TLS暗号化通信中の悪性通信識別手法について

A Method for Identifying Malicious Communication during TLS Encrypted Communication

佐藤龍・システム分科会・情報セキュリティ大学院大学

1. 研究背景

近年，情報セキュリティに関する意識の高まりやSEO対策などの目的からTLSによる通信の暗号化を行うWebサイトが急増している．しかし，TLS暗号化された通信は従来のセキュリティアプライアンスでは検査することができない．実際に攻撃者が悪性通信をTLSで暗号化することで検出を逃れようと試みる例も見られ，悪性通信を暗号化する傾向は今後益々強まってくると予想する．これに対し，SOC(セキュリティオペレーションセンタ)ではTLSの復号を行うことが可能なアプライアンスを用いて監視を行っているが，事前にネットワーク内の端末すべてにCA証明書をインストールしないと利用できず，そのような設定ができないIoT機器などでは復号機能の利用が難しいなど，TLS暗号化通信の取り扱いが大きな課題となっている．そこで，TLS通信を復号する事なく，マルウェアによる通信を検出する手法について調査，提案を行う．

2. 先行研究

[1] Oh, Chaeyeon, Joonseo Ha, and Heejun Roh. "A survey on TLS-encrypted malware network traffic analysis applicable to security operations centers." Applied Sciences 12.1 (2021): 155.

[2] Cui, Susu, et al. "MVDet: Encrypted malware traffic detection via multi-view analysis." Journal of Computer SecurityPreprint (2024): 1-23.

3. 研究課題

先行研究ではTLS1.3やQUICを対象とした方式は知る限り無く，TLS1.2とTCPを対象としていた．TLS 1.3ではプライバシーやセキュリティを重視して様々なメタデータの暗号化が行われるようになった為，検出精度の低下が懸念される．
しかし，TLS1.2とTCPを対象とした手法をTLS1.3の環境で評価した研究はまだ少なく，先行研究の手法が最新の環境でどの程度の有効性を持つかは未知数である．

4. 研究計画

a. 再現実験を通じて先行研究の有効性を確認
b. TLS1.3環境がマルウェア検出に与える影響や精度の変化に関する調査を実施
c. TLS1.3環境での利用を前提としたマルウェア通信検出手法の提案とその評価を行う