Secure Wi-Fi Sharing at Global Scales

Tobias Heer, Stefan Götz, Elias Weingärtner Klaus Wehrle
RWTH Aachen University
Distributed Systems Group
{heer, goetz, weingaertner, wehrle}@cs.rwth-aachen.de, oscar.garcia@philips.com

Abstract

The proliferation of broadband Internet connections has lead to an almost pervasive coverage of densely populated areas with private wireless access points. To leverage this coverage, sharing of access points as Internet uplinks among users has first become popular in communities of individuals and has recently been adopted as a business model by several companies. However, existing implementations and proposals suffer from the security risks of directly providing Internet access to strangers. In this paper, we present the P2P Wi-Fi Internet Sharing Architecture PISA, which eliminates these risks by introducing secure tunneling, cryptographic identities, and certificates as primary security concepts. Thus, PISA offers nomadic users the same security that they expect from a wired Internet connection at home. Based on its three fundamental mechanisms, PISA achieves a flexibility which opens significant advantages over existing systems. They include user mobility, anonymity, service levels with different performance and availability characteristics, and different revenue models for operators. With this combination of key features, PISA forms an essential basis for global, seamless, and secure Wi-Fi sharing for large communities.

1 Introduction

At the same time, the proliferation of wireless access points (APs) has lead to a dense coverage of urban areas with private wireless Internet gateways. Despite these facts, broadband Internet is rarely available to nomadic users because few access point owners are willing to altruistically open their gateways to others and to accept the ensuing security and liability risks.

Thus, mobile users need to rely on expensive commercial wireless services typically only available at points of interests such as airports. Cell-based technologies, such as EDGE or UMTS, do not offer enough throughput for medium- to high-bandwith applications, e.g., media-rich websites, streaming video at good resolutions, or file sharing.

These shortcomings have motivated Wi-Fi sharing communities in which a mobile member may access another member's residential broadband connection via their wireless access point. Originating in grass-root movements such as PTP [15] and Freifunk [4], companies like FON [3] and Wippies [14] commercialized this concept. They offer customized IEEE 802.11 access points that exclusively grant Internet access to members of the community.

Although Wi-Fi sharing communities are flourishing, they are still far from the vision of low-cost, continuous, ubiquitous, decentralized, and secure Internet access, because they do not meet the key requirements outlined below. For the remaining discussion, we refer to the following names as the elements of a Wi-Fi community (cf. Figure 1). The *User Access Point* (UAP) is the AP located at a community member's home. A *Mobile Guest* (MG) is a nomadic member who accesses the Internet via another user's AP, which thus is the MG's *Host Access Point* (HAP). The term *community operator* CO refers to the private or commercial entity that represents the community, i.e. manages member accounts and hosts central services (e.g., for authentication). The terms *user* and *member* are used interchangeably.

Security: One cannot assume community members to be trustworthy. Thus, while MGs demand the same amount of communication privacy and integrity when at their UAP at home and at a HAP when travelling, they cannot trust the HAP to provide this. Similarly, owners of HAPs expect their service not to be significantly degraded by MGs or to be held liable for an MG's actions.

Anonymity: When using mobile communication technology, people risk exposing parts of their life, such as their location, working times, and mobility, to service providers. For acceptance with privacy-conscious users, HAPs should not be able to glean information about the identity of an MG from its communication and MGs should not be traceable when roaming.

Mobility: Locally roaming users should be able to move between different HAPs with seamless connectivity,

978-1-4244-2036-0/08/$25.00 ©2008 IEEE

e.g. for such existing applications like Wi-Fi-based SIP phones. Besides being able dynamically use different HAPs while moving, support for persistent transport-layer connections is essential to prevent established connections from breaking when moving from HAP to HAP. At the same time, global roaming needs to be supported so users are not restricted to any specific geographical area.

Economic Aspects: Today's Wi-Fi sharing communities suffer from a restricted flexibility in their business models. They cannot specifically target their systems at private or commercial AP operators or mobile customers with kickbacks or incentives. Also, it is neither technically possible nor financially attractive to provide different levels of service based on the identity or location of users.

Scalability: The Wi-Fi sharing architecture needs to scale well at the AP and system levels with large numbers of registered users and consequently with the number of active network connections and the amount of local and global bandwidth usage.

Availability and Performance: The architecture needs to grant users Internet access via HAPs even if their UAP is temporarily unavailable. Also, MGs should be able to receive high-bandwidth and low-latency service at HAPs independent of other system components such as their UAP.

In [6], we outline the concept of a secure network tunnel between an MG and its UAP to fulfill the aforementioned security requirements. This paper significantly extends that idea to meet all of the above requirements necessary for a secure and flexible service that enables global Wi-Fi sharing.

The paper is organized as follows. Section 2 presents related work and discusses several related security issues. Section 3 introduces our P2P Wi-Fi Sharing Architecture PISA. Section 4 revisits the previously stated requirements and Section 5 concludes.

2 Related Work

Several commercial COs, such as FON [3] or Wippies [14], offer global Wi-Fi sharing services to substantial numbers of members (e.g. 700.000 for FON). Technically, these operators provide their customers with access points that are typically customized with a software called Chilispot [8]. It presents an MG with an authentication interface that is backed by the operator's RADIUS [12] server for IEEE 802.1x authentication. Although the authentication is secure, this scheme suffers from the following security risks:

Firstly, the HAP acts as ingress point to the Internet for the MG's traffic. By intercepting MG traffic at the Internet uplink of the HAP, the confidentiality and integrity of the guest's communication can be compromised. Consequently, MGs are prone to attacks such as eavesdropping, impersonation, or forgery. Even when using application-layer security protocols, e.g. TLS or SSL, only informed and attentive users can detect and avoid man-in-the-middle attacks against services such as online banking website. Furthermore, HAPs can be easily compromised or faked and then used to intercept the authentication procedure of MGs and to learn their credentials.

Secondly, to the outside world the owner's and guest's traffic are indistinguishable so the owner of a HAP may face legal liability for malicious guest traffic caused by the MG.

Efstathiou and Polyzos [2] propose an incentive system to counter free-riding in Wi-Fi sharing. However, their work does not address the network security aspects identified above.

Recently, two schemes have been presented that employ authenticated and encrypted tunnels between an MG and the corresponding user AP to avoid the security risks of existing systems. With tunneling, MGs gain communication integrity and privacy while for communication partners the MG application traffic appears to originate at the tunnel endpoint, thus avoiding legal liability for MG traffic at HAPs.

One such scheme, as proposed by Sastry et al. for city-wide Wi-Fi sharing communities [13], fixedly assigns each member an address from a private IPv4 address block used in the NATed wireless networks at HAPs. These addresses serve as identities, so when an MG visits a HAP, the HAP uses this address to look up member information in a trusted community directory. This information contains the user AP associated with the given MG address based on which the HAP only routes VPN packets between the MG and its UAP, thus enforcing the tunneling. Impersonation at the level of the IPv4 addresses is ineffective if UAPs authenticate connection attempts and only accept tunnels from their corresponding MGs.

Beyond this basis, Sastry et al. do not address challenges such as privacy and anonymity concerns or the flexibility in commercial settings. A central shortcoming is the use of IPv4 addresses as identities, which tightly limits the number of members in a Wi-Fi sharing community to urban scales and hampers the inter-community mobility of users. Furthermore, mobile users cannot use the sharing service if their UAP is not reachable for any reason. Note that this is not a strong incentive against free-riding, i.e., selfishly using the system (other members' HAPs) without contributing to it (granting other members access to one's own AP). For an AP, acting as a tunnel endpoint is orthogonal to providing shared Wi-Fi to other mobile users, and the latter can be prevented trivially, e.g. by removing the AP antenna.

The other tunneling-based scheme for Wi-Fi Sharing is an early version [6] of our PISA architecture. The remaining sections of this paper discuss a significantly advanced architecture and how it exceeds previous work to meet the

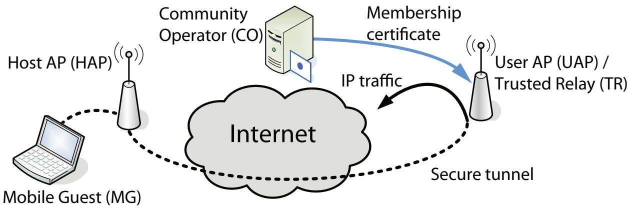

Figure 1. The elements of the PISA Wi-Fi sharing model

requirements we identified in Section 1 for a secure, practical, and economically viable Wi-Fi sharing model.

3 PISA Design

This section details the rationale and design of our Peer-to-peer Wi-Fi Internet Sharing Architecture *PISA* and its integration of the Host Identity Protocol [10, 9]. We focus the security and operational challenges and possibilities PISA faces, whereas P2P aspects are omitted for brevity's sake.

3.1 Trust Relationships in Wi-Fi Sharing

The entire design of PISA is motivated by the concept of trust relationships formed between the entities involved in a Wi-Fi sharing community. As depicted in Figure 1, the four entities of interest in PISA are the *MG*, the *UAP* at the home of a MG, the *HAP*, and the CO. We discuss their trust relationships and show how PISA incorporates cryptographic identities and secure tunnels between MGs and trusted relay points in order to form a secure Wi-Fi sharing architecture.

In a common Wi-Fi sharing network, each entity individually trusts the CO, and hence, all entities, i.e MG, UAP, and HAP form independent trust relationships with the community operator. On the basis of transitivity, a mutual trust relationship between the HAP and the MG is deducted. A common issue in established Wi-Fi sharing models is the assumption that this transitive trust relationship is sufficient for secure Wi-Fi sharing. However as pointed out in section 2, various existing security threats evidence that this trust relation does not allow to enforce security, within a system of unknown principals. In fact, this trust relationship between the CO and the community members only states that the other principal is part of the community. It cannot guarantee that the principal will act securely and reliably as expected. Moreover, if potentially insecure authentication mechanisms, such as plain passwords, are used, the trust link between both is even weaker. In this case, the identity of a principal can not be assured unambiguously. Finally, a strong trust relationship exists between a MG and its UAP as both are under the same administrative control. However, established Wi-Fi sharing communities are not using this trust relationship.

3.2 Trust Relationships in PISA

In addition to the usual, transitive chain of trust between the HAP and the MG, PISA leverages the strong trust relationship between the UAP and the MG. We use the UAP as a *Trusted Relay* (TR) to the Internet. A MG establishes an encrypted tunnel to its UAP and tunnels all its traffic to the UAP from where it is relayed to the Internet.

Tunneling to TRs removes the imbalance in the trust relationship between the MG and the HAP, that is imposed by existing Wi-Fi sharing systems. Since the HAP only forwards encrypted packets to the MG's UAP, it cannot interfere with the payload of the tunnel in any harmful way. In the following, we briefly highlight the new trust relationships.

From the perspective of the MG, the resulting chain of trust starts with the MG, which trusts the HAP only as far as that it will forward its encrypted packets to the UAP. The MG fully trusts its UAP, which can satisfy all trust requirements. Considering the MG, the weak trust relation between the CO and the HAP is not even required as the MG is the only beneficiary when using the HAP.

From the viewpoint of the HAP, it only requires that the UAP at a MG's home provides service to other community members. The transitive trust relationship between the HAP, the CO, and the UAP can fulfill this requirement because the CO can attest community membership to the UAP. There is no trust relationship between the MG and the HAP required because the UAP acts as ingress node to the Internet and thus will be held responsible for illegal actions of the MG. Therefore, using secure tunneling untangles the trust relationships and ensures that all trust relationships can fulfill their purpose.

So far we have considered the MG's UAP as the only option for relaying traffic. However, this service can also be provided by other parties, e.g. commercial service providers. These can offer services to users without UAP and can provide larger bandwidth and higher reliability than most UAPs. In Section 4.4 we discuss how both, the community and the commercial providers, can gain economic benefit from commonly using the community network. From now on we will use the term *Trusted Relay* (TR) when referring to the entity that accepts the MG's tunnel and relays its traffic regardless whether it is a private user's UAP or a commercial traffic relay.

3.3 Tunneling, Cryptographic Identities, and Certificates

In order to establish and verify the trust relationships discussed in Section 3.1, PISA uses three cryptographic techniques: secure tunneling, cryptographic identities, and certificates. In PISA, each entity (or principal) is identified by a cryptographic identity, represented by the public key of a public-private key pair. A host proves its identity by signing data with its private key, so it can be verified via its public key. Since we assume that a TR knows the identities of all MGs that are authorized to use it and vice versa, the trust binding between MGs and their TRs is ensured by mutual authentication based on these identities.

The CO, and thus, the Wi-Fi community is represented by a Certificate Authority (CA). We assume that every entity participating in the Wi-Fi community is aware of the public key of the CA, and hence can verify certificates issued by the CA. A certificate is linked to a digital identity by containing a signature of its owner's identity. In PISA, all TRs receive certificates from the community CA as verifiable proof of their membership.

When an MG associates with an HAP, the HAP allows the MG to establish a secure tunnel to its TR. During this establishment phase, the HAP verifies the membership of the TR to prevent free-riding. If the tunnel is successfully created, the HAP permits encrypted tunnel payload to be exchanged between the MG to the TR. If the tunnel setup fails, the HAP must assume that the TR is not willing to forward traffic for the TR. Therefore, the HAP blocks all tunneled traffic from the MG. Since the HAP does not depend on learning the identities of MGs and TRs, the implementation should avoid their disclosure to the HAP to allow users to stay anonymous.

In our implementation, we leverage well-understood standard mechanisms to realize the PISA design. For secure tunneling, IPSec is a natural choice as it provides the necessary integrity protection and encryption features. A perfect match to gain cryptographic identities and IPSec signalling is the Host Identity Protocol (HIP).

3.4 The Host Identity Protocol

PISA uses the Host Identity Protocol for establishing and maintaining the IPsec tunnel and for authenticating the participating parties. HIP is a signaling protocol for secure communication, mobility, and multihoming, which we briefly outline in this section.

HIP introduces a new namespace that uses self-certifying cryptographic identities to address hosts. These *Host Identities* (HIs) consist of RSA or DSA public keys. Thus, a host can prove that it is the legitimate owner of a HI by using the corresponding private key. This *Host Identity Namespace* is used by the transport layer and all layers above. Logically, HIP resides between the network and transport layers and maps IP addresses to HIs and vice versa via a distributed address resolution service.

When creating a new HIP connection, both hosts establish an IPSec tunnel that protects the payload exchanged between the hosts. If a mobile host moves to a different network location and is assigned a new IP address, HIP changes the mapping between IP addresses and HIs dynamically. HIP also adjusts the tunnel endpoints accordingly, redirecting the encrypted payload flow to the new location of the mobile host. Like all HIP addressing, this change is transparent to the transport and application layer because it uses HIs instead of IP addresses. HIP was designed to be incrementally deployable and compatible with the existing Internet infrastructure and non-HIP-aware legacy applications.

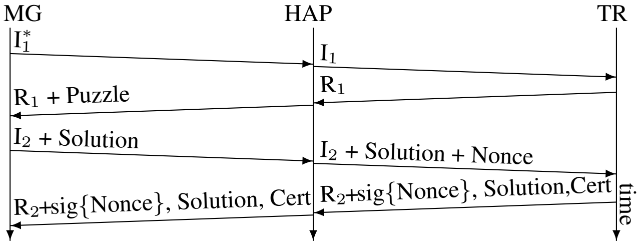

Figure 2. The PISA authentication process.

We use HIs as identities for the MG and its TR in order to facilitate a strong mutual authentication of both parties. Moreover, the community certificate of a TR contains its HI, enabling HAPs to verify the community membership of the TR.

3.5 Integration of PISA and HIP

We tightly integrate the PISA authentication process with the HIP protocol to avoid the latency incurred by additional message exchanges.

The HIP handshake is a four-way handshake during which the *initiator* of the handshake and its peer, the *responder*, authenticate each other and set up an encrypted tunnel. The standard HIP handshake is insufficient for proving the identity of the TR to the HAP. Hence, to enable the HAP to authenticate the TR, we transform HIP's two-party authentication into a three-party authentication process, involving the HAP. For the sake of conciseness, we only discuss the packet contents, parameters, and HIP functions that are important for PISA.

Figure 2 illustrates the modified HIP handshake. The four HIP handshake packets are denoted as I_1, R_1, I_2, R_2. The letters I and R indicate the origin of the message: initiator or responder. In PISA, the MG always acts as the initiator and the TR always acts as the responder.

The first packet from the MG to the TR, the I_1 initiates the HIP handshake. PISA does not modify it as the I_1 was designed to not require costly computations, e.g. public key signatures, or state establishment from the responder to prevent Denial-of-Service (DoS) attacks. When sending the I_1 message, the MG might not know the IP address of the TR. In this case, the MG leaves the address resolution to the HAP, which queries the HIP address resolution structure (e.g. a rendezvous server or the DNS system).

The actual authentication of the TR is performed in the I_2 and R_2 message. When the HAP receives the I_2 packet, it adds a nonce and forwards the packet to the TR. When the TR receives the I_2 message, it performs the usual HIP processing and adds the nonce and a signature of it to the R_2 packet. When the R_2 packet reaches the HAP, it verifies the nonce signature to verify the identity of the TR and to prevent replays. The HAP also verifies the membership of the TR by verifying the community certificate and then forwards the packet to the MG, which performs the regular HIP processing on it. The HAP lets MG payload traverse only after successful TR authentication. The HAP does not authenticate the MG, allowing this principal to stay anonymous.

The computational complexity of public-key algorithms can be exploited such that an attacker may be able to make a victim perform large numbers of cryptographic operations to exhaust their CPU resources. To frustrate such attacks on the HAP, we integrate the well-known technique of client puzzles [1]. When a HAP suspects an attack, it may add a puzzle to the PISA handshake. As requester of the handshake, the MG is required to solve the puzzle and to forward the solution to the TR, which attaches the solution to the R2 packet. The HAP can verify that the requested amount of computation has been performed by checking the puzzle before verifying the signature and the certificate.

PISA leverages the HIP mobility support to allow MGs to move between HAPs. For PISA, we extend HIP's address update process by TR authentication in a fashion analogous to the base exchange modifications described above. Further details are given in [5].

3.6 Implementation

We created a prototype of the design which encompasses the MG client, the HAP, and the TR and which is based on the *"HIP for Linux"* [7] implementation. Our implementation supports authentication of MGs and TRs, the establishment of the secure HIP tunnel, MG mobility between HAPs, and handling of community certificates. We successfully tested this implementation on Linux systems and commodity router hardware running OpenWRT, specifically the "La Fonera" and the Netgear WGT634U.

4 Evaluation

This section compares PISA to other Wi-Fi sharing models, in particular the one proposed by Sastry et al. because the concept of tunneling is present in both approaches. We evaluate PISA by revisiting the requirements stated in section 1. In the end of this section we present our implementation of PISA and provide a brief performance evaluation.

4.1 Security

PISA appropriately models the trust relations analyzed in section 3.1 by utilizing secure tunneling, cryptographic identities, and certificates. Thus, it overcomes the security issues of conventional Wi-Fi sharing communities.

Secure tunneling prevents attacks from the HAP, and as this entity only forwards encrypted traffic, it cannot eavesdrop or impersonate the MG. This also avoids the struggle of current Wi-Fi sharing operators to make APs tamper proof. In PISA, we assume that the TR does not eavesdrop on the user's traffic and does not mount impersonation attacks. This assumption is based on the similarity to the trust relationship all users share with their own AP at home and their Internet service provider.

Because Sastry's approach is also tunnel-based, PISA does not provide additional security, however PISA proves to be more flexible and scalable, as discussed in the next sections.

4.2 Anonymity

When users authenticate towards unknown parties (i.e., HAPs or TRs), attacks on a user's privacy become possible. Apart from learning a user's identity, other potentially sensitive information, like their working times, location, or mobility, can be derived from their network usage.

Conventional Wi-Fi sharing models require users to register with their real-world identities to the Wi-Fi CO. This is necessary to enable access control on the HAPs. Moreover, a guest's identity is revealed to HAPs so they can log the actions of the user. Thus, users become traceable.

In contrast to conventional Wi-Fi sharing, the system of Sastry et al. does not require the HAP to learn the identity of the guest. However, due to the fixed internal IP addresses that are assigned to each MG, it can be identified and recognized by a HAP. Obfuscating this direct mapping by assigning numeorous addresses to each guest would increase privacy but significantly reduces the amount of available addresses, making it impossible to reach a global scale (c.f. Section 4.5).

PISA allows to conceal the digital identity of an MG from the HAP. Parameters in the handshake packets that relate to an MG's identity are transferred in encrypted form. Only the TR needs to authenticate the nomadic user, however, it is expected to not misuse this information. It is not necessary for the CO to know the real-world identity of a user or of a TR operator. As only the TR must expect legal consequences for an MG's actions, it is only necessary that the TR can identify the guest. The CO and the HAP only need to be sure that the TR contributes to the system in some way by sharing bandwidth, or by providing other compensation.

4.3 Mobility

While systems like FON do not support mobility, Sastry et al. briefly discuss requirements but only sketch a possible solution for enabling mobility.

PISA relies on the separation of a host's identity from its point of network attachment for mobile host support. Especially in urban areas with many obstacles, the limited IEEE 802.11 signal propagation requires frequent handovers from AP to AP. PISA manages mobility by maintaining the tunnel between the MG and the TR in the face of guest mobility. Hence, ongoing transport-layer connections, e.g. VoIP calls and downloads, survive user mobility. PISA leverages the mobility support of HIP and extends it with authentication capabilities for enabling the HAP to verify the community membership and identity of the TR. The TR is stationary and thus represents a fixed Internet ingress point. In this sense, the TR acts very much like the home agent in mobile IP. To the best of our knowledge, PISA is the first community Wi-Fi sharing system that implements mobility.

4.4 Economic Aspects

Companies like FON primarily rely on revenue from selling access privileges to non-community-members. More fine-grained billing schemes based on, e.g., access time or used bandwidth, require reliable accounting of service usage. However in a FON-like system, the user traffic does not traverse systems directly operated by the CO, which thwarts central logging and accounting. Decentralized logging and accounting via all HAPs is also not possible because HAPs cannot be trusted by the CO to reliably deliver accurate and correct logging data.

The design by Sastry et al. does not address this issue because it only uses tunnels to UAPs.

PISA allows the CO to offer Internet access to mobile users that do not operate a UAP. In order to do so, these users can be charged for using a commercial TR operated by the CO. As for such users all traffic is tunneled to a TR controlled by the CO, fine-grained access control and accounting is possible. The trust relation between an MG and the CO-managed TR are similar to the trust relations between a broadband subscriber and its Internet provider. The CO-managed TR can log the traffic of the user, and thus, can hold the user accountable for illegal actions. Logging by a CO-operated TR is fundamentally different from the logging on the HAPs in current Wi-Fi sharing communities because users typically trust a CO but not a HAP.

4.5 Scalability

Current Wi-Fi sharing models are able to provide a well performing global service without supplementary infrastructure at the cost of system security and privacy.

The system proposed by Sastry et al. targets citywide deployment and was designed with this limitation in mind. The centralized way of maintaining the mappings between nomadic users and their APs at home makes it difficult to distribute the system. Moreover, the IPv4-based access control restricts the number of available mappings, and thus, the number of users to approximately 16.8 millions, which might turn out problematic for global usage.

When operating PISA on a global scale, tunneling traffic through a user's remote UAP can substantially increase the end-to-end latency experienced by the user. Such an increase may be acceptable for web-browsing but it is prohibitive for real-time applications like VoIP calls. However, PISA naturally supports the deployment of TRs at core network hubs close to MGs, avoiding the triangle routing via UAPs.

Moreover, the concept of digital certificates in PISA avoids the need for a single global authority for managing user accounts or resources. Thus, multiple organizations and companies can safely act as COs, with each one being represented by its own certificate authority in a hierarchy of CAs This CO neutrality helps to create competition among COs and to accelerate the global deployment of PISA.

4.6 Availability and Performance

The service availability and quality in conventional Wi-Fi sharing communities solely depends on the service offered by the HAP and the availability of the authentication server. Thus, there is no increased latency or bandwith degradation other than the one imposed by the Internet connection and the forwarding policies of the HAP.

Sastry's approach and PISA use tunnels to remote relays. Hence, the quality of service depends on the HAP and the relay. The concept of Sastry is limited to using the UAP for tunneling. Despite the advantages of a UAP as a trusted relay, this choice has the following drawbacks: First, a temporarily unavailable UAP immediately shuts a member off from Internet access at any HAP. Second, the triangle routing [11] problem and the poor UAP uplink bandwidth, which is typical for asymmetric broadband technologies, can incur a significant increase in latency and decrease of throughput.

PISA natively integrates trusted relays that are operated by COs for offering lower latency, higher bandwidth, or a more reliable service than UAPs alone can provide. By dynamically selecting the best available TR, it is possible to use such TRs as fallback whenever the UAP is unavailable

Table 1. DSA and RSA performance with 1024-bit keys.

	AR2315	Broadcom 5365
DSA 1024 bits	51.0 ms	63.7 ms
RSA 1024 bits	4.4 ms	5.6 ms

or if its resources do not suffice the required quality of service. The use of cryptographic identities and certificates aids the TR selection because TRs can delegate their responsibility to other TRs by means of certificate chains.

In contrast to existing Wi-Fi sharing communities, PISA requires the HAP to verify the community certificate and the identity of the TR by means of public-key cryptography. We evaluate the performance of public-key verification to underline the feasibility of our approach by measuring the DSA and RSA verification time using commodity hardware that is widely used as APs in community Wi-Fi sharing networks: The “La Fonera” wireless router with a 180 MHz Atheros AR2315 32-bit MIPS CPU and the Netgear WGT634U with a 200 MHz Broadcom 5365 MIPS-32 based CPU. Table 1 displays the measurement results. For each PISA association, the HAP needs to compute two public-key verifications. Even when using the slower DSA verification, both APs can handle more than 15 verifications per second, which is sufficient for processing frequent PISA authentication.

5 Future Work and Conclusion

Based on the discussed design, we are currently deploying our implementation of PISA in a university-wide testbed to gain experience with a realistic environment and to obtain more evaluation results. In this paper, we analyze the trust relationships in Wi-Fi sharing models as a basis for the design of the PISA architecture. This architecture eliminates the security risks of existing Wi-Fi sharing systems and provides several key advantages to users and operators.

PISA enables secure, decentralized Wi-Fi sharing without burdening Access Point owners with an unclear legal situation. Moreover, PISA provides a level of security for nomadic users that is at least equivalent to the security that users expect when using their Internet connection at home. Our architecture also ensures the privacy and anonymity of community members and provides protection against user tracking. With built-in mobility support, PISA bridges the isolated AP domains to enable seamless connectivity for mobile users. Overall, we address authentication, confidentiality, and integrity of communication at a fundamental level instead of applying ad-hoc measures. This forms the basis for a throughout reliable and secure system which is extremely flexible with regard to how it can be used and operated by private users, communities, and businesses.

6 Acknowledgments

We thank Shaohui Li and Miika Komu for supporting the PISA implementation and Christian Beckel, Thomas Jansen, and Raimondas Sasnauskas for their assistance on the paper.

References

[1] T. Aura, P. Nikander, and J. Leiwo. DoS-Resistant Authentication with Client Puzzles. In *Revised Papers from the 8th International Workshop on Security Protocols*, pages 170–177, London, UK, 2001. Springer-Verlag.

[2] E. Efstathiou and G. Polyzos. A self-managed scheme for free citywide Wi-Fi. *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 502–506, 2005.

[3] FON WIRELESS, Ltd. FON website. [Online] Available http://www.fon.com/, January 8, 2008.

[4] Freifunk Community. Freifunk. [Online] Available http://infrahip.hiit.fi/ January 8, 2008.

[5] T. Heer. End-Host Authentication for HIP Middleboxes. Internet-Draft draft-heer-hip-midauth-00, Internet Engineering Task Force, Nov. 2007. Work in progress.

[6] T. Heer, S. Li, and K. Wehrle. PISA: P2P Wi-Fi Internet Sharing Architecture. *P2P 2007. Seventh IEEE International Conference on Peer-to-Peer Computing*, pages 251–252, 2-5 Sept. 2007.

[7] InfraHIP Project. InfraHIP Project: HIPL. [Online] Available http://start.freifunk.net/ January 8, 2008.

[8] J. Jakobsen. Chillispot website. [Online] Available http://www.chillispot.info/, January 8, 2008.

[9] R. Moskowitz. Host Identity Protocol (HIP) Architecture. RFC 4423, Internet Engineering Task Force, May 2006.

[10] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. Internet-Draft (work in progress) Version 10, IETF, Oct. 2007.

[11] C. E. Perkins and D. B. Johnson. Route Optimization for Mobile IP. *Cluster Computing*, 1(2):161–176, 1998.

[12] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865 (Draft Standard), June 2000. Updated by RFCs 2868, 3575, 5080.

[13] N. Sastry, J. Crowcroft, and K. Sollins. Architecting Citywide Ubiquitous Wi-Fi Access. In *Proceedings of ACM SIGCOMM HotNets (HOt Topics in Networks)*, Atlanta, Georgia, 14-15 Nov 2007.

[14] Saunalahti Group Oyj. Wippies — Join the Wireless Hippies. [Online] Available http://www.wippies.com/, January 8, 2008.

[15] The Personal Telco Project. Personal Telco Project Site. [Online] Available http://www.personaltelco.net/ January 8, 2008.