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 13 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している。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している。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している。

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、平成 22 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している。また、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っている。

平成 21 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（短期的な問題解決はもとより、長期的な視野で抜本的な技術革新等の実現を目指す研究開発・技術開発）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て実施した。

①多次元、多様性に対応できる発信元追跡のための異常値検出

異常値検出方法として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継続して実施した。

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

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（2 つの暗号文 Enc（m1）、Enc（m2）が与えられた時に、平文や秘密鍵なしで Enc（m1 ○ m2）を計算できる性質を有する。ここで○は、加法＋や乗法×のような二項演算子）技術を応用した秘匿共通集合計算（2 人のユーザがそれぞれ秘密の集合を保持しており、お互いにその情報を漏らすことなく、それらの共通集合のみを得る）システムの研究を実施している。平成 21 年度は、プライバシー確保については、準同型暗号を応用した秘匿共通集合計算プロトコルに適用可能な高速演算アルゴリズムを開発した。その要素技術である紛失通信プロトコル（送信者が送信したデータのうち、受信者がどれを受信したのか、送信者が知ることができないようなプロトコル）について、従来方式と比べて、その数学的制約を大幅に緩和（Computational Diffie - Hellman 問題を解く効率的なアルゴリズムが存在しないという仮定を用いない）することに成功した。この成果の学術的価値は高く、世界最高峰の国際会議の 1 つである Asiacrypt2009 に採録された。

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（P2P）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の一環として、マルウェア捕捉のためのシステムを開発し、同システムをインターネットへ接続し

た捕捉実験を継続した。

②プライバシー確保型発信元追跡

プライバシーを確保しつつ発信元追跡を行うため、秘匿計算プロトコルの基礎理論を応用し準同型暗号を用いた秘匿共通集合計算プロトコルのシステム化及び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特定の企業や個人狙った攻撃であるか否かをお互いにその情報を漏らすことなく判定することが可能となった。また平成 20 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を実施した。その研究の一環として、P2P ネットワークにおける情報漏洩経路の可視化方式の研究開発を実施した。

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て行った。

②マルウェア再現技術

- 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当機構外の研究協力機関への試験配布を継続した。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。
- 再現ネットワークによる小規模攻撃再現に関しては、平成 20 年度に開発した小規模攻撃再現テストベッドに、再現からデータセット生成までの自動化とデータ蓄積が可能な逐次解析機能を開発し、マルウェアを含む小規模攻撃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、NICT 外部の連携機関へ試験的に配布を開始した。
- 外部から安全に利用可能なインタフェースを開発し、NICT 外部の連携機関にテストベッドとして試験公開した。同時に、教育分野への応用として、実際にマルウェア感染、標的型攻撃、情報漏洩、Web2.0 セキュリティなどの様々な事案を再現し、解析演習に利用した。
- 情報共有のための検体情報、解析環境情報、解析結果情報のスキーマのプロトタイプを定義し、スキーマに基づいて解析結果情報を生成可能とした。これにより、NICT 外部の研究機関からの再現・解析エンジンの受け入れと、再現結果の提供などの連携が可能となり、平成 22 年度以降に幾つかの学会等で正式なデータセットとして採用が予定されている。

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（自律システム）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・検証環境が必要である。そのため AS 間ネットワークの模倣環境を仮想化技術による多重化により大規模化を行なった。実際の AS 間ネットワーク規模の 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共に、その安定性を実運用環境での挿入実験で確認した。
- 模倣 AS 間ネットワークの構築までの時間短縮や安定性向上を図るための仮想環境への割り当て方式の高度化を行うと共に、AS 内部のネットワークを模倣するための OSPF 網の模倣や中核サービスである DNS を模倣する擬似 DNS 機構などにより、より現実的な規模や複雑さとサービスを備え持つ、インターネットに近い再現実験環境を提供することが可能となった。

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・解析し、多くの検体については応用実験システムにおいて、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

オーバーレイネットワーク（あるコンピュータネットワークの上に構築された別のコンピュータネットワーク）技術を用いることにより、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セキュアオーバーレイ技術の研究開発では、アプリケーションサービス事業者との間で契約締結している技術開発に関する成果の技術移転を継続した。