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（事務取扱）　　平　和昌　ほか５名

ネットワークの安全性を最適にする技術を構築し、将来のネットワークにおける安全性の確保に貢献

【概　要】

本研究室では、進化が著しいネットワークの安全性を最適に確立するための、リスク評価、認証・プライバシー保護、その安全性評価のための技術を構築し、将来のネットワークにおけるセキュリティ確保の実現に貢献することを目指しており、今年度は以下の３つの研究テーマを中心に研究開発を行った。

（1）リスク分析スマートフォン向けリスク評価技術

現在、スマートフォン等で普及が進んでいる Android 端末で用いられるアプリケーションについて、個々のアプリケーション利用におけるリスクを分析する技術の開発、約 10 万件のアプリケーションに対する分析結果を蓄積した知識ベースの構築、ネットワークサービスの提供者とユーザの間でのセキュリティレベルを合意する技術などを研究開発

（2）省リソースデバイス向け認証・プライバシー保護技術

IoT 時代における大規模ネットワーク上で多種多様の利用が想定される「RFID タグ」を省リソースデバイスの対象として、認証とプライバシー保護の両立に向けたセキュリティ技術などを研究開発

（3）理論的に網羅性をもった安全性評価技術

ネットワークを利用した通信の安全を保つ目的から、暗号を利用する通信の手順を規定した「暗号プロトコル」について、理論的に網羅性をもった安全性評価技術を研究開発するとともに、代表的な暗号プロトコルの安全性情報を発信

【平成 26 年度の成果】

（1）リスク分析スマートフォン向けリスク評価技術

ネットワークを用いたサービスを一般ユーザが利用する際、当該サービスの利用によりユーザが直面するリスクを分析し、ユーザの端末にその分析結果及び推奨される対策方法を提示するシステムの構築を行っている。今年度は、ネットワークサービスの対象を Android のアプリケーション（Android アプリ）とし、個別の Android アプリが有するリスクの定量評価手法を提案し実装した（図 1）。本手法の特徴は、Web から取得したそれぞれの Android アプリに対する情報を活用してリスクを判定している点にある。本システムは、これまで検討してきたリスク分析フレームワークと同様、個別のセキュリティ情報を蓄積している「セキュリティ知識ベース」を活用する。今年度は約 10 万件の Android アプリの分析結果及びメタ情報をセキュリティ知識ベースに蓄積した。

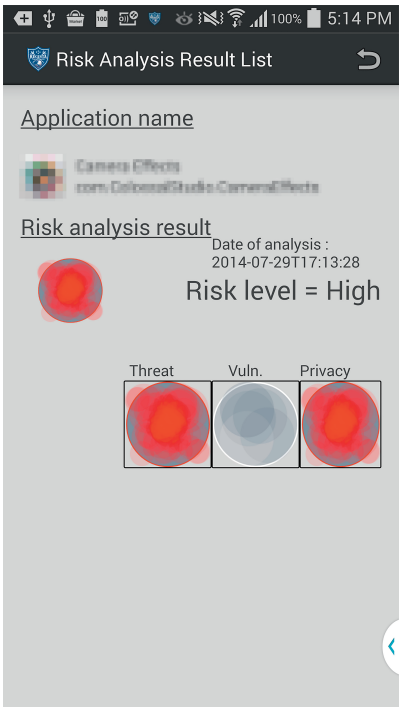

図 1　Android アプリに対するリスク分析結果の例

各組織で得られたリスク分析結果など、組織間で何らかのセキュリティ情報を交換する際、その情報構造を合意しておく必要がある。これまで当研究室では、IETF（The Internet Engineering Task Force）において、セキュリティ情報に対する構造の国際標準化を先導し、本年度に RFC 7203 として発行されることが決まった。

各組織によりリスクの判断基準が異なることから、基準となるセキュリティ要件を定義する研究をタンペレ工科大学（フィンランド）と共同で実施した。本年度は、昨年度までに実施してきたセキュリティ SLA（Service Level Agreement サービスレベル合意書）の構築技術全体をまとめた。

(2)　省リソースデバイス向け認証・プライバシー保護技術

IoT 時代における大規模ネットワーク上で多種多様の利用が想定される「RFID タグ」を省リソースデバイスの対象として、RFID タグの利用における認証・プライバシー保護技術の研究開発を実施している。本年度は、複数タグへの高速な読込の証拠を残すプロトコルを対象に、中間者攻撃に対する高い安全性を証明可能とするプロトコルを提案した。暗号プロトコルと PUF (Physical Unclonable Function：物理的複製困難関数) を融合して省リソース端末における物理的な安全性を確保する仕組みを確立するため、安全性証明を行う上で必要となる PUF に対する様々な安全性要件を定義した。また、PUF を利用することにより物理的な安全性が確保されている RFID 認証プロトコルを構築した。さらに 100 台の FPGA を用いて SRAM PUF の挙動を分析し、構築した認証プロトコルの回路規模及び演算時間を実装により得た (図 2)。

図 2　100 台の FPGA を用いて SRAM PUF の挙動を分析

プライバシー保護型の RFID 認証プロトコルを実際の RFID タグの製造プロセスに載せることにより、回路規模や動作性能、通信可能距離等、実用面での性能評価を委託研究により実施した (図 3)。特に動作性能に関しては、各構成要素の消費電力の差のために確率的に不揮発性メモリへの書き込みミスが見られることが分かった。本研究成果について委託先から報道発表した。

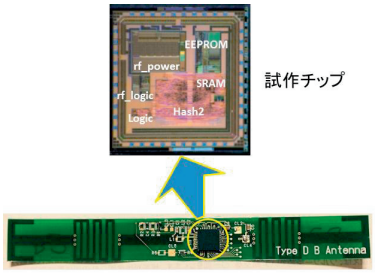

図 3　プライバシー保護型 RFID 認証プロトコルを実装した RFID タグの試作品

Twitter や Dropbox 等、既存の Android 端末向けのサービスに対して、ユーザを主体としてセキュリティの向上が図れる方式を検討し、Android OS 付随の暗号技術を用いた暗号プロトコルを考案した。また、当該プロトコルを Android 端末上で実行した際の処理遅延について実証した 。

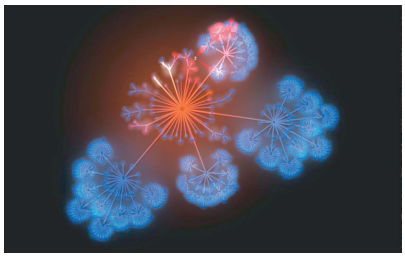

図 4　暗号プロトコルの安全性評価過程の可視化
(攻撃を発見した瞬間の例)

(3)　理論的に網羅性をもった安全性評価技術

ネットワークを利用した通信の安全を保つ目的から、暗号を利用する通信の手順を規定した「暗号プロトコル」の安全性を評価する手法の研究開発を実施している。本年度は、理論的に網羅性をもった評価手法として、あらゆる実行環境における安全性評価が可能な手法を確立した。当該手法を用いて、世界的に著名な国際会議において提案された新規の暗号プロトコルを評価したところ、国際会議での提案時には発見されていなかった脆弱性を検出することができた。形式手法による安全性評価においては、様々な攻撃の可能性を網羅的に確認することが重要である。そこで本年度は、様々な攻撃の過程を可視化するシステムを試作した。本システムでは、理論的な網羅性の確認や、仮に攻撃が発見されたときには発見過程と脆弱性の詳細を直観的に理解することができる (図 4)。

インターネットにおける代表的な暗号プロトコルである SSL/TLS (Secure Sockets Layer/ Transport Layer Security) について、新たに発見された脆弱性の技術的な裏付けと実システムへの影響を評価し、暗号プロトコル評価技術コンソーシアム (CELLOS) に評価結果を提供することで、CELLOS による安全性情報の迅速な発信に寄与した (図 5)。これにより、世界に大きなインパクトを与えた Heartbleed Attack や POODLE Attack を回避する適切な暗号プロトコルの利用促進に貢献できた。

図 5　CELLOS による安全性情報の発信