PISA: P2P Wi-Fi Internet Sharing Architecture

Tobias Heer, Shaohui Li, Klaus Wehrle
Distributed Systems Group
Computer Science Department
RWTH Aachen University
Email: [lastname]@cs.rwth-aachen.de

***Abstract*— The demand for cheap broadband Internet for nomadic users has created a market for Internet sharing. Wi-Fi communities which allow their users to share their wired Internet connections have emerged and become increasingly popular. Organizations like FON promise to provide free wireless Internet access in many places. However, user authentication is the Achilles heel of these systems. A user that allows other community members to use its access point must expect to be held responsible for other users' actions. Moreover, these Wi-Fi sharing systems are often insecure which allows eavesdroppers to gather sensitive information on the wireless link. This work provides efficient, scalable, and secure access control for large Wi-Fi sharing systems. The Host Identity Protocol (HIP) is used as a building block for a solution which supports strong user authentication as well as mobility support for nomadic users. In our presentation, we show the feasibility and effectiveness of this approach by demonstrating the PISA authentication protocol in action.**

I. Introduction

Nowadays, residential broadband deployment is spreading rapidly. In industrialized countries, there are nearly 200 million broadband Internet subscribers [1]. This ubiquity of wired Internet access stands in stark contrast to the limited availability of publicly accessible wireless access points. Mobile users are bound to use expensive commercial wireless hotspots which are mostly located in places like airports where a high density of customers is expected. The fact that many modern consumer network products are equipped with Wi-Fi allows communities of nomadic users to share their Internet connection and to use other users' Wi-Fi Internet routers in return. FON [2] is a company which has adopted this community idea as a business model. More than 160.000 FON members have already installed an access point and grant access to other FON members. FON members that provide an access point themselves can use any FON access point for free and, hence, use wireless Internet in many paces all over the world.

To allow easy Internet access over public access points, most Wi-Fi sharing systems use open 802.11 networks. Typically, Internet access is granted after a successful web-based authentication. The authentication process is secured by SSL but following transmissions are unprotected. This is problematic because neither confidentiality nor proper access control is guaranteed. Since all user traffic is sent over an unprotected wireless link, it is visible to any eavesdropper. However, the fact that the user authenticates by using a name and password might falsely imply a secure connection. Thus, private data like e-mails, login data, etc. might be exposed while using the access point. Moreover, the authentication mechanism is susceptible to identity theft. By spoofing the MAC and IP address of an authenticated user, attackers can send and receive traffic on behalf of that user, which allows attackers to covertly use the access point. A serious issue for access point owners is related to this weakness in access control. Depending on the local law and the contracts of commercial broadband service providers, the owner of an access point is responsible for illegal traffic associated with its IP.

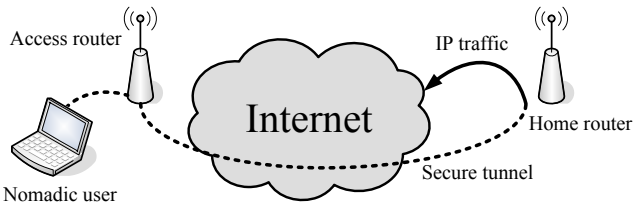

Fig. 1. The PISA model uses the *home router* as a traffic relay.

II. The Wi-Fi P2P Internet Sharing Architecture

To overcome the shortcomings of the current Wi-Fi-sharing models, a system that allows for encryption of user traffic and strong authentication of users is required. We propose PISA, a *secure P2P Internet Sharing Architecture* that, firstly, enables Wi-Fi sharing without legal issues for access point providers and, secondly, offers security for mobile users. Similar to existing Wi-Fi sharing models, users contribute to the system by allowing other users to use their access points. What makes PISA different is the use of a second router: the router which is owned by the mobile user. We denote this router *home router* because it is typically located in the mobile users' homes. This router acts as an endpoint of an encrypted tunnel to the mobile device. A mobile user that sends data to the Internet uses this tunnel. Therefore, the traffic which is visible to Internet hosts originates from a user's *home router*. This solves all legal issues because owners of a router are only responsible for their own traffic. Using an encrypted tunnel between the mobile device and the *home router* also solves the problem of eavesdropping because all Wi-Fi traffic is encrypted. The basic setting of PISA is depicted in Figure 1.

The access points over which mobile users can connect to their *home routers* are denoted *access routers*. These routers are responsible for verifying the identity of a *home router* and, thus, the identity of the mobile user. The *access router* must also verify that the user belongs to the Wi-Fi community before allowing IP traffic to traverse the tunnel.

PISA utilizes the *Host Identity Protocol* (HIP) [3], [4] in

0-7695-2986-0/07 $25.00 © 2007 IEEE
DOI 10.1109/P2P.2007.12

IEEE computer society

order to achieve end-to-end encryption and authentication. HIP creates a new namespace above the IP layer, the Host Identity (HI) namespace. Host Identities are cryptographic identifiers that are based on asymmetric keys. A HIP communication begins with a handshake phase in which both communicating hosts mutually authenticate and set up an encrypted IPsec tunnel. During the ongoing communication, HIP can update the IP addresses of a host, which allows for end-host mobility. PISA delegates the task of end-host authentication and creating an encrypted tunnel to HIP. However, it needs to extend HIP in order to adapt it for the task of Wi-Fi-sharing authentication.

To set up a connection to the *home router*, the mobile user initiates a HIP handshake with it. The *access router* forwards and observes the HIP handshake between the mobile device and the *home router*. HIP was designed to allow mutual authentication of end-hosts. Middleboxes like the routers in PISA can observe the HIP handshake and use the public keys in the handshake to authenticate the communicating end-hosts. However, as the middleboxes do not participate actively in the handshake, a malicious *home router* that collaborates with a mobile device can replay previously recorded HIP handshakes and, hence, undermine the HIP authentication on the middlebox. Thus, PISA middleboxes must actively take part in the handshake to be able to verify its timeliness and authenticity. PISA allows *access routers* to add a nonce to the handshake messages which both, the *home router* and the mobile client must process and sign.

The *access router* operates as a packet filter that drops all non-PISA traffic and only lets HIP traffic to *home routers* pass through. Before allowing traffic to pass, *access routers* must verify that the user belongs to the Wi-Fi community. It does this indirectly by verifying that the *home router* is part of to the Wi-Fi community. This is done to ensure that illegal actions relate to the a *home router* that the community has approved. The membership in the Wi-Fi community is proven by a certificate that contains the HI of the *home router*. This certificate is sent from the mobile device to the *home router* and, thus, is also visible to the *access router*. The Wi-Fi community is represented by a Certificate Authority (CA) that can create such certificates. The registration of the *home router* requires to contact this central instance but after the registration, PISA works completely decentralized.

In addition to PISA's basic mode of operation, further features which enable seamless mobility between different *access routers* and data compression between the *mobile router* and the *home router* to mitigate the effects of asymmetric links are possible. To allow mobility, the *access router* must be able to gather all required authentication information not just from the HIP handshake but also from HIP update messages. Compression is necessary because most home-user broadband connections use an asymmetric distribution of bandwidth between up- and downlink. Thus, the uplink speed of the *home router* limits the downlink speed of the mobile host. PISA uses data compression to increase the throughput on such asymmetric links.

PISA also supports a mode that does not require a tunnel to the *home router* in order to avoid *triangular routing*. In this mode, the *access router* acts as a tunnel endpoint. The benefit of using HIP and its cryptographic identities is that community members can not read encrypted HIP traffic and that the identity of hosts can be determined in case of fraudulent use. The mapping between real world identities (the owners of a home routers) and the HIs of a mobile users can be created by letting the home router sign the mobile users' HI. This allows the *access router* to relate mobile users' traffic to their home routers and, therefore, –via the community certificate– to the owners' identities without the need to contact the *home router*.

III. Demo Presentation

In the presentation, we will show the feasibility and effectiveness of our approach by demonstrating a prototype of the PISA. We use the *HIP for Linux implementation* (HIPL) as a basis of our work. HIPL has been extended to allow appropriate access control and authentication for PISA. The demonstration will show a mobile client that connects to the Internet over a *home router* located off site. We modified two consumer routers as *home* and *access router* to demonstrate the feasibility of our approach in practice. The routers are capable to run OpenWrt[5], a lightweight Linux distribution for embedded devices, especially wireless routers.

We will demonstrate the distributed authentication protocol which forms the core of PISA. All steps will be visible from the output of the *access router*. Additionally we will show the perspective of the HIP instances on the mobile device and the *home router*. During a slowed down connection establishment we will discuss the necessity and intent of our HIP modifications. The demo will also show the view of an attacker. Although the attacker is able to observe the HIP handshake it can not read the IPsec-encrypted payload.

IV. Conclusion

PISA solves the shortcomings of today's Wi-Fi sharing systems and enables additional features like mobility. PISA operates in a peer-to-peer fashion in which every user contributes bandwidth but still uses its own network infrastructure for Internet access. Its redirection approach closes security loopholes and resolves legal issues by utilizing the Wi-Fi router at a mobile user's home. Thus, illegal use of Internet resources can be traced to the address of misbehaving users.

References

[1] Organisation for Economic Co-operation and Development: OECD Broadband Statistics 2006. Website. Retrieved May 19, 2007. ⟨http://www.oecd.org/sti/ict/broadband⟩

[2] Fon wireless Ltd.: FON: Perspektive - Wachstumsmanagement vordringlich. Website in German. Retrieved May 19, 2007. ⟨http://blog.fon.com/de/archive/business/fonperspektive-wachstumsmanagement-vordringlich.html⟩

[3] Moskowitz, R. and Nikander, P. and Jokela P. and Henderson P.: Host Identity Protocol (HIP) Architecture. RFC 4423, Internet Engineering Task Force, May 2006.

[4] Moskowitz, R. and Nikander, P.: Host Identity Protocol. draft-ietf-hip-base-07. IETF Internet draft. Feb. 2007. Work in progress.

[5] The OpenWrt project. Website. Retrieved May 19, 2007. ⟨http://openwrt.org⟩