Ass. Prof.	Rie Shigetomi YAMACUCHI	Campus	Hongo (Eng.Bld.2)	Field	Information Security

Information Security: Personal Authentication and Privacy Protection

Various problems including information theft and fraud exist in the infrastructure for e-commerce. In development of safe and secure systems applicable to such problems, we propose implementation of new information security technologies using next generation techniques in personal authentication. We research these systems in open collaboration with Sakai-lab.

Contact: yamaguchi.rie@i.u-tokyo.ac.jp

1. Personal Authentications and Sensor Information

User authentication is important for secure personal communication on the Internet. Authentication by ID and password is the most popular user validation technique. However, as the technique is based on user literacy and memory, many studies have identified security problems and propose new authentication techniques. The recent prevalence in cases of leaked IDs and passwords mean that changes are urgently required.

In this study, we focused on applying techniques using data collected from portable or handheld devices to personal authentication such as GPS, Wi-Fi, user history, and biometric information. We will apply these techniques to user authentication so that the server can identify who the user is based on the device. Some similar techniques have already been proposed in the field of recognition and classification but not in the field of security for authentication.

We are also interested in evaluating multimodal personal authentication. Multimodal personal authentication identifies individuals using multiple indicators such as biometric fingerprint and finger-vein. By using multiple individual identifiers, the level of accuracy is increased. Multimodal authentication has been applied for practical use, but its theoretical verification as a security evaluation technique has so far been insufficient. This evaluation investigates key technology for multiple sensor authentications.

2. Trust Platform and Security

The root of trust on the system is required for security techniques. When users manage certain computing systems such as clouds, they need to trust part of a device in order to ensure whole system security. For example, if a system has a trust point used to gain access, a root of trust such as a smart card can be used to unlock the trust point.. We discuss the use of anti-tamper devices including secure processors or smart cards for the root of trust.

3. Privacy Protection Techniques by Real Data

Privacy protection techniques are an alternative security method to personal authentication as the latter identifies a user while the former gathers user information without identifying. We focus on analyzing real data collected by sensory input devices, and discuss the risks that would identify how much information is necessary to complete tasks versus how much causes privacy risks. We also discuss privacy issues including what kinds of information are classified as key data and what information is necessary for making use of another application.

You can choose any research topic in the field of information security and I would be very happy to encourage you to pursue new challenges.