Providing Ubiquitous Networks Securely Using Host Identity Protocol (HIP)

Work-in-Progress Paper

Akihiro Takahashi
Graduate School of Informatics
Kyoto University
Yoshida Honmachi, Sakyo-ku
Kyoto, 6068501, Japan
takahashi@net.ist.i.kyoto-u.ac.jp

Yasuo Okabe
Academic Center
for Computing and Media Studies
Kyoto University
Yoshida Honmachi, Sakyo-ku
Kyoto, 6068501, Japan
okabe@i.kyoto-u.ac.jp

ABSTRACT

In an ideal ubiquitous network, anyone is supposed to be able to get connection to the Internet as long as some connectivity to the Internet exists there. A network administrator is supposed to provide a network to public visitors without any explicit permission like registration of users. At the same time, when an incident has occurred, such as an illegal access by an user, the network administrator needs to be able to trace the user, and to clear who the user is. Additionally, the proof that the network administrator has not commit incorrect accesses should be ensured because the network administrator is not trusted. That is to say, nonrepudiation should be ensured. To solve these problems, we apply Host Identity Protocol (HIP) to implement secure ubiquitous networks. In our network, users can connect only by HIP. We propose an authentication that does not impose management work on the network administrator. We would like to discuss how the network administrator can ensure nonrepudiation, and the traceability of users.

Categories and Subject Descriptors

C.2.2 [**Network Protocols**]: Protocol architecture (OSI model), Protocol verification; C2.3 [**Network Operations**]: Network management, Public networks; C2.5 [**Local and Wide-Area Networks**]: Internet (e.g., TCP/IP)

General Terms

Design, Security

Keywords

ubiquitous network, Host Identity Protocol, network security

1. INTRODUCTION

Today, every electronic equipment, such as Personal Data Assistant (PDA), has various network connection interfaces, ubiquitous networks is expected to be realized. What we call a ubiquitous network is a network environment where anyone can get connection to the Internet anytime while there exists Internet connectivity. To that end, a network administrator is supposed to provide a network to public visitors without any explicit permission like registration of users. At the same time, when an incident has occurred, such as an illegal access by an user, the network administrator needs to be able to trace the user, and to clear who the user is.

Recently, we can use public wireless Internet access services in various places, a cafe and the Shinkansen, for example. These services are provided by a company such as an Internet Service Provider (ISP) or an organization such as a university. In these network services, we call services provided as free, such as FON[1] and eduroam[2], Open Ubiquitous Network Architecture.

In this architecture, the network administrator is responsible for protection against attacks, for instance incorrect access to the outside network, sending illegal contents (movies, documents, etc.), and slanders against someone, using such network by an anonymous user. Additionally, to specify a malicious user when an incident has occurred, the network administrator needs to authenticate users. That is, the network administrator needs to manage many accounts and take logs, it is a burden for the network administrator.

If a malicious user attacks to a correspondent, the correspondent raises a complaint to the network administrator because the correspondent can trace the user only by the IP address, so cannot recognize the malicious user's identity. This is also a burden for the network administrator. There is an approach that giving ID different from IP address to users. A malicious user who has attacked someone also should not be able to make excuses, and to put the blame on the network administrator. This is called nonrepudiation.

We apply Host Identity Protocol (HIP)[3] to implement secure ubiquitous networks. In our network, users can connect only by HIP, but only if users connect by

HIP, all HIP connections are allowed. We propose a user authentication that does not impose management work on the network administrator. We would like to discuss how the network administrator checks an access of a user and ensures a traceability of a user's identity, and how the network administrator can ensure the nonrepudiation.

The rest of this paper is organized as follows. We introduce some basic architecture of HIP in Section 2. In Section 3, we define a problem of a burden for the network administrator. Then, we discuss our approach in Section 4. Finally, we conclude and describe future works in Section 5.

2. HOST IDENTITY PROTOCOL

HIP strengthens security against some attacks, and supports host mobility and multi-homing as extension[4]. In this section, we describe some basic architecture of HIP, which is supposed to be important to consider secure ubiquitous networks.

2.1 Locator/ID Split

In an ordinary Internet connection, an IP address has two roles, these are a host identifier (ID) and a location of the host in the Internet topology (Locator). Because of this, it is difficult to cope with various requests flexibly. For instance, a mobile host wants to connect to an another network seamlessly. In this case, the host needs to change only its Locator without changing its ID.

Based on this Locator/ID Split concept[5][6], HIP uses Host Identity and Host identity Tag as an ID, and uses an IP address as Locator.

2.2 Host Identity, Host Identity Tag

All HIP hosts have a pair of a public key and a secret key. These keys are unique, then hosts are able to be authenticated. This pair is called Host Identity (HI), which is generated by the host itself with RSA algorithm. Their length is 512, 1048, or 2048 bits.

Host Identity Tag (HIT) is designed as Overlay Routable Cryptographic Hash Identifiers (ORCHID)[7], which length is 128 bits. HIT is a special class of IPv6 address. Last 32 bits of HIT is called Local Scope Identifier (LSI), which is usually used at local network. HIT and a public key of a host are stored in DNS[8].

HIP uses this HI and HIT as the identifier of the host. Figure 1 shows their format.

2.3 Base Exchange

In HIP, endpoints perform a key exchange at the beginning of a session, called Base Exchange. It is a 4-way handshake process, consisting of packets called I1, R1, I2, R2 packets. Base Exchange distributes Diffie-Hellman keys[9] and authenticates the hosts. HIP connection is encapsulated by IPsec ESP mode using this

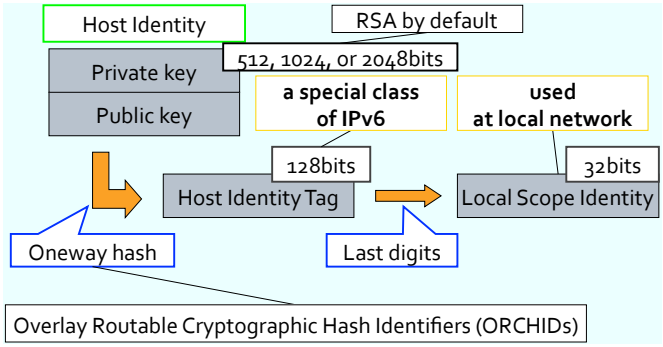

Figure 1: HI, HIT

key, hence data are encrypted between endpoints. Because of this, HIP strengthens security against eavesdropping and falsify packets. How Base Exchange proceeds is shown in Figure 2.

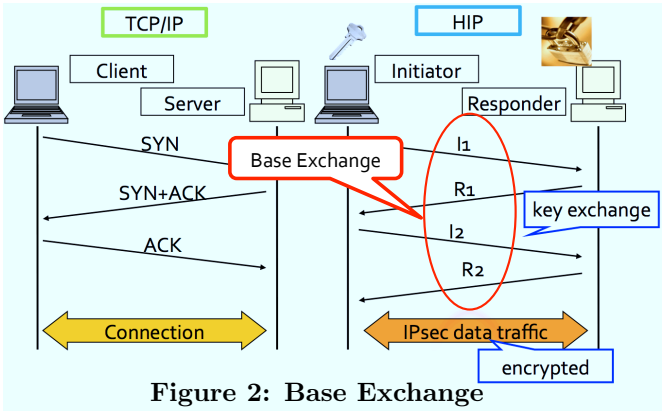

Figure 2: Base Exchange

3. PROBLEM DEFINITION

For the environment that everyone can provide a network, it is expected that reducing or dividing authentication costs with someone. The network administrator also can trace users, in other words, the network administrator should ensure the traceability of users. Additionally, the proof that the network administrator has not commit incorrect accesses like eavesdropping packets should be ensured because the network administrator is not trusted. That is to say, nonrepudiation should be ensured.

We propose applying HIP to ubiquitous networks to solve these problems. In our network, users can connect to the Internet only by HIP. HIP is an end-to-end security protocol, and data is encrypted. That is, HIP ensures the nonrepudiation. Moreover, each HIP host has an ID unique in the world. We propose that a DNS operator authenticates users using this ID to divide authentication costs.

On the other hand, as stated in Section 1, services like FON and eduroam are provided. In eduroam, the administrator divides authentication costs with RADIUS server. Ohira et al. [10] also discuss how securely public

wireless Internet access service models can be provided. Komura et al. [11] have been serving public wireless Internet access network called Mobile Internet Access in KyotO (MIAKO), using Microsoft Point to Point Tunneling Protocol (PPTP)[12] as a Virtual Private Network (VPN) tunneling protocol. In MIAKO network, users can connect to the Internet only by PPTP, VPN tunneling protocol. It is managed by a non-profit organization and supported by citizens in Kyoto, Japan.

Table 1 shows these concepts.

Table 1: Concepts comparing

	Authentication	Logs
FON	FON operate team	not need
eduroam	RADIUS server	need
MIAKO	VPN server	not need
Our proposal	DNS server	need
	Nonrepudiation	—
FON	NG	—
eduroam	NG	—
MIAKO	OK	—
Our proposal	OK	—

Ohira et al. [13] operate MIAKO network. In MIAKO network, a VPN server operator manages accounts of users, hence a labor of the network administrator can be lightened. There might be large overhead, however, in case a user connect MIAKO network from a distance, because the user must access to the network via the VPN server, even if users are side by side. We also solve this problem.

4. OUR PROPOSAL

We propose Open Ubiquitous Network Architecture based on HIP in this paper. We would like to discuss the following four things, dividing authentication costs, nonrepudiation, traceability, and some threats. We give some considerations about the validity of applying HIP for Open Ubiquitous Network Architecture by network administrator's point of view.

4.1 Dividing authentication costs

In our approach, a DNS operator provides the authentication. The DNS operator registers users beforehand, and manages relationship between HIs and personal data of users. The network administrator can trace users by asking the DNS operator who the user is. This concept is shown as Figure 3.

As stated in the Section 2.1, HI and a public key of host are stored in DNS. HIP uses these information in authentication, so that DNS security is very important. Because of this, HIP strongly recommends the use of the DNS Security Extensions (DNSSEC)[14]. In this paper, we define the use of DNSSEC with HIP. DNSSEC ensures that DNS records indeed come from trusted DNS,

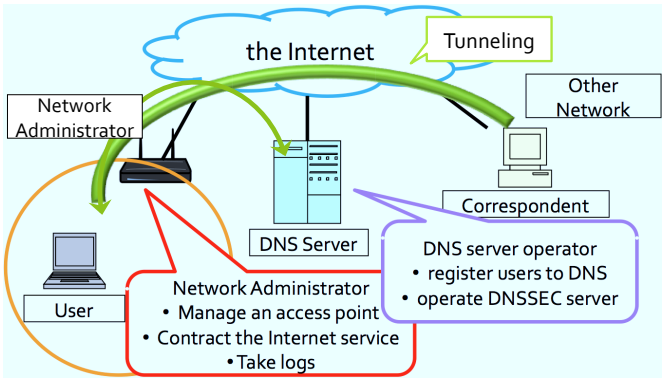

Figure 3: Dividing costs

and have not been modified using electronic signature (Figure 4).

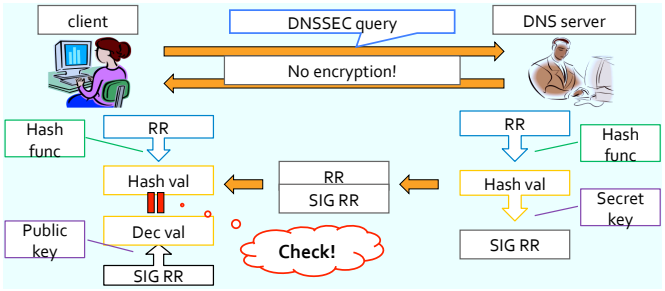

Figure 4: DNSSEC

4.2 Nonrepudiation

In conventional Internet access services, there are some threats as follows. For example, a malicious network administrator can forge packets, and make an IP spoofing attack. A third party cannot make it clear that the network administrator has not attacked anyone. Thus, a malicious user who has attacked someone can make excuses, and put the blame on the network administrator. In our network using HIP, however, a user and the network administrator are clear while their connection has being established because a user and a correspondent authenticates each other. Their packets can be verified by themselves or the network administrator, using DNSSEC as the trusted third party. Additionally, HIP encrypts data between endpoints, so that packets after Base Exchange are protected against eavesdropping and falsifying packets. The network administrator cannot eavesdrop data packets. That is why, the nonrepudiation is ensured in our approach. In other words, if an incident has occurred, the network administrator can assert that the network administrator is not the attacker.

4.3 Traceability

HIP works between endpoints, some middleboxes can verify packets on the other hand. Data packets after Base Exchange is encapsulated by IPsec ESP mode, but

Base Exchange packets is not encrypted. The network administrator can get HI, HIT, and IP address by checking Base Exchange packets, and can trace users by asking the DNS operator about the person who has that HI. On the other hand, an encryption key between a user and a correspondent is protected by Diffie-Hellman key exchange.

4.4 Threats

There are some threats remaining, such as Denial of Service (DoS) attacks, and session hijacking. It is difficult to protect against DoS attacks and DDoS (Distributed DoS) attacks. Several countermeasures, such as bandwidth control, shutting out ICMP packets, and using firewall, should be taken same as an ordinary network.

In HIP, it is supposed to be protected against session hijacking because users authenticate each other. However, in case that an attacker in the network administrator's network conspires with another attacker in other network. That is, once Base Exchange has been completed by a proper user and correspondent, the attackers can forge packets using their IP addresses by eavesdropping the header of data packets. Then, the attackers can hijack their session. If an attacker try to hijack session alone, the attacker cannot connect to a correspondent because the attacker does not have the encryption key. The conspiracy of attackers is needed to hijack session.

5. CONCLUDING REMARKS

In this paper, we apply HIP to implement secure ubiquitous networks. We have given some considerations about providing securely ubiquitous network using HIP.

We divides authentication costs of the network administrator with the DNS operator. We have described the network using HIP is more secure than ordinary Internet access services in some ways. For example, the protection against forging packets, an IP spoofing attack, and eavesdropping is strengthened. However, there are some threats remaining, such as DoS attacks and session hijacking in case that attackers conspire each other.

The network administrator can verify packets, and can trace users using their HI and HIT. The traceability of users is ensured. On the other hand, the administrator cannot eavesdrop data because data is encapsulated by IPsec ESP mode. A malicious user who has attacked someone cannot make excuses, and cannot put the blame on the network administrator because users authenticates each other. The Nonrepudiation is ensured in our approach.

Future works include more deep consideration about such problems that packet filtering methods and the format of logs. We would like to design secure ubiquitous network architecture which is easier to operate, and to implement and evaluate our architecture in practice.

6. REFERENCES

[1] FON. `http://www.FON.com/`.

[2] eduroam. `http://www.eduroam.org/`.

[3] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. In *RFC 5201*, Apr. 2008.

[4] P. Nikander, T. Henderson, C. Vogt, and J. Arkko. End-Host Mobility and Multihoming with the Host Identity Protocol. In *RFC 5206*, Apr. 2008.

[5] V.P. Kafle, H. Otsuki, and M. Inoue. An ID/locator split architecture of future networks. In *Second ITU-T Kaleidoscope event on INnovations for Digital Inclusion*, 2009.

[6] V.P. Kafle, K. Nakauchi, and M. Inoue. Generic identifiers for ID/locator split internetworking. In *First ITU-T Kaleidoscope event on Innovation in NGN*, 2008.

[7] P.Nikander, J. Laganier, and F. Dupont. An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID). In *RFC 4843*, 2007.

[8] P. Nikander and J. Laganier. Host Identity Protocol (HIP) Domain Name System (DNS) Extension. In *RFC5205*, Apr. 2008.

[9] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22, No.6:644–654, Nov. 1976.

[10] K. Ohira, Y. Huang, Y.Okabe, K. Fujikawa, and M. Nakamura. Security Analysis on Public Wireless Internet Service Models. In *WMASH '05*, pages 107–110, Sept. 2005.

[11] Takaaki Komura, Kenji Fujikawa, and Yasuo Okabe. The MIAKO.NET public wireless internet service in Kyoto. In *Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, WMASH '03, pages 56–63, 2003.

[12] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn. Point-to-Point Tunneling Protocol (PPTP). In *RFC2637*, July. 1999.

[13] Kenji Ohira, Atsushi Sumioka, Yuki Kitaoka, Takaaki Komura, Kenji Fujikawa, and Yasuo Okabe. Design and Management of the MIAKO.NET Public Wireless Internet Access Service. *The Transactions of the Institute of Electronics, Information and Communication Engineers*, J93-B:759–768, 2010.

[14] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. In *RFC4033*, Mar. 2005.