Inter-device Authentication and Authorization Framework: Demonstration System based on Novel Smart Card Software

Manabu Hirano
Department of Information and Computer Engineering
Toyota National College of Technology
2-1 Sakae, Toyota, Aichi 471-8525, Japan
+81-565-36-5870
hirano@toyota-ct.ac.jp

ABSTRACT
Future networked device interacts with each other and they will provide useful services to users. This demonstration's goal is to show the usability of proposed novel authentication and authorization framework guaranteeing explicit ownership for an inter-device communication paradigm.

Categories and Subject Descriptors
H.4 [**Information Systems Applications**]: Miscellaneous

General Terms
Security

Keywords
Inter-device communication, authentication, authorization

1. INTRODUCTION
The concept of '"ubiquitous computing" Mark Weiser first proposed essentially indicates future network will be connected to a large number of non-PC networked devices naturally. Future networked device interacts with each other and they will provide some useful services to users. This demonstration shows a novel security mechanism for an inter-device communication paradigm.

2. BASIC CONCEPT
The basic idea of our proposal [1] is a novel ID management model for future networked devices shown in Figure 1. Our framework can manage the device's ID issued by a manufacturer, ownerships defined by a user and other attributes like purchased rights for services. Our proposal employs X.509 public key certificate (RFC3280) for device's ID and attribute certificate (RFC3281) for ownerships and other attributes. The ownerships and other attributes are strongly associated with the device's ID. It is based on PKI cryptographic techniques using trusted authorities of each certificate and their authorized digital signatures. The device can authorize accesses from other devices based on the device's ACL (Access Control List). Proposed novel smart card software can store the device's ID, user's ownerships and an ACL in a safe manner. The smart card software also can execute inter-device authentication function securely.

SIGCOMM'08, August 17–22, 2008, Seattle, Washington, USA.
ACM 978-1-60558-175-0/08/08.

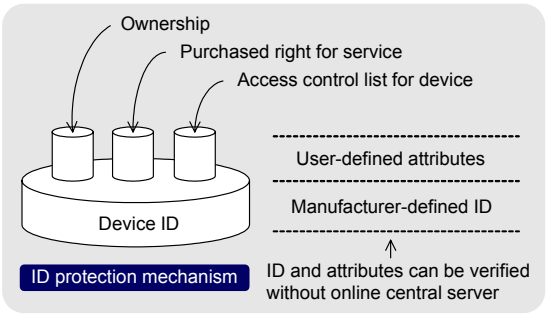

Figure 1. Novel ID management model for an inter-device communication paradigm.

3. DEMO SYSTEM
This demonstration employs a micro server with proposed IC chip (smart card) as a security proxy for target appliances. Micro server runs Debian GNU/linux and our middleware system based on customized IKEv2 and IPsec. Communication between two target appliances is automatically protected by IPsec-VPN. IKEv2 executes inter-device authentication and UPnP service authorizes requests using proposed novel smart card software. Figure 2 shows the demonstration system for a conventional home appliance (TV device). The micro server can control conventional home appliances using IR control unit. This demonstration also shows the application for an IP-based security camera. Proposed micro server runs customized *racoon2* (latest implementation of IKEv2) and *USAGI* IPsec stack on Linux.

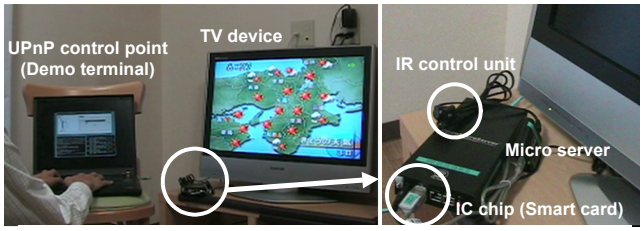

Figure 2. Proto-type system using micro server with smart card and UPnP controlled TV device.

4. REFERENCE
[1] M. Hirano, T. Okuda and S. Yamaguchi, Inter-device Communication Paradigm: Requirements Analysis for Its Security Mechanisms. In Proceedings of IEEE/IPSJ SAINT 2008, the Fifth Workshop for Ubiquitous Networking and Enablers to Context-Aware Services, July 2008 (to appear).