, 悪性サーバ群それぞれから 23,000 ずつを選択した. サーバによっては応答しない場合もあった. 結果を表 2 に示す.

収集した結果のうち, 証明書の有効期間やルート認証局において顕著な違いが見られた. 証明書の有効期間の結果を図 1 に示す. 平均日数は良性サーバ群で 556.6 日, 悪性サーバ群で 359.4 日であった. 悪性サーバ群では有効期間が 90 日のサーバが多く, これは Let's Encrypt 等の無料証明書が多く使われているためである. ルート認証局の結果を図 2 に示す. 悪性サーバでは Let's Encrypt で用いられるルート認証局など特定の認証局が集中して使われていた.

4. 特徴量出現確率の計算と評価

本研究にてベイジアンフィルタを用いるためには, 抽出した特徴量が特定の値になる確率をカテゴリ別に求める必要がある. 例えば, ある良性サーバが特定のルート認証局 A を利用している確率は, 収集済みの良性サーバ群の証明書情報における A の利用率を用いて求められる. また, 特定の有効期間の出現確率は, 有効期間を一定期間で区切った区間を用いる. その有効期間を含む区間に含まれる証明書の数が, テストデータ全体に対して占める割合を用いて出現確率を求める. なお, 表 1 にて示した他の特徴量については, 出現確率を求める方法を検討中である.

5. おわりに

今後の課題として, 収集した情報から抽出した特徴量の出現確率を求め, ベイジアンフィルタで使用する手法を特徴量ごとに検討することが挙げられる. 例えば, 証明書・ドメインの有効期間については, 区間の適切な分割方法を決定する必要がある. またドメイン名の文字列について, 特定の単語と悪質さの相関を調査し, サーバ識別における有効性を確認する.

参考文献

[1] 岩永, 田端, 櫻井. "ベイジアンフィルタリングを用いた迷惑メール対策における多言語環境でのコーパス分離手法の提案と評価 ". **情報処理学会論文誌**. *Vol.46 No.8.* pp.1959-1966. 2006.

[2] 田端利宏. "SPAM メール フィルタリング：ベイジアンフィルタの解説 (<特集>情報のフィルタリング)". **情報の科学と技術**. *Vol.56 No.10.* pp.464-468. 2006.

[3] 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)

[4] RiskAnalytics. BH DNS Files, DNS-BH Malware Domain Blocklist by RiskAnalytics. http://malware-domains.com/files/domains.zip (accessed Oct 26, 2018)