暗号化 C2 通信検出用マルチビューモデルの分析及び改善に関する研究

Analysis and improvement proposal of encrypted C2 communication detection multiview model design.

佐藤 龍　システム分科会　情報セキュリティ大学院大学

Abstract: This study examines multi-view models for threat detection in TLS-encrypted communications, where payload-based analysis is ineffective. Using visualization experiments, it evaluates model robustness under TLS protocol changes and identifies design factors that degrade adaptability. The proposed improvements enhance the stability of threat detection in evolving real-world environments.

1. 背景と目的

近年、Web 閲覧トラヒックの 81%以上が TLS で暗号化され、マルウェアの C2 通信も 87.2%が暗号化を利用している [1,2,3]。これにより、従来のペイロード分析が困難となり、SOC における脅威検出の障害となっている。

これに対し、複数の視点から通信特性を捉える**マルチビューモデル**（MVDet[4] 等）が注目されているが、最新の **TLS 1.3 環境**やプロトコル変化に対する頑強性の検証は不十分である。本研究では、環境変化に対するモデルの頑強性を分析し、具体的な改善策を提案・検証することを目的とする。

2. 現状分析と課題

■ TLS 1.3 の影響可視化実験

予備調査の結果、一意の指紋数は TLS 1.2 の 105 通りに対し、TLS 1.3 では **6 通りまで減少**し、特定の指紋に利用が偏ることが判明した。これは TLS 1.3 の仕様変更により、サーバ証明書等の情報が秘匿され、アプリケーションの区別が困難になったためである。

■ 設計上の見落とし

既存モデルは TLS ビューに **JA3 ハッシュ値**を採用している。ハッシュ関数の**雪崩効果**により、TLS パラメタが 1 ビットでも揺らぐと全く異なる指紋となり、モデルの頑強性が著しく低下する課題が浮き彫りとなった。

3. 提案手法

【提案 1】カテゴリ特徴量への転換

JA3 ハッシュ値の使用を廃止し、Extensions や Cipher Suite 等の各パラメタを**カテゴリ特徴量 (0/1)** として直接扱う設計を導入する。これにより、微小なパラメタの変化がハッシュ値によって極端に増幅されることを防ぐ。

【提案 2】ドメイン知識を活用した調整

変異解析の知見に基づき、揺らぎが発生しやすいことが既知のパラメタに対し、学習時の重み付けを調整する。人間による分析知見をモデル設計に反映させることで、未知の揺らぎに対する耐性を高める。

4. 評価実験と結果

評価指標として、偽陰性率が 0 となる最大閾値（**ZFT: Zero-FNR Threshold**）を用いた可視化実験を行った。

- **従来手法（揺らぎあり）**：ZFT = **0.008**
- **TLS ビュー削除**: ZFT = 0.427
- **提案手法 1（カテゴリ化）**：ZFT = **0.857**
- **提案手法 2（カテゴリ化＋ドメイン知識）**：ZFT = **0.960**

提案手法により、パラメタに揺らぎ（遮蔽）を付加した最悪のケースにおいても、高い精度で悪性通信を識別可能な頑強性を実現した。

5. 結論

SOC で実績のある TLS 指紋をそのまま機械学習に適用すると、環境変化に対する頑強性を損なうことが明らかになった。本研究の貢献は以下の 3 点である。

1. 特徴量選択の不備がモデル全体の頑強性を低下させる影響を実験的に解明。
2. ハッシュ値からカテゴリ特徴量への転換による頑強性向上を実証。
3. ドメイン知識の活用がモデルの安定性向上に寄与することを示した。

今後は、他のビューへの分析拡大や、より大規模な実環境データセットでの評価が望まれる。

6. 参考文献

[1] Google LLC. ウェブ上での HTTPS 暗号化 - Google 透明性レポート
[2] Sophos Ltd. 約半数のマルウェアが通信の隠蔽に TLS を利用-Sophos News
[3] Zscaler, Inc. ThreatLabz Report: 87.2Channels — Zscaler.
[4] Susu Cui, Xueying Han, Cong Dong, Yun Li, Song Liu, Zhigang Lu, and Yuling Liu. MVDet: Encrypted malware traffic detection via multi-view analysis. Journal of Computer Security, Vol. 32, No. 6, pp. 533–555, 2024.