3.4.2　ネットワークセキュリティ研究所　セキュリティアーキテクチャ研究室

室長　　松尾真一郎　ほか 10 名

利用形態に応じた過不足のないセキュリティ技術の研究

【概　要】

クラウドやモバイル等の先進的なネットワーク及びネットワークサービスにおいて適材適所にセキュリティ技術を自動選択し最適に構成するためのセキュリティアーキテクチャの研究開発として、過不足のないセキュリティ技術を判断するための、「セキュリティ知識ベース」、「分析エンジン」の構築に着手するとともに、個別のネットワーク利用方法におけるセキュリティ上のリスクをモバイル端末に表示する Risk Visualizer を構築した。また、RFID のような省リソースデバイス、モバイル端末、クラウドを統合したサービスにおける認証・プライバシ保護を効率的に行うためのセキュアプロトコルの確立を行った。また、暗号プロトコルの安全性評価に関する知見を、電子政府推奨暗号の安全性評価を行う CRYPTREC 活動を通じてドキュメント化し、社会還元を行った。

【平成 23 年度の成果】

（1）ユーザのセキュリティリスクを可視化する“Risk Visualizer”

セキュリティ技術に関する十分な知識を持たない一般的な IT 端末ユーザに対し、あるネットワークサービスを利用する際にユーザが直面しているリスクを、iOS や Android が動作するモバイル端末上で可視化するシステムの構築を行った。現プロトタイプでは、5 万レコードの脆弱性 DB などを用い、ネットワーク利用時の潜在的リスクをタブレット上で可視化することが可能である。

図 1　Risk Visualizer プロトタイプ

（2）セキュリティ知識ベース構築技術

ネットワーク利用におけるリスクの可視化、利用方法に応じて過不足のないセキュリティ技術の導出にあたっては、ネットワーク上のリスクやセキュリティ対策技術などの情報が蓄積された、セキュリティ知識ベースが必要である。平成 23 年度は、セキュリティ知識ベースの基本的な構造の検討を行うとともに、ネットワーク上に存在する様々なセキュリティ情報をお互いにリンクし、検索可能にすることにより、インターネットを巨大なセキュリティ知識ベースとする”Discovery”技術を構築した。本技術は、ITU-T 勧告 X.1570 として標準化を果たしており、我々は、本勧告に基づく実装にも着手し、そのプロトタイプ（図 2）を構築した。セキュリティ知識ベースは上述の Risk Visualizer がリスクを判定する際に参照される。但し、既存のセキュリティ情報だけではリスクを効率的に判定するには不十分であると考えており、次年度以降セキュリティ知識ベースを拡張すべく、その要求条件を定義した。

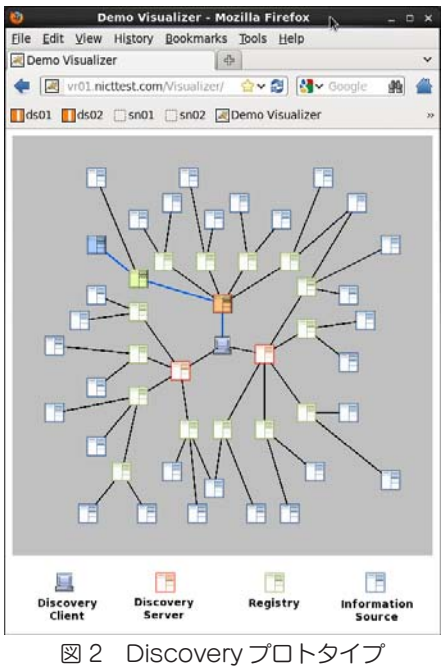

図 2　Discovery プロトタイプ

（3）情報交換の自動化を促進する“CYBEX” / “IODEF extension”

セキュリティにおけるインシデント発生時の情報交換を自動化し、オペレーションの自動化を補助する技術として、セキュリティ情報交換フレームワーク “CYBEX” 及び、インシデント情報を記述するフォーマット “IODEF extension” を構築した。前者については ITU-T 勧告 X.1500 として規格化を終了しており、後者については、IETF にて規格化を図っており、既にワーキンググループドラフトとして受理され、更なる発展が求められている状況である。

(4) 省リソースデバイス向けプライバシ保護プロトコルの確立

今後の大規模ネットワークの需要を踏まえ、様々な利用用途に対してそれぞれのシーンに対応できる安心・安全を提供できる技術の確立を目指し活動を進めた。

従来のネットワークの利用シーンと大きく異なる点の１つとして、携帯電話やスマートフォンなどの省リソースデバイスが通信に多用され、その需要が今後も拡大し続けることが予想される。そのため、省リソースデバイスの利用を想定したうえでの安全な通信の確立が重要となる。一方で、省リソースデバイスに対しては、従来の PC などを想定した安全性を守るための暗号プロトコルなどの適用が困難な場合が多い。そのため、省リソースデバイスの利用を想定する場合は、従来とは異なる様々な制約条件を前提とする必要がある。例えば、利用可能な消費電力が小さい、物理的デバイスの形状が小さい、基本的に無線による通信である、デバイス自体の位置情報が変化する、などが挙げられる。本研究室では、この課題に対し、現実的な 2 種類のプライバシ定義に対応した省リソースデバイス向けのセキュリティモデルを確立するとともに、RFID タグの認証について、ブロック暗号のみをベースとした提案プロトコルについて実装評価を行い、性能面での有効性を確認した。また RFID タグのような省リソースデバイスを対象としたセキュリティモデルや安全性の捉え方について、米国 NIST や欧州の今後の技術戦略を議論する会議で提案を行った。また、これらの提案に基づく、省リソースデバイスからクラウドまでを統合した統一的セキュリティモデルの研究を、コロンビア大学と開始した。

(5) クラウド向けプライバシ保護プロトコルの確立

大規模ネットワークの利用用途の拡大に伴い、特にプライバシを保護する技術は、今後ますますその重要性が増す。それぞれのユーザが、異なる立場で異なる要求条件を持ちネットワークで通信を行う。さらには、異なるサービスを異なる利用用途･目的を持って利用する。従来のプライバシ保護のための仕組みは、サービス固有のプライバシ保護の要求条件にあわせて個別に設計されていた。しかし、プライバシ保護における異なる要求条件を持った複数のサービスが大規模ネットワーク上で連携することを考えると、ネットワーク上の不正行為を防ぎ、さらにはそれぞれの目的に応じて守るべきプライバシ情報を保護できるような共通の仕組みを構築することが重要である。本研究室では、異なるユーザが異なる目的の下で通信を行うシーンに対してフレキシブルに個々のプライバシ情報を保護することができる仕組みの基盤となる署名方式を提案した。

さらに大規模ネットワーク上では様々なプロトコルが存在し、必ずしも共通の設定条件に基づき構成されているとは限らない。ある利用用途を目的とし、異なる設定条件に基づく 2 つのプロトコルを組み合わせることは一般的には難しく、利用用途に沿ったプロトコルを新たに設けざるを得なかった。そこで本研究室では、特に需要の高い署名方式について、異なる設定条件に基づくプロトコル間で、異なる設定条件の一方（合成数に基づく方式）をもう一方の設定条件（素数に基づく方式）に変換し、異なるプロトコルを組み合わせて利用することを可能とする技術を提案した。

また、プライバシを保護しながら、クラウドなどで情報処理を行う技術として、ネットワーク上のユーザが秘密に保有する集合データの和集合、および積集合を、データ自身は秘匿しながら計算する効率的な方式を確立した。上記の方式は、それぞれ実装評価を行い、現実的なアプリケーションにおいて十分な性能を有することを確認した。

(6) 暗号プロトコルの安全性評価と社会貢献

電子政府向けの推奨暗号技術の推奨を提示する総務省と経済産業省のプロジェクトである CRYPTREC では、暗号化や電子署名のような単機能の技術である暗号アルゴリズムだけでなく、暗号アルゴリズムと通信を組み合わせて、認証などの高度なセキュリティ機能を提供する暗号プロトコルについての推奨についても、「リストガイド」というドキュメントで提示している。このリストガイドの作成にあたり、セキュリティアーキテクチャ研究室で実施している暗号プロトコルの安全性に関する検証の知見を標準的に利用されているセキュアプロトコルである SSL/TLS や DNSSEC における暗号利用方法に適用し、「CRYPTREC リストガイド 2011」を作成し、安心・安全な電子政府の利用方法に関する情報の社会還元を行った。また、この分野で必要とされている将来的な研究テーマの実施にも着手している。セキュリティポリシーの異なる複数のシステムを利用した際の適正なセキュリティ確保、およびクラウド機器や、モバイル機器や省リソースデバイスなど性質の異なるデバイスやシステムを統合して構築する大規模システムにおけるセキュリティ基盤は、国民が安心してネットワークを利用する上で必要だが、これまで世界的にも研究されていない。この分野は、中立な組織において研究する必要があり、組み合わせによって生じるセキュリティ課題を統一的に解決する理論および手法を確立することは、社会的にも、技術的にもの大きな意義のある活動である。