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　安井哲也　ほか7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19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実施することができた。

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に着手した。

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ことができないか探索を行い、DARPA データセットにおいて検知率を改善できることを確認した。

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を実用化した。また、本システムのスピア型サイバー攻撃に対する有効性を検証するため、実証実験を行った。

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　仮想マシン技術を応用したデータ捕捉機構

仮想マシンモニタを改良し、不正アクセス発生時点のメモリ、ディスク内容を捕捉することが可能となった。またメモリ内容を自動分類し、高い精度でメモリ内の攻撃ベクタを捕捉できる機械学習アルゴリズムを開発した。

②　暗号化ネットワーク上のマルウェア捕捉機構

当グループで開発した、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を、インターネットへ設置する実験を開始した。本システムにより、暗号化されたファイル交換ネットワーク等で拡散している、従来検出することが難しかったマルウェアを捕捉し解析に供することができる。

③　ハードウェアによる高速化

高速ネットワークへの対応及びサイバー攻撃解明時間の短縮のため、機械学習アルゴリズムや秘匿計算プロトコルをハードウェアにより高速化する必要がある。平成19年度はハイレベル論理合成技術の有効性を確認するため、ストリーム計算アルゴリズムをハードウェア上に実装した。

(3)　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。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が再現できることを確認した。

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検討を行った。

③　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を検討し、プロトタイプ実装を行った。

④　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・解析できることを確認し、多くの検体については応用実験システムで解析実験を実施した。また､特定のアプリケーションソフトウェアの脆弱性を攻撃する検体の再現について検討を行った。

(4)　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　認証システムにおける単一障害点の解消

従来型の認証基盤では認証局が集中型となっており、単一障害点となっている。そこでセキュアオーバーレイ上に従来とは異なる形式の認証基盤を実装した。これにより、認証局が単一障害点となることを解消した。

②　機能目標の達成

上記①と、トークンを用いて認証を行うことにより、なりすまし攻撃等によるインフラの破壊に対して頑健なセキュアオーバーレイが構成できた。

③　実証システムの構築

性能評価及び機能評価のため、サイバー攻撃下において電気通信事業者間の連携を支援するシステムをセキュアオーバーレイネットワーク上に構築している。