Security Analysis on Public Wireless Internet Service Models

Kenji Ohira
Kyoto University
Kyoto, Japan
ohira@net.ist.i.kyoto-u.ac.jp

Ying Huang*
Kyoto University
Kyoto, Japan
ying@net.ist.i.kyoto-u.ac.jp

Yasuo Okabe
Kyoto University
Kyoto, Japan
okabe@i.kyoto-u.ac.jp

Kenji Fujikawa
Kyoto University
Kyoto, Japan
fujikawa@i.kyoto-u.ac.jp

Motonori Nakamura
Kyoto University
Kyoto, Japan
motonori@media.kyoto-u.ac.jp

ABSTRACT

A new service model of public wireless Internet access, called autonomous distributed public wireless Internet access, is presented. In the service model any volunteer with broadband Internet access lines can provide his access points for public service without any fear of malicious use. A user of such service is assumed to have his own account on a authentication server at home in the Internet, and all the Internet access through any of those access points can be treated as if it is from the home. In this paper, we present how the autonomous distributed Internet access services can be securely provided with the combinations of two aspects: treatment of authentication transactions at access points and data path of communication transaction.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication*

General Terms

Security

Keywords

Grass-root Public WLAN Service, Minimum Procedure for Security

*She currently belongs to Goldman Sachs Japan.
Mailto: ying.huang@gs.com

WMASH'05, September 2, 2005, Cologne, Germany.

1. INTRODUCTION

In the past few years, rapid growth has been seen in public wireless Internet access service. Today, mobile users tend to access the Internet at a variety of locations, such as restaurants and airports, for email, web and so on.

Some of such service are managed by Internet Service Providers (ISPs). Coverage, management cost and pricing challenges have been addressed [2]. There is another type of services, so called grass-root services, managed by voluntary individuals. Here we call them *self-managed* hotspots. Typically a small cafe provides their customers wireless access. Cost is not an important issue since the extra cost for such service is relatively small for the owner if he already subscribes an Internet access service. Hence such services are provided free or with relatively cheaper fee than that of ISP service.

The most serious issue in such services is security. In most of self-managed services no authentication of users is done at all. Nowadays anonymous access to the Internet is nothing but a threat. To cope with the problem, some self-managed hotspots restrict the ports which they permit to limited applications. However even they restrict ports only for mail and web access, malicious user may send SPAM email or slander in BBS. On the other hand, self-managed hotspots are less reliable for mobile users than those by ISPs. Mobile users are exposed to the threat of their communication being eavesdropped, manipulated or spoofed by malicious access points.

In this paper, we propose a new service model, what we call *autonomous distributed Internet access service* model. The model has both good points of security in the ISP model and cost benefit in self-managed model. The essential difference of our model from the conventional roaming is that no pre-organized trust between the owner of access points and the administrator of the authentication mechanism is assumed. We then show secure model from two aspects: treatment of authentication procedure at an access point and data path of communication transaction. Finally we analyze and evaluate the security level achieved in our proposed implementation.

This paper will be organized as follows: in section 2, we

defines three models of public wireless Internet access services. In section 3, we clarify the security requirements for the public wireless Internet access service. In section 4, we propose four models using two approaches — authentication at access point and tunneling mechanism. Finally, in section 5, we make some notes on our conclusion.

2. CATEGORIZATION OF PUBLIC WIRELESS INTERNET SERVICE

In this section, we introduce some existing public wireless Internet access services. We will compare their features and problems with the two aspects: security and management cost. Security is the fundamental premise. Considering the adoption in grass-root manner, however, most of the owners cannot to be expected to be specialists of the Internet nor security. It is required to reduce their management cost for security.

2.1 ISP Model

In this model, ISPs are in charge of the access points and the access line to the authentication server. They are responsible to manage user accounts, save authentication records and ensure the authentication process secure.

Mobile users trust their facilities, including the access points, authentication servers and access lines provided by the ISPs. They sign contracts and obtain their accounts before using the connectivity services provided by the ISPs. Currently security problems of the ISP type public wireless Internet are caused by the wireless property.

In ISP models, their coverage, management cost and pricing challenges have been addressed. As most of the single ISPs lack widespread coverage, roaming among multiple ISPs [6] with a centralized authentication server and layered authentication, have been taken. However, both solutions cost too much.

2.2 Self-managed Model

Most of the currently available services of self-managed spots are provided with naive configuration of access point — no user distinction, shred WEP only or even none. Some add extra features to restrict a limited application to pass through.

In the self-managed model, however, an owner of an access point is more strongly required to identify users of his access point and to keep access log than in the ISP model. On the request of the ISP Law [1], the owners of those access points are responsible to identify the illicit user when requested.

For the identification, some owners check their users' public ID such as a passport or a driving license card at the user registration. Others use cell phone for registration. After the registration, a user gets an account by a scratch-off card or an e-mail via cell phone carrier.

Comparing with the ISP type, on the other hand, access points in self-managed type public wireless Internet access services can be malicious. In conventional self-managed services, mobile nodes are exposed to the threat that their communication being eavesdropped, manipulated or spoofed by some malicious access points.

2.3 Autonomous Distributed Model

In this paper, we propose autonomous distributed Internet access services — access points are managed by anyone with a broadband Internet access line; mobile nodes with accounts to any authentication infrastructure in the Internet can enjoy the access service through any of these access points.

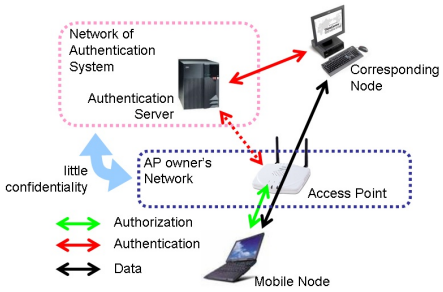

Figure 1: Autonomous Distributed Model

As the owners are not required to prepare authentication facilities, the management cost is very low. This encourages more people to provide this type of services. As the services in our proposed type is independent to any ISPs, anyone in the wireless coverage can obtain the Internet connectivity.

Our proposed model will be higher security level than that of the rest two models and lower management cost than the ISP model.

3. SECURITY REQUIREMENTS

Without authentication and encryption, security problem will be crucial. In this section, we first categorize security threats. Then we discuss some conventional security approaches and explain why these features are not applicable to the autonomous distributed public wireless Internet access services.

3.1 Threats

Because of one or more property of wireless, mobile or public, the following threats are possible.

- **To Wireless Mobile Nodes**
  i) Message eavesdropping by a malicious wireless node or access point.
  ii) Message manipulating and spoofing by a malicious wireless node or access point.

- **To the Internet**
  Falsely redirected messages, DoS Attack, SPAM / virus distribution by a malicious wireless mobile node.

- **To Access Points**
  Legal responsibility when some attacks with the source IP address access points assigned are detected.

3.2 Conventional Approaches

MAC address filtering, WEP and IEEE 802.1x are used for authentication and data encryption. However, none of the three solutions is enough for security and authentication purpose for public wireless Internet access.

A MAC address can be masqueraded through address spoofing, while the 40-bit WEP key can be broken in time [3, 4]. Moreover, the MAC address filtering and the WEP mechanisms lack user scalability. It is impossible to register MAC addresses to all the access point that every mobile node may visit; it is also impossible to share the secret key between the destination access point and the mobile node ahead of time.

The IEEE 802.1x is more secure but the centralized authenticate mechanism makes it more cumbersome and more expensive to implement.

Moreover, they are completely useless to keep the security of mobile nodes if an access point is malicious.

4. CATEGORIZATION OF AUTONOMOUS DISTRIBUTED PUBLIC WIRELESS SERVICE

In this section, we first demonstrate our design principle. Then we propose four secure models of autonomous distributed public wireless Internet access services.

4.1 Categorization Criterion

We design secure models using two approaches — data path and treatment of authentication transaction at access point.

Authentication Transaction at Access Point

Relayed Authentication processes at access points can reduce the chances of DoS attacks from malicious nodes, because if a mobile node has been successfully authenticated before, at least the mobile node is verified by some components.

Passed Through No authentication at access points can reduce the management cost. All what the access points have to do is to permit some specific VPN protocols to pass through.

Data Path

Tunneling A mobile node obtains an IP address from its VPN tunneling server. If any illicit use with the source IP address is detected, it is not an access point but the tunneling server who owes the responsibility.

Direct Direct communication between mobile nodes and their correspondent nodes enables optimal routing. For this, authentication mechanism has to be deployed on every probable corresponding node accessed by a mobile node.

By combining the two approaches with two options each, we classified the proposed models into four cases.

4.2 Models of Autonomous Distributed Public Wireless Service

4.2.1 *Passed Through Authentication, Tunneling Path (PATP) Model*

Figure 2 shows communication under PATP model.

In this model, an access point permits only packets of well-known VPN protocols to pass via itself. A mobile node, therefore, has to set up a VPN tunnel to its tunneling server. After that, all communications between the mobile node and corresponding node(s) in the Internet will go through with the tunnel. At this time, the source address a corresponding node is accessed from is derived by the tunneling server not by the access point. Obligations to identify the mobile node are therefore laid on the tunneling server not on the access point. In this meaning, this model can achieve a degree of security near a wired Internet access service. The only exception is transactions of setting up a VPN tunnel itself. In other words, a fear that an address derived by an access point is used for DoS attacks to VPN protocols remains.

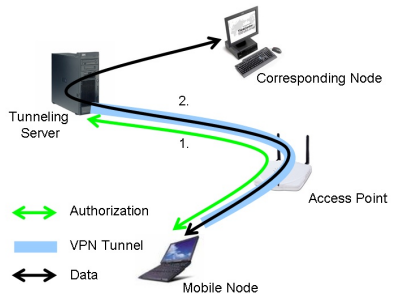

Figure 2: PATP Model

4.2.2 *Relayed Authentication, Tunneling Path (RATP) Model*

Figure 3 shows communication under RATP model.

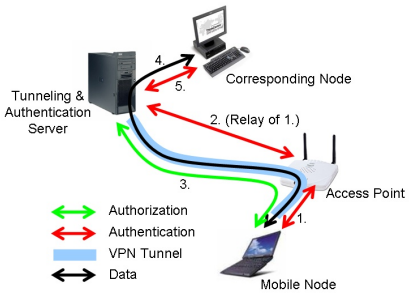

Figure 3: RATP Model

In PATP model, a communication to setup a tunnel itself is remained as a security weak point. In this model, in addition to the procedure in PATP model, an authentication is done by an access point. Only if the access point ensure that the mobile node is valid, the access point forwards a transaction for setting up a VPN tunnel. After that, the following communication procedure is as same as that in PATP model.

In this model, a mobile node has to show an access point that the mobile node is a valid client of an authentication

server. However, in autonomous distributed public wireless service model, confidential relationship between the authentication server and the access point cannot be assumed. Therefore, we have to avoid the possibility that the AP spoofs the MN with replay or other methods. For this reason, an authentication protocol is requested to be able for an AP to get only the result of authentication without account information itself.

4.2.3 *Passed-through Authentication, Direct Path (PADP) Model*

Figure 4 shows communication under PADP model.

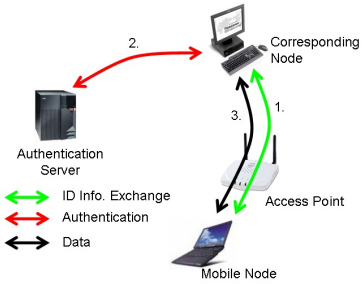

Figure 4: PADP Model

In this model, a mobile node notifies its identification information to a corresponding node in advance of sending a data packet. After the corresponding node ensures that the information is valid, the corresponding node accepts the following communications from the mobile node.

In this model, sender identification is based on the authentication relationship. In order to prevent forgery by an access point, the mobile node is recommended to append a signature to every packet.

As same as PATP model, however, there is a threat for an access point that a mobile node can send (malformed) identification information exchange packets to a corresponding node with a source IP address derived from the access point.

4.2.4 *Relayed Authentication, Direct Path (RADP) Model*

Figure 5 shows communication under RADP model.

In PADP model, there is possibility of DoS attacks to identification information exchange mechanism itself.

In this model, on the other hand, a mobile node adds its identification information to every packet for authentication by an access point and by a corresponding node. This can eliminate the possibility of above mentioned DoS attacks. From the viewpoint of a corresponding node and an authentication server, if an illicit use is detected, they can specify the sender in charge of each packet by tracing the identification relations. A mobile node cannot deny the responsibility at all.

5. CONCLUDING REMARKS

The rapid global diffusion of wireless public Internet is accelerated by the demand of ubiquitous Internet. Current

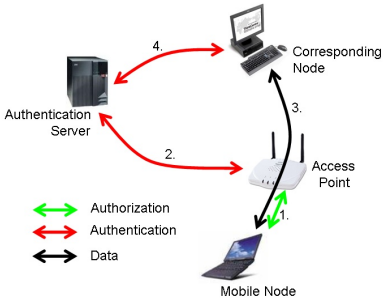

Figure 5: RADP Model

ISP models of wireless Internet access services are expensive to manage and do not scale. In the meantime, conventional self-managed model is not secure enough.

In this paper, we have categorized security problems that are specific or more crucial in public wireless Internet. Then we have discussed some secure models to meet the security requirement.

The proposed secure models can provide value for all the components in the autonomous distributed public wireless Internet. Mobile nodes and their correspondent nodes will benefit from the secure communication. Owner of the access points will benefit from providing public Internet access with low operation cost and minimum legal responsibility. The Internet will benefit from shifting to a secure ubiquitous communication environment with few DoS, virus and SPAM e-mails attacks.

Based on the idea described in this paper, we have started a new service, called MIAKO3 since May 2005, in our MIAKO.net [5] public wireless Internet service which consist of more than 100 access points around Kyoto, Japan. In MIAKO3 network, as a near-term solution, we employ pass through authentication transaction tunneling model.

6. REFERENCES

[1] Law concerning limitation of damages to specific telecommunications service provider and disclosure of sender information, 2002.

[2] A. Balachandran, G. M. Voelker, and P. Bahl. Wireless hotspots: current challenges and future cirections. In *Proc. of WMASH 2003*, 2003.

[3] N. Borisov, I. Goldberg, and D. Wagner. (in)security of the wep algorithm, 2001. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[4] D. Golombek. Single computer breaks 40-bit rc4 in under 8 days, 1996. http://catless.ncl.ac.uk/Risks/17.65.html.

[5] T. Komura, K. Fujikawa, and Y. Okabe. The miako.net public wireless internet service in kyoto. In *Proc. of WMASH 2003*, 2003.

[6] Y. Matsunaga, S. Merino, T. Suzuki, and R. H. Katz. Secure authentication system for public wlan roaming. In *Proc. of WMASH 2003*, 2003.