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およ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に加え、喫緊の課題であるスマートフォンアプリケーションに内在するリスクの可視化を行った。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して、国際的な協力のもと評価技術に関する議論、知識共有、公表を行うコンソーシアムを設立するとともに、暗号プロトコル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 25 年度の成果】

(1)　ユーザのセキュリティリスク評価プラットフォーム REGISTA の開発

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 について、エンタープライズ (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を行った。

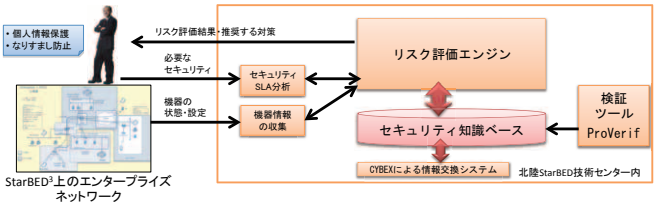

図 1　REGISTA によるリスク評価

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) を元に、個別のネットワーク利用に潜むリスクを提示する (図 1)。セキュリティ知識ベースは、形式的評価理論を実装した ProVerif を元に構築されるほか、ITU-T において標準化された情報交換の共通プロトコルである CYBEX を利用して、NIST などの海外の研究機関から取得する。

平成 25 年度は、NICT のテストベッドである StarBED 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。また、この実証システムを Interop Tokyo 2013 に出展した。

(2)　REGISTA のスマートフォン対応

近年スマートフォンアプリケーションから、意図しない情報の漏えいが発生するなど、セキュリティ・プライバシ上のリスクを含んだアプリケーションが多数流通している。そのため、既存の Android アプリケーションのファイルを解析して、このようなリスクの存在に関する情報を REGISTA のセキュリティ知識ベースに追加し、ユーザ向けの Android エージェントアプリケーションから自分が所有するスマートフォンにインストールしているアプリケーションのリスク情報を即座に把握できる機能を REGISTA に追加した。この機能により、スマートフォンユーザはアプリケーションを利用

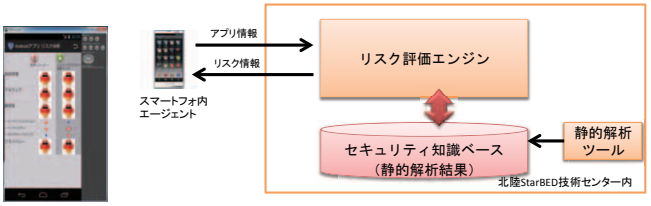

図 2　スマートフォンにおけるリスク可視化

することによる情報漏えい等のリスクを把握することが可能になるとともに、同じ機能を持つ複数のアプリケーションを比較して、よりリスクの低いアプリケーションを選択できるようにするなど、利用者にとってのリスク低減方法をガイドすることが可能となった。

(3) クラウドにおける認証・プライバシ保護プロトコルの設計

近年、個人のスマートフォン、タブレット、パソコンの情報、および企業システムの情報が、クラウドサーバ上に保存されたり、クラウド間を流通したりするようになってきている。また、SNS などではこれらの情報が活用され様々なサービスが行われている。このような状況において、クラウド上を流通する情報について、不必要なマッチングによるプライバシ漏えいや、クラウド管理者の不正による情報漏えいを防止する必要がある。この問題に対応するために、以下の暗号プロトコルの設計を行い、安全性の証明を行った。

- 匿名認証と部分秘匿認証を同時に行える認証方式（墨塗り認証）
  文書作成者の電子署名を付与したまま、オリジナルの文書を墨塗りしても原本性の証明と、匿名性の確保が可能となる方式。
- 秘匿集合演算方式（秘匿情報処理）
  クラウド上にある情報から、和集合や積集合を、情報を秘匿したまま計算することができるプロトコル。クラウド上の情報を暗号化したまま、共通の趣味を持つユーザなどを探すことが可能となり、SNS におけるプライバシ保護が可能となる。
- インデックスサイズを 1/7 に削減した検索可能暗号方式
  サーバ上の情報を暗号化したまま、情報の検索が可能となる方式においては、従来プライバシ保護の実現のために巨大なインデックスデータベースが必要であったが、そのデータベースサイズを 1/7 に削減することに成功し、情報を秘匿したままでのビッグデータ解析が可能となる。

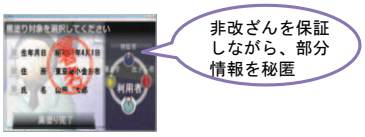

図３　墨塗り認証方式

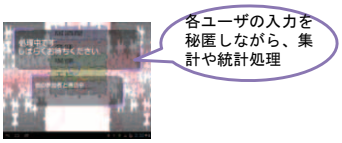

図４　秘匿集合演算

(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設計と評価

今後、センサーネットワークなどの普及により、RFID タグのようなメモリや計算能力が低い「省リソースデバイス」が様々な場所で利用されることが見込まれている。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。この課題に対し、RFID タグにおけるプライバシ保護の安全性基準を提案するとともに、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、実際の 1 チップ RFID タグにおいて、物理回路も含めて実装可能であることを実証した。

(5) 暗号プロトコルの安全性評価と国際的協力体制の確立

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 11770-2,3 について、プロトコル上の脆弱性とその修正案を ISO/IEC に提案し、問題点の修正を行った。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。

さらに、暗号プロトコルについては、近年数多くの脆弱性が発見されており、安全性評価を行うための技術、および脆弱性情報について迅速に議論し、社会にその議論結果を還元していくことが求められている。また、この議論は、多面的な評価を取り入れる必要があり国際標準化活動への反映を考えると、国際的である必要がある。そこで、NICT を始めとして、日本のみならず、英国、スイス、フランス、エストニア、米国の研究機関を含めた国際的なコンソーシアム「暗号プロトコル評価技術コンソーシアム」（英文名：Cryptographic protocol Evaluation for Long-Lived Outstanding Security （CELLOS））を立ち上げ、SSL/TLS など広く使われている標準的な暗号プロトコルに関する安全性情報の議論とレポートの公表を開始した。

図５　CELLOS コンソーシアム