3.6.2　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　　高橋幸雄　ほか 10 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た。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た。

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た。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た。

【平成 22 年度の成果】

(1)　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）となる目標を設定し、実用性をもたらす研究開発と、基本問題へ帰着する方式研究を実施した。

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

攻撃識別、異常状態検知機能を有する、ネットワーク監視と解析システムに関する研究を行った｡「分割統治法」に基づいたアンサンブル分類器と進化的コンピューティングの実装により、ネットワーク攻撃の高速検出を実現し､方式の正当性と有効性の向上を実証した。国際学会のワークショップを共催することにより、機械学習理論とセキュリティに関連した新たな学際領域を立ち上げた。

②　誤検知率の改善方式の探索

誤検知率改善のため識別器に複合法を用いる手法の研究を継続した。さらに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、ディスクの内容を捕捉可能とすることにより、メモリ内容を自動分析し、99%以上の確率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である。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として、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た。平成 22 年度は、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の開発を継続した。

(2)　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に開発したシステムを用いた捕捉実験を継続した。

②　情報漏えい経路追跡方式

平成 20 年度より開発を続けている仮想マシンを用いた P2P ネットワークにおける情報漏えいを追跡する方式の研究の一環として、情報漏えい経路の可視化方式のためのデータベースの構築を行った。

(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 NICT 外部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継続した。

・ トレーサブルネットワーク運用の各プロセスにおける情報の構造化を行い、運用者の連携･工程間分業の効率化を図る研究の一環として、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おいて、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の、NICT 外部の連携機関への試験的な配布を継続した。

・ 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、解析演習への利用を継続した。

・ 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（情報の構造を定義するための記述）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、幾つかの学会等で正式なデータセットとして採用された。

③ 発信源追跡のための再現ネットワーク技術

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 のサービス網を模倣する模倣 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。また、標的型攻撃に対応するために擬似インターネットを容易にカスタマイズ可能とするインタフェースを開発した。

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て、解析実験を継続して実施した。

(4) 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）技術を利用した、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技術の研究では、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。

(5) Web サイトにおける詐称対策技術

フィッシングサイトの収集・再現・分析の観点から研究を行った。Web サイトの難読化に対応するためブラウザを制御するクローラを用いた収集技術を駆使し、収集されたコンテンツをひとつのサイトとして再現する技術を開発した。また、人間の過去の判断履歴を活用し、フィッシングサイトの検知精度を高める分析方式を提案した。被験者実験により、有用な判断履歴を持つユーザに見られる意思決定の過程の分析を実施した。

(6) サイバーセキュリティ情報交換技術の研究と国際標準化活動

組織間でサイバーセキュリティ情報の交換を実現すべく、情報をコンピュータ上で扱うためのセキュリティの情報オントロジを構築した。本オントロジは、サイバーセキュリティオペレーションの観点から必要なオペレーションドメイン、エンティティ、情報をモデル化しているため、交換すべき情報とその情報の利用形態を抽象化し共通化できる。本オントロジに従ったセキュリティ情報を特定･交換するディスカバリー技術のテスト実装を実現した。上記成果を ITU-T SG17 の Question 4 に入力し、X.1500 の制定に貢献すると共に、本コミュニティの成果の発展に主導的な役割を果たした。