

修士論文

再帰問い合わせ名前解決へのハッシュ関数を用いた
DNS Exfiltration 緩和策の提案

高須賀 昌烈

2020 年 3 月 15 日

奈良先端科学技術大学院大学
先端科学技術研究科

本論文は奈良先端科学技術大学院大学先端科学技術研究科に
修士(工学) 授与の要件として提出した修士論文である。

高須賀 昌烈

審査委員：

門林 雄基 教授 (主指導教員)

笠原 正治 教授 (副指導教員)

林 優一 教授 (副指導教員)

妙中 雄三 准教授 (副指導教員)

再帰問い合わせ名前解決へのハッシュ関数を用いた DNS Exfiltration 緩和策の提案*

高須賀 昌烈

内容梗概

キーワード

DNS Exfiltration, 秘匿通信, ハッシュ関数, 再帰問い合わせ

*奈良先端科学技術大学院大学 先端科学技術研究科 修士論文, 2020 年 3 月 15 日.

Proposal for Mitigation of DNS Exfiltration using Hash Function to Recursive Name Resolution*

Shoretsu Takasuka

Abstract

Keywords:

DNS Exfiltration, Covert Channel, Hash Function, Recursive Name Resolution

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2020.

目次

1. 序論	1
1.1 研究背景	1
1.2 研究目的	1
1.3 研究対象	1
1.3.1 仮説	1
1.3.2 脅威モデル	1
1.4 本論の構成	1
2. 準備	2
2.1 DNS プロトコル	2
2.1.1 概要	2
2.1.2 DNS over HTTPS	2
2.1.3 DNS Exfiltration	2
2.1.4 DNS Tunneling	2
2.2 暗号学的ハッシュ関数	2
2.2.1 定義	2
2.2.2 性質	2
3. 関連研究	3
3.1 トラフィック特徴に基づいた悪性 DNS トランザクションの検知	3
3.1.1 同ドメインあたりのクエリ頻度	3
3.2 ペイロード特徴に基づいた悪性 DNS クエリの検知	3
3.2.1 文字列分布特徴	3
3.2.2 ペイロード特徴	3
3.3 ポスト DNS プロトコルによる悪性 DNS クエリの発生緩和	3
4. 提案手法	4
4.1 再起問い合わせにおけるハッシュ関数の適用	4

5. 評価	5
5.1 シミュレーション	5
5.2 結果	5
6. 議論	6
6.1 課題	6
6.2 貢献点	6
6.3 既存アプローチとの比較	6
7. 結論	7
7.1 総括	7
謝辞	8
参考文献	9
付録	10
A. 発表リスト (国内研究会)	10

图 目 次

表 目 次

1. 序論

1.1 研究背景

1.2 研究目的

1.3 研究対象

1.3.1 仮説

1.3.2 脅威モデル

1.4 本論の構成

2. 準備

本章では，本論において使用する用語及び技術について説明する．

2.1 DNS プロトコル

2.1.1 概要

2.1.2 DNS over HTTPS

2.1.3 DNS Exfiltration

2.1.4 DNS Tunneling

2.2 暗号学的ハッシュ関数

2.2.1 定義

2.2.2 性質

3. 関連研究

3.1 トラフィック特徴に基づいた悪性DNSトランザクションの検知

3.1.1 同ドメインあたりのクエリ頻度

3.2 ペイロード特徴に基づいた悪性DNSクエリの検知

3.2.1 文字列分布特徴

3.2.2 ペイロード特徴

3.3 ポストDNSプロトコルによる悪性DNSクエリの発生緩和

4. 提案手法

4.1 再起問い合わせにおけるハッシュ関数の適用

5. 評価

5.1 シミュレーション

5.2 結果

6. 議論

6.1 課題

6.2 貢献点

6.3 既存アプローチとの比較

7. 結論

7.1 総括

謝辞

ご指導ご鞭撻賜りありがとうございました.

参考文献

付録

A. 発表リスト (国内研究会)

1. 高須賀 昌烈, 妙中 雄三, 門林 雄基, “非実在ドメインに対するネガティブキャッシュの拡張と再帰問い合わせハッシュ化の提案”, 電子情報通信学会情報ネットワーク研究会, 2019-10-ICTSSL-IN, 2019 年 10 月.