リスク可視化システムの検討とプロトタイプ構築

ーセキュリティ意識の向上に向けてー

高橋 健志（たかはし たけし）
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 研究員

大学院修了後、2002年、Tampere University of Technologyにて研究員、2004年、早稲田大学国際情報通信研究科にて研究員、2006年、株式会社ローランド・ベルガーにてコンサルタントを経て、2009年より現職。情報通信プロトコル、サイバーセキュリティ情報、及びマルチメディア符号化に関する研究に従事。博士（国際情報通信学）。

1.はじめに

セキュリティインシデントの件数はサイバー社会の発展と共に増加傾向にあります。その原因の1つに、セキュリティリスクに対するユーザの意識の低さがあり、サイバー社会でのセキュリティを維持するためには、平均的なITユーザのセキュリティ意識レベルを向上する必要があります。

本問題に対応するため、ここではユーザの通信に関わるセキュリティリスクを可視化するシステムを提案します。このシステムにより、ユーザはリスクを瞬時に認識可能になります。ウイルス対策ソフトとは異なり、通信全体を鑑みてのリスクの可視化を実現しており、通信経路上にあるルータの脆弱性などについても可視化を実現します。既にこれまでに、ネットワーク管理者向けのインシデント可視化システムなどが提案されていますが、我々は、エンドユーザに対し直接的にリスクを可視化するシステムを提案します。

また、我々はiOSとAndroidを対象に、本システムのプロトタイプ実装を行ったため、本実装についても紹介します。本実装は、セキュリティリスク情報に対するユーザごとのニーズの違いを考慮し、複数のリスク可視化モードを用意しています。

2.システムの概要

このシステムは、コンピュータとネットワークを監視し、関連情報を収集し、ユーザの通信に潜むセキュリティリスクを解析し、そのリスクをリアルタイムに可視化するものです。

2.1 システムを構成する4つのロール

このシステムは、図1の通り、ユーザ端末、ネットワークセンサ、アナライザ、知識ベースという4種類のロール（役割）から構成されます。知識ベースはセキュリティに関する各種知識を蓄積しています。ネットワークセンサはネットワークを監視し、ユーザの通信経路上のセキュリティに関連する情報を収集します。アナライザは知識ベース、ネットワークセンサ、ユーザ端末から得られる情報に基づき、リスクを解析します。ユーザ端末は、端末から得られるセキュリティに関連する情報を収集してアナライザに共有すると同時に、リスク解析結果をユーザに分かりやすい形で可視化します。

これら4種類のロールがお互いに連携することにより、リスクの可視化を実現します。尚、実装時には1つのエンティティ（実体）が複数のロールを兼ねることも可能です。

図1●提案システムを構成するロール

2.2 実現すべき機能

本システムは、最低限以下の4つの機能を実現します。

●通信・ネットワークの現状に関する情報を取得:

通信・通信経路上のリスクが存在し得る場所から、そのリスク判定に必要な関連情報を取得します。例えば、端末などのユーザ環境におけるソフトウェア（OS含む）のバージョンID、無線LANアクセスポイントでの暗号化適用状況、ネットワーク上のルータ、サービスを提供しているクラウドやホスト群のセキュリティ設定、サーバークライアントで利用されている通信方法、ユーザが利用しているサービスに用いられる情報種類、などの情報をそれぞれの場所より取得します。

●既存のリスクに関する知識を収集・蓄積:

今後のリスク判定のために既知のリスク情報を知識として収集・蓄積します。例えば、利用者側や経路途中のルータ、サーバで用いられているソフトウェア等の各バージョンIDに対応する脆弱性情報、暗号の強度に関する情報、それぞれの機器やシステムが利用できる機能、セキュリティ対策手法、現時点での脅威トレンド情報などを収集・蓄積します。なお、自ら収集する

だけでなく、米国NISTのNVD[*1]などの外部データベースと連携します。

●取得した情報からリスクを分析:

前述の現状情報とリスク関連知識に基づきリスクを分析します。後述のプロトタイプでは、CVSS[*2]スコアと専門家の知見をもとにした脅威・リスクデータベースに基づくリスク判定を行なっていますが、様々なアルゴリズムを柔軟に実装可能になっています。

●分析結果を表示:

リスク分析の結果に従い、脅威の存在する場所それぞれについてのリスクの表示を、ユーザの知識レベルに合わせて表現を行います。後述のプロトタイプでは、全体評価を信号機を模した記号により赤・黄・緑の3段階表示を行う通常表示と、ネットワーク上のエンティティを簡易表示し、そのそれぞれが抱えるリスクを3色で表示する簡易トポロジ表示、各リスクの詳細を記載するリスク詳細表示の3段階のリスク表示を実現しています。

図2●プロトタイプのユーザ端末画面 (iPad端末上)

3.プロトタイプ実装

本プロトタイプは、モバイル通信に焦点を当て、iOS及びAndroid端末を利用しているユーザに対しリスクを可視化します。例えば、信頼できない無線LANを利用してインターネットバンキング手続きをしようとしているユーザに対し、リスクを可視化し、警告を発するものとなっています。ここでは、その中のリスク解析とリスクの可視化について紹介します。

3.1 リスク解析

リスク解析プロセスは、ユーザ端末が解析リクエストを送信したところから始まります。本リクエスト中にはユーザ端末のOSとアプリケーションのIDとバージョン番号、通信に利用している暗号などの情報が含まれています。本リクエストを受信すると、アナライザはルータに対し、そのOSバージョン情報を要求します。それらの情報に基づき、アナライザは知識ベースを参照し、現在のユーザの通信に関しリスクが存在しないかどうかを確認します。現在、本知識ベースは、5万件以上の脆弱性情報が保存されているNVDの情報を中心に構築されています。

知識ベースを参照し、関連するリスク情報があった際には、そのリスクの重大度を評価します。具体的には、知識ベース内の脆弱性情報に記載されているCVSSベーススコアを参照し、その値の大・中・小により、リスクレベルの高・中・下を決定しています。また、知識ベースには、利用している暗号技術の組み合わせやサービスタイプとリスクレベルを紐付けた表が存在しており、アナライザは上記の脆弱性情報に加え、この表を参照することで、リスクレベルを判断しています。

3.2 リスク可視化

図2は本プロトタイプの3種類の可視化モードを示しています。

図2 (a) はシンプルモードであり、ブラウザの右上の信号機のみを利用し、その信号機をリスクレベルに応じて赤・黄・緑のいずれかに点灯させることにより、リスクを可視化しています。前述のリスク解析結果に基づき、色が変化する仕組みになっており、赤はリスクが高く、緑は低い状況を示しています。

図2 (b) はトポロジモードであり、現在ユーザが実施している通信に関係するエンティティを簡略表示しています。シンプルモードから信号機をタップすると本モードが表示されます。そして、各エンティティごとに、リスクレベルに応じて赤・黄・緑の色付けをしています。本モードにより、通信中のどの部分にリスクが存在しているのかを容易に把握可能となります。

図2 (c) は詳細モードであり、前述の各エンティティのアイコンをクリックすると、本モードが表示されます。本モードでは、各エンティティのリスクレベル評価結果の理由となる元データを表示しています。例えば、CVE (Common Vulnerabilities and Exposures: 共通脆弱性識別子) 情報やCVSS Base Score情報などをそのまま示しています。本モードは、実際にセキュリティリスクに対して対策を講じる際に、参考となる情報を提示しているものの、平均的な端末ユーザが利用することは現時点では想定していません。また、本モードから画面右上の信号機をタップすると、シンプルモードへと戻れるようになっています。

4.まとめと今後の課題

この記事では、ユーザの通信時のセキュリティリスクを可視化するシステムとそのプロトタイプ実装について紹介しました。現時点において、概念実証を目的とした実装となっているものの、今後、我々の研究室での研究成果を本システムに組み込み、大きく成長させていきたいと考えています。今後は、様々な課題が存在するものの、各情報源が提供する情報の「機密性を保持した」リスク分析機能の実現や、高精度の分析に必要なセキュリティ知識ベース (Knowledge Base) を拡充していきたいと考えています。詳細は、以下をご参照ください。

[参考文献] T. Takahashi, S. Matsuo, et. al, “Visualization of user’s end-to-end security risks,” In SOUPS, 2012.

用語解説

*1 NVD
National Vulnerability Database: 米国 NIST が管理している脆弱性データベースであり、5万件を超える情報が蓄積されています。

*2 CVSS
Common Vulnerability Scoring System: FIRST が主体となって構築している脆弱性のスコアリング手法。スコアが高いほど、その脆弱性に対する対処の優先順位が高いことを示しています。