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 8 名

過不足のないセキュリティのためのリスク提示と、大規模ネットワークにおける認証・プライバシ保護の実現

【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、ネットワーク利用者が現在利用しているセキュリティ対策技術の有効性と残存リスクを認知するためのシステム REGISTA（Risk Evaluation and Guidance on Information Security Technology Application）の構築を行い、企業ネットワークへのリモートアクセスにおけるリスク評価の可視化を行った。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と実装を行った。さらに、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 24 年度の成果】

（1）ユーザのセキュリティリスクを、安全性理論に基づき分析し可視化する REGISTA の構築

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分析し、利用者端末にその分析結果と推奨される対策技術を提示するシステム REGISTA の構築を行い、その有効性の実証を行った。

REGISTA は、ネットワーク利用者が必要とするセキュリティの要求と、利用しているネットワークに存在する脆弱性（セキュリティ攻撃が発生する場所）の情報を入力として、REGISTA 内のセキュリティ知識ベース（ネットワーク機器の脆弱性に関する情報、セキュリティ対策技術の有効性に関する情報）をもとに、個別のネットワーク利用に潜むリスクを提示する。また、セキュリティ知識ベースには、リスクが少ないことが理論的に確認されているセキュリティ技術の組み合わせをホワイトリストとして保持しており、その結果を出力することで、リスクを軽減できる対策を提示する（図 1）。

平成 24 年度は、NICT のテストベッドである StarBED[3] 上に REGISTA システムと、仮想的な企業ネットワークを構築し、企業ネットワークへのリモートアクセスによって企業内の機密情報にアクセスする際の、ネットワーク上のリスクを提示するシステムの実証を行った。

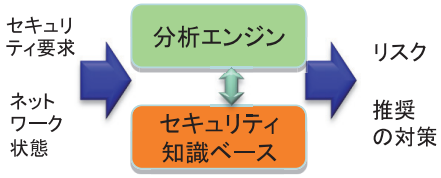

図 1　REGISTA の概要

（2）セキュリティ分析エンジンの構築

REGISTA におけるリスク分析では、理論的に網羅性を持ったセキュリティ分析が必要である。そのために、脆弱性情報に基づく分析だけでなく、暗号プロトコル評価などで利用される形式化手法を加味し、REGISTA の中に組み込んだ。また、企業ネットワークなどのリスク分析では、ネットワークから取得する情報を秘匿したまま分析を行う必要がある。そこで、マルチパーティ計算の手法を利用し、情報を秘匿しながら脅威分析を行う実証を行い、現実的な時間内で分析が可能であることを示した。

（3）セキュリティ知識ベース構築技術

REGISTA のセキュリティ知識ベースの核の 1 つは、個々のネットワーク機器上のソフトウェアなどに、攻撃の可能性となる脆弱性の有無についての情報を集約することである。これらの情報は、世界的に分散され、非同期にアップデートされる。そのため、世界的に分散された情報をリアルタイムで情報交換し、集約するための仕組みが必要である。平成 24 年度は、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”技術を実装した。また、この仕組みについての標準化として、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、その標準化をほぼ完了している状況である。

（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・安全を提供す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。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、NICT の研究成果である RFID 向けのプライバシ保護機能付き認証プロトコルについて、実際の１チップパッシブ RFID タグに搭載するための実装実験を実施している。また、暗号回路を使わずに「チップの指紋」と呼ばれる物理的性質を利用して認証を行う方式 PUF（物理的複製困難関数）について、世界で初めて物理デバイスを用いて評価を行った（図 2）。

図２　PUF 安全性評価システム

さらに、近年セキュリティ・プライバシ問題が発生しているスマートフォンアプリについて、5,000 アプリをサンプリングし、アプリケーションのセキュリティ上の問題を解析した。

（5）大規模ネットワーク向け認証プロトコル、クラウド向けプライバシ保護プロトコルの確立

新世代ネットワークにおいては、ネットワークに接続されるデバイスの数が 10 兆個（100 億人 ×1,000 デバイス）を想定しており、この規模のネットワークを効率的にカバーできる認証やプライバシ保護のための基盤は存在しない。そこで、デバイス数が大規模になってもスケーラビリティを確保できる認証方式 Revocable IBE/IBS を確立し、性能上の実証を行った。この方式は、サーバで管理すべき情報が、デバイス数の log オーダーとなることが特長である。その上で、この方式のスケーラビリティの面での有効性を、StarBED[3] において実証した。

また、クラウドに保管され、クラウド間を流通する情報のプライバシ保護に関する技術は、今後ますますその重要性が増す。特にクラウドにおいては、それぞれのユーザが、異なる立場・要求条件を持ち、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。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、その実装と墨塗り署名方式としての実証を行った。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及び積集合を、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、SNS におけるプライバシ保護など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

一般的に利用されているセキュリティ技術は、暗号技術と通信を応用した暗号プロトコルとして設計されている。そのため、個別の暗号プロトコルの安全性が正しく評価されている必要がある。暗号プロトコルの安全性評価で重要な点は、内部で利用している暗号技術が安全でも組み合わせ方によっては、脆弱性が発生することにある。そこで当研究室では、REGISTA の分析で利用することも想定し、標準的な暗号プロトコルに対する評価を実施した。ISO/IEC で標準化されているエンティティ認証プロトコル ISO/IEC 9798 について、プロトコル上の脆弱性を発見し、その修正案を ISO/IEC に提案し、問題点の修正を行った。その成果を電子政府向けの推奨暗号技術の推奨を提示する CRYPTREC でのエンティティ認証の選考に適用した。また、暗号プロトコル評価の知見を、CRYPTREC で発行する「リストガイド」と呼ばれるドキュメントで提示した。インターネットで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 IPSec における暗号利用方法にプロトコル安全性評価の知見を適用し、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。さらに、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、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、技術的にも大きな意義のある活動である。