PISA-SA - Security and Mobility in a Collaborative Muni-Fi

René Hummen, Hanno Wirtz, Nicolai Viol, Tobias Heer, and Klaus Wehrle
Communication and Distributed Systems
RWTH Aachen University
Germany
{hummen, wirtz, viol, heer, wehrle}@cs.rwth-aachen.de *

1. INTRODUCTION

Municipal Wi-Fi (Muni-Fi) networks aim at providing city-wide wireless access to selected city services for a variety of users. Such networks may be established by a municipality itself or by a commercial network provider, acting as the sole provider of the network infrastructure. However, establishing a Muni-Fi network is a financially challenging task due to the initial deployment and subsequent maintenance costs. A cost-efficient alternative is the establishment of a Wi-Fi-sharing community, which bases on the existing deployment of private access points (APs) in city areas. Community-driven networks, however, typically only provide Internet access to participating members and lack the open service characteristics of a Muni-Fi. *Collaborative Muni-Fi networks* leverage elements of both approaches by establishing a distributed Wi-Fi access network that is based on existing private APs and provides controlled access to a set of city services [2].

The users of collaborative Muni-Fi networks play a dual role. On the one hand, they use the provided Muni-Fi infrastructure with their mobile devices as *clients*. On the other hand, they contribute their Wi-Fi AP to the Muni-Fi infrastructure and act as network access providers. A third important element in Muni-Fi networks are city services. These services typically range from public tourist guides to user-specific services with sensitive data. Hence, depending on the purpose of the service, these city services are either openly available to civil servants, citizens, and tourists alike or have restricted access requiring user authentication. In a collaborative network comprised of strangers, it is essential to control and restrict client access to a defined set of city services in order to prevent misuse of the network by rogue clients and illegal services. However, the distributed and decentralized nature of collaborative Muni-Fis makes access control for city services challenging.

With PISA [1] and the PISA Service Architecture [3], we proposed a decentralized, collaborative Muni-Fi architecture that integrates a digital certificate- and tunneling-based approach to enable secure client access to city services. In our approach, we require city services to use certificates that attest the legitimacy of services in the Muni-Fi network to the AP that grants network access to the client. The certificate mechanism also allows us to exclude rogue city services from the Muni-Fi network. The tunnel solution ensures that client traffic cannot leak to the Internet, such that client access is restricted to city services. These tunnels can either span from the client to the service (see Figure 1) or from the AP to the service (see Figure 2) depending on the capabilities of the client to support our protocol stack extensions. In this short paper, we discuss how client integration in such a collaborative network with regard to today's mobile client devices and platforms can be established. Our primary focus are the resulting security and usability implications.

*This work is supported by Ziel2.NRW and the ERDF fund of the European Union – Investition in unsere Zukunft –

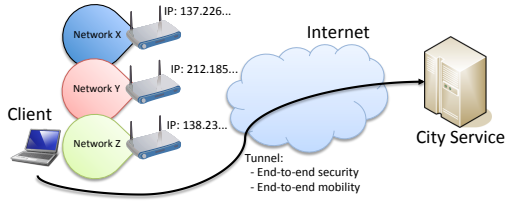

Figure 1: Client centric design: Client terminates security associations and manages mobility.

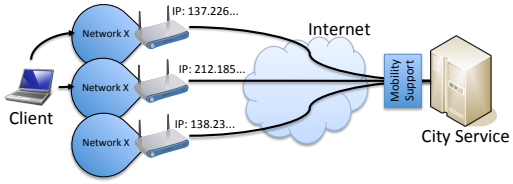

Figure 2: Network centric design: APs emulate one bridged Wi-Fi network. Network manages mobility.

2. CLIENT CAPABILITY-DRIVEN DESIGN

When implementing a secure collaborative Muni-Fi system, such as the PISA Service Architecture, the modification of software running on client devices like smart-phones and Internet tablets to, e.g., establish their authenticity is challenging. Firstly, the large variety of operating systems and devices dramatically increases development and maintenance costs. Secondly, the closed software stack below the application layer of modern mobile operating systems, such as iOS and Android, hinders the deployment of new network-layer functions. Adding new functionality to the network infrastructure at the last mile, however, proves feasible due to the availability of open operating systems (e.g. OpenWRT) for selected Wi-Fi access point models. Hence, we identify two high-level design possibilities for a collaborative Muni-Fi depending on client capabilities:

In a **client centric design**, the client plays an active role and can be freely configured and extended with additional software. This adaptivity enables authenticated and secure communication between a client and a service and may improve mobility support compared to unmodifiable clients.

However, these benefits come at the cost of high implementation efforts due to platform diversity and may prevent a number of client platforms from accessing the Muni-Fi.

In a **network centric design**, where a client cannot be modified, Muni-Fi tasks need to be performed by the network infrastructure on behalf of the client. A collaborative Muni-Fi network targeting such raw clients limits the architecture to in-network security mechanisms and requires the network to perform mobility handling without dedicated client support. The advantage of this design is the possibility for spontaneous use of the network by clients without prior preparation as no changes on the client side are required.

The two design possibilities differ mainly with respect to the security relations between the client and the network as well as mobility and usability. We now discuss each of these characteristics.

2.1 Security Implications

A **client centric design** allows to freely configure the standard security mechanisms supported by a device and to extend the client platform with additional security features and protocols. In PISA [1, 3], we use this capability to set up secure tunnels between the client and the service provider by means of HIP [4]. Furthermore, we use the protocol handshake to authenticate the user to the service during the tunnel establishment. The authenticated secure tunnel allows the service provider to grant access based on the user privileges and presents a general method of providing access to both open and restricted city services. Furthermore, we employ service certificates in the connection handshake. Service certificates are issued by a (possibly distributed) network entity, the *Community Operator*. Hence, certificates allow the Wi-Fi AP to verify the membership of the service provider and prevent client access to rogue services.

In a **network centric design**, clients are not assumed to support specific network security solutions (e.g., VPN) and cannot be extended with tailor-made security protocols. Hence, the client is not expected to allow for network-level user authentication at the service and, thus, the user remains anonymous. In such a scenario, PISA [1, 3] uses the shared APs at the users' home to emulate one large Muni-Fi network consisting of selected services. To this end, an AP verifies the validity of a service within the Muni-Fi network while establishing a connection on behalf of the client. We apply a *certificate and tunneling solution* between the AP and the service that is similar to our client centric design to exclude unauthorized rogue services. However, the network centric design does not allow clients to securely access city services per se as traffic in the Wi-Fi network is unencrypted. Hence, in order to enable access to services with sensitive information, client support for service-level authentication mechanisms such as HTTPS is required.

2.2 Mobility support

The unplanned deployment of wireless APs in collaborative Muni-Fi scenarios results in a patchwork of heterogeneous networked islands with short but overlapping range. In order to make these network islands appear like a single homogenous network and to provide a network experience similar to the services of a provider-driven solution, a concept for handling mobility is required. We focus on two aspects of client mobility: a) the selection and seamless association with the next AP and b) the re-authentication of the communication end-points.

A **client centric design** allows to customize client software in order to enable scenario-specific mobility decisions, thereby supporting reliable and faster handovers. The client can identify the best AP (e.g., by means of the RSSI strength or more sophisticated measures) and decide when to switch between APs. Furthermore, the membership of the service has to be checked at the new AP and the client needs to be re-authenticated towards the service in order to ensure that communication takes place between the same parties as before the mobility event. In PISA, we use HIP to re-authenticate the client and the service as well as to handle mobility events without the need for additional infrastructure. HIP thereby allows to maintain transport layer connections across multiple mobility handovers enabling a client to roam between different APs in the Muni-Fi network.

In a **network centric design**, the limited client capabilities prevent the use of customized client-driven mobility management solutions. As a result, a mobility event needs to be handled within the network infrastructure in order to prevent application layer connections from breaking. In PISA, we set up the APs to appear like a single bridged Wi-Fi network towards the client despite the fact that they are located in distinct domains without coordination. Using the same SSID but different BSSIDs between the APs achieves this seemingly identical wireless network. In addition, the IP and MAC-layer addresses of the Wi-Fi routers must be identical to avoid ARP timeouts. Moreover, the APs and services implement mobility support for the clients to enable continued communication after a client moves. In order to mitigate client impersonation attacks for unauthenticated services, the AP thereby informs the service about the newly arriving client's MAC address during the mobility handling procedure.

3. CONCLUSION

In our work, we briefly discuss the conceptual differences between a client and a network centric design to providing secure large-scale collaborative Muni-Fis. A network centric design allows arbitrary clients to use the network and is more likely to be compatible with future generations of mobile devices. However, compared to a client centric design it adds complexity to the network for providing mobility support and may not allow for end-to-end client authentication. We implemented both approaches in PISA in order to cater for unmodified clients and secure service provisioning alike. We consider both valid solutions depending on the scenario.

4. REFERENCES

[1] T. Heer, S. Götz, E. Weingaertner, and K. Wehrle. Secure Wi-Fi Sharing at Global Scales. In *Proc. of 15th International Conference on Telecommunication (ICT)*, 2008.

[2] T. Heer, R. Hummen, N. Viol, H. Wirtz, S. Götz, and K. Wehrle. Collaborative Municipal Wi-Fi Networks - Challenges and Opportunities. In *Proc. of IEEE PerCom Workshops, PWN'10*, 2010.

[3] T. Heer, T. Jansen, R. Hummen, H. Wirtz, S. Götz, E. Weingaertner, and K. Wehrle. PiSA-SA: Municipal Wi-Fi Based on Wi-Fi Sharing. In *International Conference on Computer Communication Networks, ICCCN*, 2010.

[4] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. RFC 5201.