A Study on Security Management Architecture for Personal Networks

Takashi Matsunaka[1], Takayuki Warabino[1], Yoji Kishi[1],
Takeshi Umezawa[2], Kiyohide Nakauchi[2], and Masugi Inoue[2]

[1] KDDI R&D Laboratories, Inc.,
Ohara 2-1-15, Fujimino, Saitama, Japan
{ta-matsunaka,warabino,kishi}@kddilabs.jp
[2] The National Institute of Information and Communications Technology,
Nukui-Kitamachi 4-2-1, Koganei, Tokyo, Japan
{umezawa,nakauchi,inoue}@nict.go.jp

Abstract. The authors have studied the security management architecture for Personal Networks (PN). The main feature of the proposed architecture is to exploit a trusted cellular system, namely, an IMS (IP Multimedia Subsystem), to provide security functions for PNs over open networks like the Internet. They also proposed two security functions to solve security issues for a PN, PE ID and Key Assignment (PIKA) function and a PN Key Sharing (PNKS) function. The PIKA function assigns an ID and key to non IMS–compliant devices (Peer Equipment: PE) to authenticate the user of the PE with the assistance of the IMS–compliant terminal (User Equipment: UE). The PNKS function makes it possible for PEs to share a common cipher key (PN Key) in a PN, which is used to protect a PN against eavesdropping on application data.

Keywords: Personal Network, Mobile Computing, Key Sharing.

The authors proposed the security management architecture for Personal Networks (PN) [1] (Fig. 1 shows an example of PN concept). The architecture has two features, (1) to exploit a trusted cellular network system, the IMS (IP Multimedia Subsystem) [2], to provide security functions for PNs over open networks like the Internet, and (2) to reduce the management cost on the centralized server in order to deal with multitudes and a wide variety of information devices (e.g. a computer, an information appliance, a sensor device and a specific-use device such as a portable music player). Fig. 1 shows an overview of the proposed architecture. There is a PN Server (PN–S) to provide PN establishment service. The PN–S is accommodated in the IMS as an IMS Application Server and also is connected to the Internet. The PN–S plays the role of mediator for the security functions and interworking with the IMS. Users have an IMS–compliant terminal (User Equipment (UE)), e.g. a cellular-phone, and non–IMS compliant devices (Peer Equipment (PE)). UEs are connected to the IMS, and PEs are connected to the Internet over several access systems. PEs in a PN directly exchange application data with each other without the intermediation of the PN–S.

To realize the secure establishment of PNs, two security issues need to be considered. (1) Accommodation of PEs in a PN securely, and (2) Secure communication in a PN. To solve the issues, the authors proposed two security functions, a PE ID and Key Assignment (PIKA) function, and a PN Key Sharing

P. Sénac, M. Ott, and A. Seneviratne (Eds.): MobiQuitous 2010, LNICST 73, pp. 344–346, 2012.

(PNKS) function. The PIKA function provides an identity and a key (a PE ID and a PE Key) to a PE so that PN–S can authenticate the user of the PE. In the proposed approach, a PE ID includes information to derive the PN Key so that the PN–S can generate the PE Key corresponding to the PE on demand. This approach alleviates key management cost in PN–S since the PN–S does not need to keep all PE Keys. The PNKS function enables PEs to share a common key (PN Key) in a PN, which prevents outsiders of PN from eavesdropping application data in the PN. For secure PN Key delivery, the function employs Broadcast Encryption (BE) [3], which has a revocation method to prevent digital contents being viewed by nonsubscribers without changing all the key information users own. In addition, from the viewpoint of scalability, the function adapts the hierarchical membership management to reduce the computational load of device management imposed on the PN–S. A PN convener's UE only manages the PN participant's UE membership of a PN, and a PN participant's UE only the PE membership. In Fig. 1, Alice's UE (UE_{PN}) recognizes Bob's UE (UE_b) is a member of her PN (PN_y), and UE_b recognizes PE_4 is a member of PN_y. The overview of the PN Key delivery flow is as follows, (1) a PN convener's UE sends the PN Key to each PN participant's UE via the IMS, (2) a PN participant's UE encrypts the Key with BE so that only PEs in the PN can decrypt it, and sends it to the PN–S, (3) a PE receives the encrypted Key from the PN–S, and decrypts it.

The authors also implement the proposed architecture and perform a qualitative analysis. Through the analysis, security and scalability of the proposed architecture are validated. It is notable that the PNKS function reduces the key management cost of the PN–S from $O(N_{all})$ to $O(N_U)$, where N_U be the number of participants in a PN, N_{all} be the number of all PEs which could potentially join a PN, compared with the centralized approach where only the PN–S manages all PEs' security information.

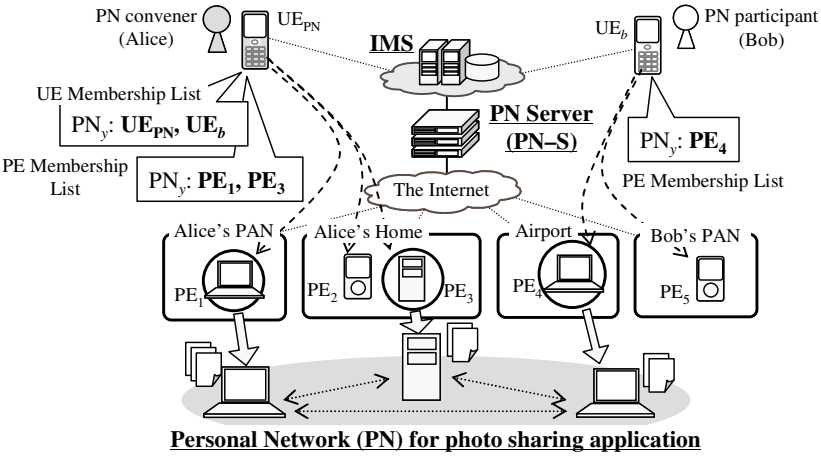

Fig. 1. Overview of Personal Networks and Hierarchical Membership Management

This is the case where Alice (PN convener) wants to provide a photo sharing application using her PC at home (PE_3). She wants to look at her private photos on her laptop PC (PE_1), and Bob (PN participant) also wants to look at them on a laptop PC at the airport lounge (PE_4). Alice constructs a PN, which consists of PE_1, PE_3 used by Alice and PE_4 used by Bob.

References

1. IP Multimedia Subsystem (IMS) Stage 2 (Release 8), 3GPP Technical Specification 23.228
2. My personal Adaptive Global NET, http://www.telecom.ece.ntua.gr/magnet/index.html
3. Naor, D., Naor, M., Lotspiech, J.: Revocation and Tracing Schemes for Stateless Receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001)