3.7.2　情報通信セキュリティ研究センター　トレーサブルネットワークグループ

グループリーダー　　米子房伸　ほか４名

ネットワークセキュリティ技術の研究開発

概　要

サイバー攻撃や不正アクセスの発信元からのパケットの推移を解明する時間軸方向の追跡を行う技術などのトレーサブルネットワーク技術の開発を実施する。また、このトレーサブルネットワーク技術の評価のため再現ネットワーク技術の研究開発を実施する。さらに、サイバー攻撃等による不正・異常なパケットの存在下においても一定の通信性能を確保する通信方式としてセキュアオーバーレイ技術の開発を実施する。

従来のIPトレースバック技術の高速化・実用化についてはNICT委託研究の成果を前提としつつ、2010年のバックボーンで用いられるネットワークを対象として、各種解析処理手法を応用した新たなアプローチによる飛躍的精度向上と高速化を目指す。時間軸方向のトレースバックに取り組むため再現テストベッド技術を核として理論的アプローチとシステム的アプローチを融合し、発信元からのパケットの推移を時間軸に沿ってトレースバックする技術の開発を行う。

平成20年度の成果

⑴　時系列を含む多次元、多様性に対応できる発信元追跡技術の研究開発

グランドチャレンジとなる研究目標を設定し、プロジェクト終了時に実用性をもたらす研究開発を推進した。これにより、基本問題への帰着と方式研究の推進を継続した。

①　多次元、多様性に対応できる発信元追跡

サポートベクタマシンは多次元、多様性を取り扱うのに適しているが、従来手法では多クラスの分類問題に対し適用できないという制約があった。このためサポートベクタマシンを理論的に拡張する方法の応用研究を実施した。これに関連して異常値検出と分類アルゴリズムに関する研究を開始した。

②　誤検知率の改善方式の探索

既存の機械学習アルゴリズム単体では誤検知率が10％程度となる場合が多い。このため識別器に複合法を用いて誤検知率を低減させる手法の研究を継続した。

③　秘匿計算プロトコルの基礎理論及び実装

本プロジェクトでは通信の秘密が実用上の大きな課題となっている。このため、通信の秘密を確保しつつ発信元追跡を行うための暗号プロトコルの開発に取り組み、準同型暗号技術を応用した秘匿共通集合計算システムの研究を継続し､秘匿計算プロトコルに係る計算を従来方式に比較して100倍以上高速化できる新たなアルゴリズムを考案し、実装・評価試験によりその有効性を確認した。

⑵　発信元からのパケット解明技術の研究開発

不正・異常なパケットはますます先鋭化・多様化しており、パケットの捕捉能力と解析能力の向上が急務である。このため以下の研究開発を行った。

①　暗号化ネットワーク上のマルウェア捕捉機構

Winny等のPeer-to-peer型ネットワークにおいて拡散しているマルウェアを捕捉するシステムの研究開発を行い、当該システムをインターネットへ設置する実験を実施中である。

②　プライバシ確保型発信元追跡

プライバシを確保しつつ発信元追跡を行うため、準同型暗号を応用した秘匿共通集合計算プロトコルのシステム化、ソフトウェアの公開を行った。これにより同技術を応用してスピア型攻撃を判定することが可能となった｡また前年度より開発を続けている仮想マシンを用いた追跡技術と組み合わせることで､P2Pネットワークにおける情報漏洩を追跡する方式の研究に着手した。

⑶　再現ネットワーク技術の研究開発

脅威への対応手法を検証するため、攻撃再現環境、不正アクセス再現環境を構築する技術を確立する研究を継続した。また本技術の精度・実用性評価のため再現ネットワーク技術の研究開発を継続して行った。

①　インシデント再現方式の検討

プロセッサ仮想化技術によるインシデント再現方式のプロトタイプ実装を行い、実際の脆弱性に対して観測された未知の攻撃ベクタを用いてインシデントの再現法の研究を継続した。

② 再現実験環境を応用した実験システムの研究開発

プロトタイプ実装に半自動の再現・解析機能を付加し、これを用いて検証実験を実施した。また、プロセッサ仮想化技術と実ノードの組合せによるハイブリッド型の再現環境の構築を行った。

③ マルウェア再現技術

昨年度までのプロトタイプに自動構築機能の強化を行い、マルウェアの再現によって得たメモリダンプやパケットダンプなどのデータセットを研究グループ内向けに試験的に配布を開始した。さらに、教育分野への応用として、実際にマルウェアの解析演習に利用した。これらの技術を踏まえ、マルウェアを含む小規模攻撃再現テストベッドのプロトタイプの開発を行った。

④ 発信源追跡のための再現ネットワーク技術

インターネットの主要な要素であるAS間ネットワークを模倣する模倣AS間ネットワークの構成技術に関しては、大規模な再現・検証に必要となるインターネットの模倣技術として、インターネットの中核部分であるAS間ネットワークの模倣環境について、仮想化技術を用いた多重化による大規模化を行った。実際のAS間ネットワークの規模の 3 分の 1 に相当する10,000ASからなる模倣AS間ネットワークの構築に成功するとともに、その安定性を実運用環境への挿入実験で確認した。

⑤ 外部からの検体入手・解析

協力関係にある複数の大学の事案対策チームから検体を入手し、実際に再現テストベッドにおいてインシデントを再現・解析し、多くの検体については応用実験システムで解析実験を継続して実施した。

⑷ セキュアオーバーレイ技術の研究開発

サイバー攻撃状況下においても通信性能の劣化を抑えるため、セキュアオーバーレイの研究開発に取り組んだ。

① セキュアオーバーレイネットワーク技術については、実証システムを用いた評価を行った。10万ノード規模での長時間耐久試験を行い、同技術の実用化にあたって問題となっていたマルチコアプロセッサでの並行制御の問題や、ノード大量離脱時の安定性について問題解決を行った。

② アプリケーションサービス事業者との契約を締結し、開発成果の技術移転を行った。