

2007 Annual Computer Security Application Conference
Work in Progress Abstract Proposal

**Towards securing inter-device communication:
Applying Inter-device Authentication and Authorization Framework
to Home Appliances**

Manabu Hirano^{1,2}, Takeshi Okuda², Suguru Yamaguchi²

¹ Toyota National College of Technology, Aichi, 471-8525, Japan

² Nara Institute of Science and Technology, Nara, 630-0192, Japan
{mana-hi, okuda, suguru}@is.naist.jp

1 Background

Future networks everywhere will be connected to innumerable Internet-ready home appliances. A device accepting connections over a network must be able to verify the identity of a connecting device in order to prevent device spoofing and other malicious actions. In recent works, some major existing home network specifications consider device-specific security functions. For example, UPnP Security [1] has a sophisticated mechanism to guarantee personal ownership of a device. UPnP Security defines a special terminal device called “Security Console” to set up security configurations on each device remotely. UPnP Security also has an inter-device authentication and authorization mechanism using a public key pair, Security ID and ACL. Bluetooth [2] has a secure simple pairing mechanism to take ownership of a device. After the taking ownership of the device, two devices generate a shared secret (called a link key) for future mutual authentication. As mentioned above, some major specifications already consider a security mechanism for devices. We have also proposed a novel security mechanism not for human being but for devices [3]. In this report, we show a practical tiny security surveillance system for conventional home appliances to achieve our proposed inter-device authentication and authorization framework.

2 Multiple Ownership Model

In existing security mechanism for devices like UPnP Security, an owner initially takes ownership of a device (typically, by inputting a password). As a result, the device can act as an agent for the owner. Most conventional systems restrict this taking ownership operation to a single owner only. They only permit single ownership on a device. However, we assume that some devices are shared by multiple users. So we extend the conventional model to multiple ownerships. Fig.1 shows our proposed multiple ownership model for inter-device authentication and authorization. Our proposal will be effective for a device shared by multiple users, especially autonomously-controlled device such as home robot, automatically-controlled security equipment and home appliances. These devices are not controlled by user directly, but they interact with other devices autonomously. In this report, we discuss a security mechanism for inter-device communication. We distinguish user-to-device communication and device-to-device communication. Our proposal focuses on a security mechanism for device-to-device communication without user interaction.

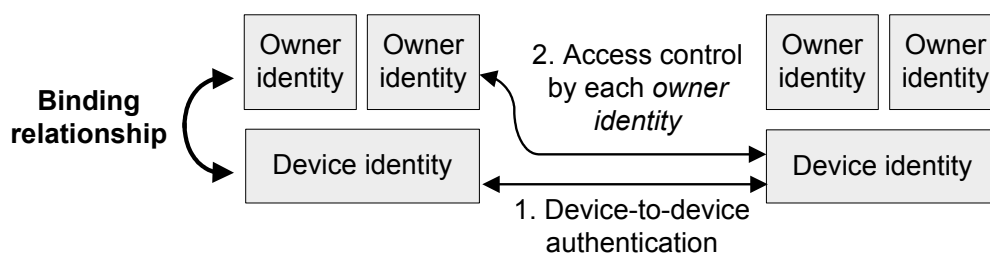


Fig.1 Multiple ownership model for inter-device authentication and authorization

3 Applying Inter-device Authentication and Authorization Framework to Home Appliances

We have already developed original IC chip software to execute inter-device authentication and authorization functions [3]. The software employs a *public key certificate* to guarantee a device identity and an *attribute certificate* to guarantee device's ownership. We utilize this IC chip software to achieve the multiple ownership model shown in Fig.1. We are developing a practical security surveillance system as a sample application of our framework. Fig.2 shows the design of the system. The micro server in fig.2 enables us to connect conventional home appliances to the Internet securely. In our proposal, a user can install her or his ownership information and ACL onto each device's IC chip. This system consists of a micro server (AMD Alchemy, PoE powered) with Debian/Linux and the IC chip (Gemalto Cyberflex e-gate 32k). We extend latest IKEv2 (Internet Key Exchange version 2) implementation "racoon2", and it can execute inter-device authentication with proposed IC chip software. This system can attach and control a conventional home appliance easily by IR remote control and basic UPnP architecture at this time. Fig.3 shows the security architecture of the prototype system. Communication between two home appliances is protected by IPsec-VPN automatically except UPnP discovery and IKEv2 negotiation. In our proposal, the device can authorize other device's request based on her or his ownership (i.e. an attribute certificate in the IC chip). Fig.4 shows the prototype system.

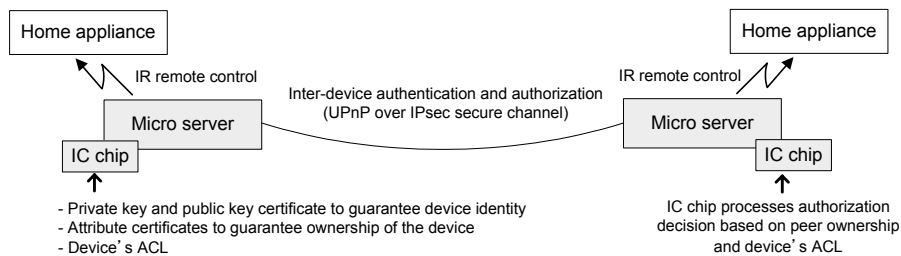


Fig.2 Design of the proposed security surveillance system for a home appliance

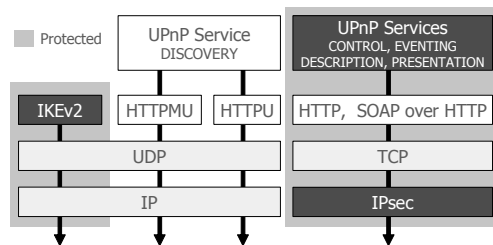


Fig.3 Security architecture of the prototype



Fig.4 the prototype

4 Conclusion and Future Plans

In this report, we show the practical security surveillance system to illustrate the usability of our proposed inter-device authentication framework. A traditional user-to-device authentication and authorization mechanism is still useful. However, future networks will consist of many autonomously-controlled devices. So we have proposed novel inter-device authentication and authorization framework and its prototype system. We plan to apply our proposal to autonomously-controlled devices such as a home robot and an automatically-controlled security equipment, etc. Our goal is to realize secure end-to-end device communication on practical wide-area network environment.

References

1. Carl Ellison, "UPnP Security Ceremonies Design Document For UPnP Device Architecture 1.0", 2003.
2. Bluetooth SIG: Specification of the Bluetooth System Version 2.0 + EDR, 2004.
3. Manabu Hirano, Takeshi Okuda, Suguru Yamaguchi, "Application for a Simple Device Authentication Framework: Device Authentication Middleware using Novel Smart Card Software", Proceedings of IEEE SAINT 2007 Workshops, Hiroshima, Japan, 2007.