Poster: Visualization of user's end-to-end security risks

Takeshi Takahashi, Shin'ichiro Matsuo, Akira Kanaoka, Keita Emura, Yuuki Takano
National Institute of Information and Communications Technology, Tokyo Japan
takeshi_takahashi@nict.go.jp

1. INTRODUCTION

The number of security incidents is growing along with the development of cyber society. One reason for that is the lack of users' awareness on security risks. The awareness level of average IT users needs to be improved to maintain security in the cyber society.

To cope with that, this paper introduces a system architecture that visualizes the security risks of user's end-to-end communication so that the user can instantly recognize the risks. Different from anti-virus software that can visualizes security risks of users' terminals, it visualizes security risks residing in the end-to-end communication, including the vulnerabilities of the software running on routers. Different from NICTER [1] that visualizes incidents occurring over network by monitoring network anomaly and providing alerts, it visualizes security risks for users, rather than administrators.

This paper also presents a prototype implementation, which focuses on visualizing risks for iOS and Android tablet users. It is capable of providing differing modes of visualization to accommodate differing needs of security risk information.

2. SYSTEM ARCHITECTURE

The proposed system monitors computer and network systems, collects related information, analyzes security risks of a user communicating over networks, and visualizes the user's security risks in real time. It provides alerts to the user directly, thus improving its security awareness. It supports multiple modes of risk visualization to accommodate differing needs for the depth of risk information; most of users simply wish to see simplified risk alerts, while some wish to know more details on the risks to judge countermeasure. By providing multiple modes of risk visualization, differing types of users can enjoy the system.

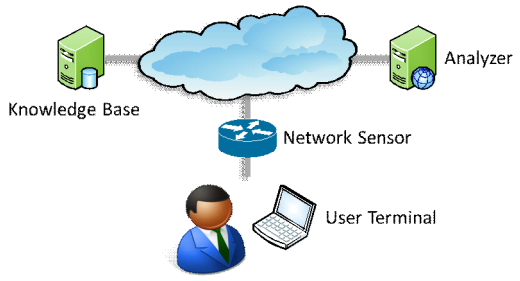

Figure 1: Architecture Overview

Figure 1 describes the needed four roles, i.e., Knowledge Base, Network Sensor, Analyzer, and User Terminal.

Knowledge Base accumulates and organizes assorted knowledge on cybersecurity [2]. Several entities may collaborate to take the role. The National Vulnerability Database (NVD) [3], the Open Source Vulnerability Database [4], and the Japan Vulnerability Notes [5] are its typical instances.

Network Sensor monitors the network and collects information on networks and user's communications. It needs to be implemented on network entities, such as routers, en route from User Terminal to its correspondent node. Several network entities may take this role, and they could be incrementally deployed over networks.

Analyzer analyzes user's security risks based on the information gathered from Knowledge Base, Network Sensor, and User Terminal. Arbitrary risk analysis algorithms could be implemented. Simple example is judging the level of security risks based on the Common Vulnerability Scoring System (CVSS) scores [6] that are derived from Knowledge Base, and is used in our prototype implementation.

User Terminal visualizes the results of security analysis sent from the Analyzer so that users can easily realize and understand the security situation. It also provides differing modes of visualization to accommodate differing types of users. To obtain security analysis result, it shares information on user's communication, such as OS/application versions, SSL cipher suite, and WEP/WPA, with Analyzer.

3. SIGNALING PROTOCOL

The four roles mentioned above need to collaborate with each other to analyze and visualize risks. Figure 2 describes the signaling protocol among them.

This process is triggered by the analysis request sent by a User Terminal. It sends the request to an Analyzer with information on itself, e.g., OS version, application version, and SSL cipher suite information, which is needed for analyzing user's current risks. Upon receiving the request, the Analyzer sends information request to Network Sensor, which replies with the information on the user's communication and related network entities, e.g., en-route routers' IOS version. Note that there exist multiple Network Sensors, thus the Analyzer needs to aggregate the reply from Network Sensors. Upon receiving the reply, the Analyzer queries information on the risks related to the information gathered from User Terminal and Network Sensor to a Knowledge Base. Upon receiving reply from the Knowledge Base, the Analyzer analyzes risks based on the information gathered from the User Terminal, Network Sensor, and Knowledge Base, and then sends the analysis result back to the User Terminal, which visualizes user's risks based on the result. Note that Analyzer could use cache and omit message exchange with Network Sensor and Knowledge Base to minimize the processing overhead.

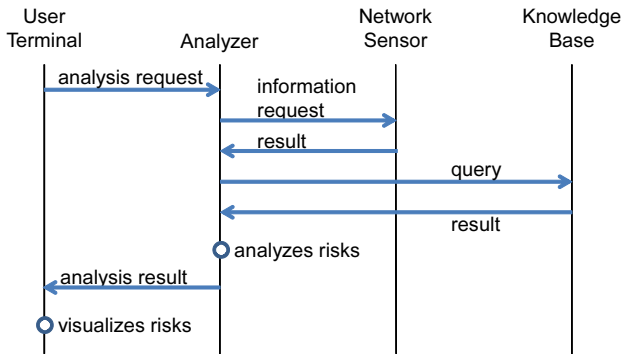

Figure 2: Risk Analysis Procedure

4. PROTOTYPE IMPLEMENTATION

A prototype is built to demonstrate the architecture's usability. User Terminal is implemented on the browsers of iOS and Android, and Analyzer is implemented on Cent OS version 6. Vulnerability data registered inside NVD is used as the Knowledge Base, and CISCO routers are used as Network Sensors.

4.1 Risk Analysis

Analysis procedure is triggered by analysis request sent by User Terminal. The message contains the names and versions of user device's OS and applications, SSL/TLS cipher suite in the access, and WLAN security methods. Upon receiving the analysis request from the User Terminal, it requests information to the routers, which replies with their IOS version information. Note that the Analyzer knows all the routers and can communicate with them via SSH in this prototype. Then it queries to the knowledge base, which contains information on software vulnerability (from NVD with 50,000 records), cipher suites, WiFi security, service type, authentication methods.

Based on the reply, Analyzer analyzes risks. This prototype takes simple approach for that: the Analyzer looks up the CVSS Base Score of the vulnerability information, which indicates the urgency and severity of security risks, obtained from the knowledge base and judges risk levels. The Analyzer judges whether the risk level is either "high", "medium" or "low" depending on the score.

Additionally, the knowledge base has tables for mapping each cipher suites or security type and its risk level, such as (RSA-MD5, risk=high) and (ECDHE-RSA-AES256-SHA, risk=low). Likewise, it maps service type with specific authentication methods and its risk level, such as (banking service with ID/password authentication, risk=high) and (banking service with multi-factor authentication (ID/ password and one time password token), risk=low). The Analyzer judges risk level by looking up this table as well.

4.2 Risk Visualization

Fig.3 depicts three risk visualization modes implemented in the prototype, i.e., simple, topology, and detailed modes.

Simple mode provides red, yellow, and green color signal at the upper right corner of the view. The signal's color changes depending on the value of the aforementioned risk level. This mode is simple and visible for general users, thus helps improving security awareness of general users.

Topology mode provides a simplified network topology map that consists of icons of tablet, WiFi, access point, router, web, and links among them. It is useful to understand the point of risks on the network. Each icon is also colored red, yellow, and green depending on its risk level. This mode is available when the signal is tapped.

Detailed mode provides detailed information on the reason of the above icons' coloring. The information includes CVE (Common Vulnerabilities and Exposures) [7] information and CVSS Base Score. This mode helps to deepen the understanding of the current risk status, and helps to consider countermeasures. It is available when the icons of the simplified network topology map are tapped.

Note that the view goes back to simple mode when the signal at the upper right corner of the view is tapped.

(a)simple mode (b)topology mode (c)detailed mode

Figure 3: Three Modes of Risk Visualization

5. CONCLUSION AND FUTURE WORKS

The proposed system architecture and its prototype implementation visualized user's end-to-end security risks. This will improve the security awareness of average users. Assorted works are needed to advance this system. One of them is enrichment of database to cover wide range of risks. Another is privacy enhancement in information exchanges with assorted entities. It facilitates and encourages the entities to exchange information. We believe this work will improve security awareness and contribute to the advancement of cybersecurity.

6. REFERENCES

[1] Inoue D, et al. Malware behavior analysis in isolated miniature network for revealing malware's network activity. In ICC. 2008.

[2] Takahashi T, et al. Ontological approach toward cybersecurity in cloud computing. In SIN, 2010.

[3] National Institute of Standards and Technology. National Vulnerability Database (NVD). http://nvd.nist.gov/, 2012.

[4] The Open Source Vulnerability Database (OSVDB). http://osvdb.org/, 2012.

[5] JPCERT/CC and IPA. Japan Vulnerability Notes. http://jvn.jp/, 2012.

[6] Mell P, et al. The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems. NIST Interagency Report 7435, 2007.

[7] The MITRE Corporation. Common Vulnerability and Exposures (CVE). http://cve.mitre.org/, 2012.