Webサービスにおける信頼性を考慮したMTDシステムの提案

Proposal of Moving Target Defense Approach on Reliability in Web Services

研究駆動コース
13R 齋田 衛

モチベーション

- 新攻撃手法の登場と防御策作成の繰り返しを解消したい
- 数理的な観点からセキュリティに貢献したい

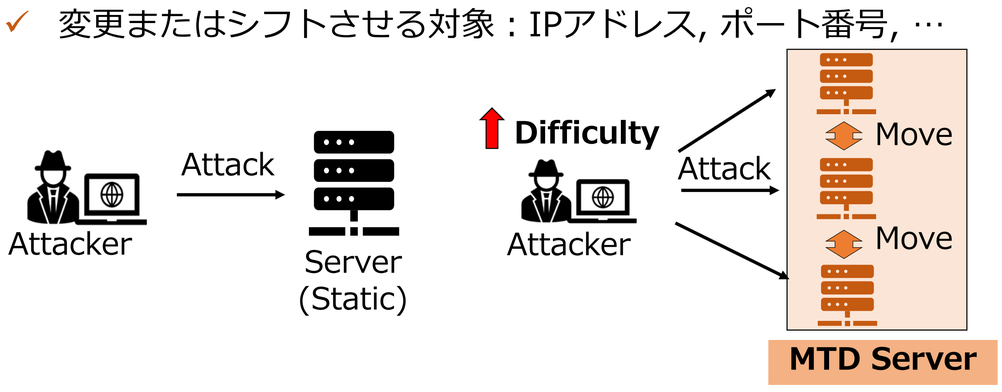
背景：Moving Target Defense (MTD)

従来 (静的) の防御策の限界

- 未知の脆弱性に対処することが難しい

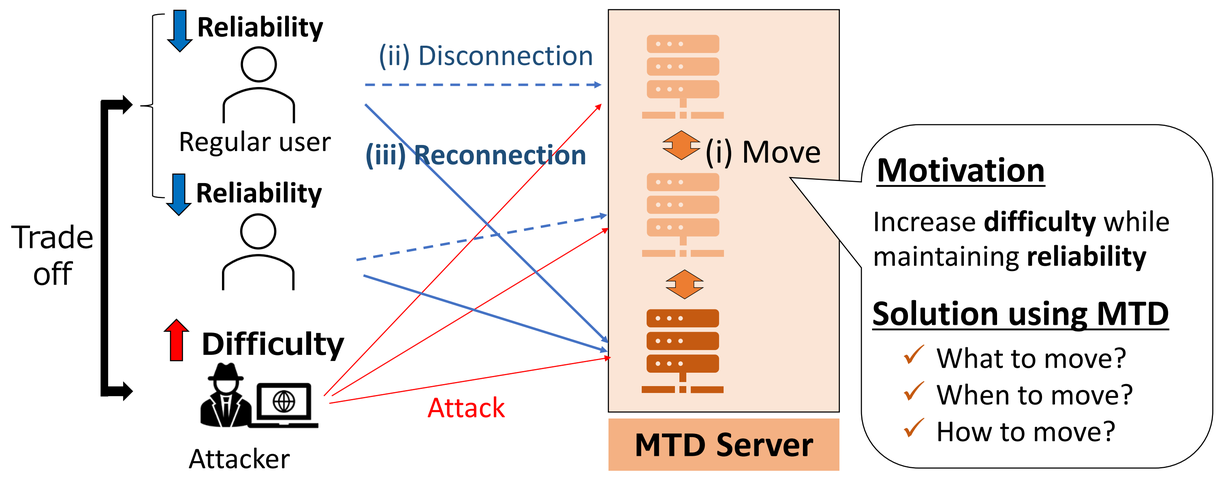
MTD[1]: Attack Surface を変更する手法

- システムの攻撃対象を継続的に変更またはシフトさせることで、攻撃者の攻撃難易度を増加させる
  - ✓ 攻撃者が獲得した情報の無効化
  - ✓ 変更またはシフトさせる対象：IPアドレス, ポート番号, …



従来の防御策 (静的)　　MTDを用いた防御策 (動的)

課題： MTDの実運用時のサービスの利便性



- **Reliability**：正規ユーザーがサービスを利用できる指標として定義
  - ✓ DifficultyとReliabilityはトレードオフの関係
- 実運用を考慮して, Reliabilityに着目したを研究は少ない
  - ➡ MTDの社会実装の課題

目標：Reliabilityを考慮したMTDシステムの設計法の提案

アプローチ: 信頼性を考慮したネットワークレベルのMTD

提案法

1. M/M/c (∞) 待ち行列モデル[2]を用いて，信頼性 Rを定義

λ：到達率　　μ：処理速度

$$\begin{cases} T_{service} = \dfrac{1}{\mu} \\ T_{wait} = \dfrac{1}{\mu}\dfrac{C(a,c)}{c-a} \\ a = \dfrac{\lambda}{\mu} \end{cases}$$

$$R = \frac{T_{service}}{T_{service} + T_{wait}}$$

$T_{service}$: 平均サービス時間

T_{wait}: 平均待ち時間

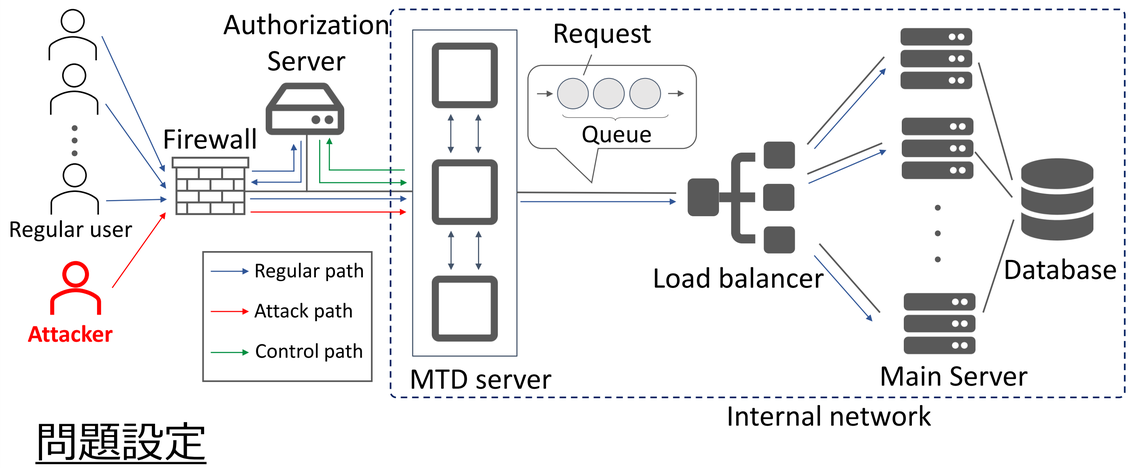
2. Reliability (R) のMTDへの拡張: $(0 \le R \le 1)$

$$R = \frac{\text{サービスを受けた時間}}{\text{総接続時間}} = \frac{T_{service}}{T_{service} + T_{wait} + \text{MTDによる損失}}$$

3. Difficulty[3]を定義: $P_{success}$ $(0 \le P_{success} \le 1)$
   - ✓ $P_{success}$: 攻撃成功確率 (Attack Success Probability)

Reliabilityを維持し、Difficultyが高いシステムの設計法を提案

Webサービスを想定した提案法の評価実験



問題設定

- MTDサーバはアドレス空間 (IPおよびポート) を無作為に変更
  - ✓ ターゲットアドレスは１つ
- 正規ユーザー:
  - ✓ 認証済ユーザー
  - ✓ シャッフリング時に再接続
    - ➢ 再接続時間: T_{loss}
- 攻撃者:
  - ✓ 未認証ユーザー
  - ✓ 脆弱性を知っている
- Reliability (R):

$$\begin{cases} R = \dfrac{T_{service}}{(T_{service}+T_{wait})(1+\alpha)} \\ \alpha = \dfrac{T_{loss}}{T_{interval}} \end{cases}$$

- Difficulty ($P_{success}$):

$$P_{success} = \frac{C_{trial} \times T_{interval}}{N-1}$$

$T_{service}$: 平均サービス時間　　C_{trial} : 攻撃者の接続試行回数
T_{wait}: 平均待ち時間　　$T_{interval}$: シャッフリング間隔
T_{loss}:再接続時間　　N : 有効アドレス数

提案法の評価実験結果

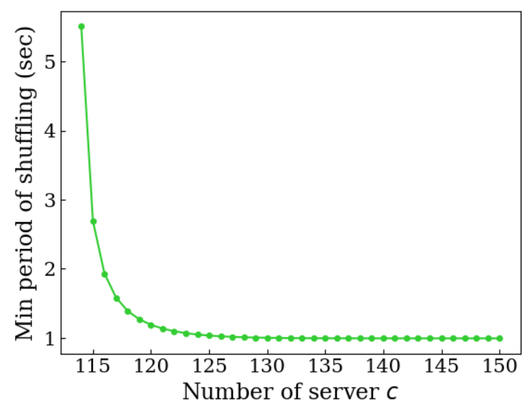
概要

- 信頼性の下限値を設定時にMTDの有効性を評価

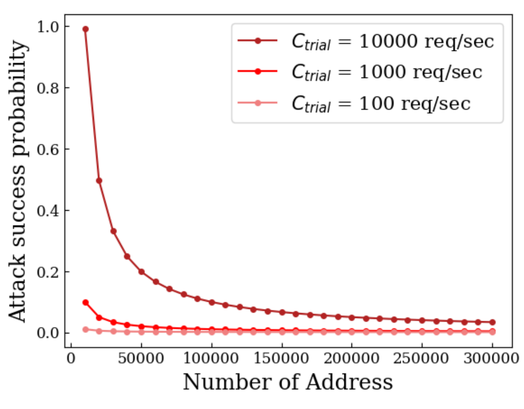
実験条件

- N = 64512
- T_{loss} = 10 ms
- 信頼性の下限値 R_{min} = 0.99

結果・考察



サーバ数と最大シャッフリング間隔の関係



有効アドレス数と攻撃成功確率の関係
(サーバ数 c = 143)

- 信頼性を考慮時, 最大シャッフリング間隔に下限値が存在 (左図)
  - ➡ 提案法により信頼性と攻撃難易度のトレードオフを表現
- 有効アドレス数の増加により攻撃難易度が低下 (右図)
  - ➡ 有効アドレス数の増加により，トレードオフの解消が示唆

結論と今後の課題

まとめ

- 待ち行列モデルを用いて, 信頼性を考慮したMTD手法を提案
- 信頼性を考慮時における有効アドレス数の重要性を示した

今後の展望

- DDoS攻撃を想定した適応的なMTDに対する提案法の拡張
- 第66回ICSS/SPT合同研究会にて口頭発表予定

References

[1] Cho, J. H. *et al,* "Toward proactive, adaptive defense: A survey on moving target defense.“, *IEEE Communications Surveys & Tutorials*, *22*(1), 709-745, 2020.
[2] 塩田茂雄. 待ち行列理論の基礎と応用. 未来へつなぐデジタルシリーズ ; 29. 共立出版, 東京, 2014.
[3] Carroll, T. E. *et al,* “Analysis of Network Address Shuffling as a Moving Target Defense.”, *In 2014 IEEE ICC*, pp. 701-706, 2014.