Demo: Prototype System for Visualizing Security Risks on Mobile Devices

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

1. INTRODUCTION

To maintain information security in the cyber society, it is necessary to improve the awareness level of information security for ordinary IT users. This awareness issue is especially important for mobile communication since devices can be used under insecure environment without users' realizing that. For instance, the wireless connection outside could be less reliable than office network. Visualization of user's end-to-end security risk will improve the security awareness level, and a risk visualization architecture and its prototype are proposed in [1]. This paper demonstrates the prototype's usability.

2. DEMONSTRATION SETUP

The prototype visualizes user's end-to-end security risks and provide alerts to the user directly to improve the security awareness level. By analyzing various information, it visualizes and notifies of potential security risks upon detecting potentially hazardous computer events or communications. It supports both iOS and Android tablets.

Figure 1 depicts the demonstration environment, which consists of a user terminal (User Terminal), an access point and four routers (Network Sensors), an analyzer (Analyzer), a knowledge base (Knowledge Base), and web sites, where User Terminal, Network Sensor, Analyzer and Knowledge Base are the names of the roles defined in [1].

The user terminal accesses to one of the web sites through access point and routers. The analyzer may receive information from the user terminal, access point, routers and web sites to analyze user's end-to-end security risks.

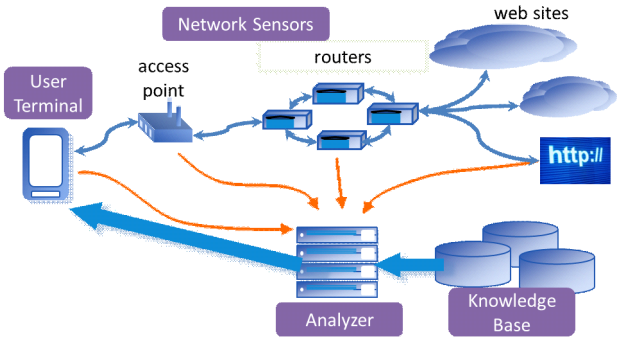

Figure 1: Demonstration Environment

3. RISK ANALYSIS PROCEDURE

When the analyzer receives risk analysis request from the user terminal, it collects information from access point, routers, and the knowledge base that contains information on software vulnerability (from National Vulnerability Database [2] with 50,000 records), cipher suites, WiFi security, service type, authentication methods.

For simplicity, the prototype simply judges risks based on the Common Vulnerability Scoring System [3] Base Score obtained from the knowledge base. Additionally, it has tables for mapping each cipher suites or security type and its risk level. For instance, the table has entries, such as (RSA-MD5, risk=high) and (ECDHE-RSA-AES256-SHA, risk=low). Likewise, the table maps service type with specific authentication methods and its risk level. For instance, the table has the entries, such as (banking service with ID/password authentication, high risk) and (banking service with multi-factor authentication (ID/password and one time password token), low risk).

4. RISK VISUALIZATION MODES

When a user accesses to a service website, this system gathers information on client environment from various entities (e.g. user terminal, access point, and routers). The information includes user device's application name/version, router's iOS version, SSL/TLS cipher suite in the access, and WLAN security method, Then it sends each data to analysis system and receives risk information about client system and accessing service.

Fig. 2 depicts three risk visualization modes of the system.

Simple signal mode.

It provides red, yellow, and green colors when the situation is risky, partially risky, and non-risky respectively. This mode is simple and is useful for general users. This mode is available anytime in the upper right corner of the system,

Topology mode.

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

Detailed mode.

It provides detailed information on the reason of color-

Figure 2: Prototype client system for iPad

ing of the above two modes. Detailed information dialog includes CVE (Common Vulnerabilities and Exposures) [4] information, CVSS (Common Vulnerability Scoring System) [3] Base score, Vulnerability Detail, etc. This mode is available by tapping icons of the simplified network topology map mode.

5. DEMONSTRATION SCENARIOS

This section describes three scenarios, where the signal becomes green, yellow, and red respectively.

Case 1: (home→ bank) with up-to-date tablet.

In this scenario, a user connects to a bank from home by using up-date tablet. The tablet runs up-to-date OS (green), the WiFi connection uses WPA (green), an en-route router has IOS with vulnerability (red), the end-to-end SSL connection uses 2048 bit RSA key exchange, 256 bit AES, and SHA-1 hash-based MAC (green), and the web provides ordinary ID and fixed password authentication (yellow).

Though the web's authentication scheme may leave a little concern, the end-to-end security risk is judged as low since the tablet's OS is up-to-date with no reported vulnerability and the WiFi connection uses WPA, and the key length for the SSL connection is long enough. Thus the signal becomes green.

Case 2: (home→ bank) with old tablet.

In this scenario, a user connects to a bank from home by using old tablet. The tablet runs old OS (red), the WiFi connection uses WPA (green), an en-route router has IOS with vulnerability (red), the end-to-end SSL connection uses 1024 bit RSA key exchange, 128 bit RC4, and MD5 hash-based MAC (yellow), and the web provides one time password (green).

The use of WPA, a key with sufficient length (though not the best) for SSL communication maintains, secure authentication method at the website, maintains security of the communication, and the probability of information leakage from the communication is small. The tablet, nevertheless, uses old OS, which poses vulnerability, and it may cause security incidents in the future communication. Thus the signal becomes yellow to encourage precautions.

Case 3: (net cafe→ bank) with old tablet.

In this scenario, a user connects to a bank from net care through public wireless LAN. The tablet runs old OS (red), the WiFi connection implements no authentication method (red), an en-route router has IOS with vulnerability (red), the end-to-end connection does not use SSL (red), and the web provides ordinary ID and fixed password authentication (yellow).

Tablets provided by net cafes often run old OS with vulnerability, and considers no security when connecting to the Internet. Thus the information inside the tablet could be stolen. Though the current communication has secure SSL communication with the current web page, the web provides only the ordinary ID and fixed password authentication. Thus, if the tablet stores ID and password inside, these information may leak. Thus the signal becomes red to alert security risks.

6. CONCLUSION AND FUTURE WORKS

This prototype visualizes risks to users of mobile tablets (i.e., iOS and Android) using authorized vulnerability database. It monitors computers and networks and visualizes potential risks when needed. As a future work, we will enrich the database of the system to cover wide range of risks, will provide accurate analysis, then will incorporate with privacy enhancing technology in gathering information from mobile device and network sensors to give incentives to do this for users and network operators.

7. REFERENCES

[1] Takahashi T, et al. Visualization of user's end-to-end security risks. In SOUPS. 2012.

[2] National Institute of Standards and Technology. National Vulnerability Database (NVD). http://nvd.nist.gov/, 2011.

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

[4] The MITRE Corporation. Common Vulnerability and Exposures (CVE). http://cve.mitre.org/, 2011.