radioActive WiFi Sharing for Autonomous Peers

Till Elsner   Nhan-Tam Nguyen   Björn Scheuermann

Institute of Computer Science
Heinrich Heine University Düsseldorf, Germany
{elsner, scheuermann}@cs.uni-duesseldorf.de, nhan-tam.nguyen@uni-duesseldorf.de

Abstract—**WiFi sharing communities offer an attractive alternative to commercial hot-spots and cellular networks for users who seek Internet access while being away from home. The growing number of mobile devices with Internet usage capabilities has formed a basis for the establishment and growth of several such communities. However, critical security problems exist in all current WiFi sharing approaches because they employ a central operator. We show how to overcome these issues by decentralizing the community's organization structure and present *radioActive WiFi*, a system that implements this approach.**

I. Introduction

Being attractive as a free-of-charge alternative to mobile Internet access methods such as 3G or commercial hot-spots, WiFi sharing communities gain more and more popularity. As the number of users increases and the usage of WiFi sharing broadens, security issues attract more attention. Although several WiFi sharing communities with significant user base are established and actively used (e. g., FON [1]), participating in them still leaves members with security concerns. First, in the role of a *guest*, a member connects to the Internet using the access point of an unknown (and therefore untrusted) *host*; all of her traffic travels via this access point. Therefore the guest's (potentially sensible) data becomes vulnerable to eavesdropping not only by the host, but also by other clients using the host's unencrypted wireless network.

Second, in the host role, a member connects guests to the Internet. To any communication partner on the Internet, the host's Internet connection appears as the source of her guests' traffic. She therefore, in a certain sense, takes the responsibility for this traffic. Even worse, in a centralized WiFi sharing approach *not the host, but the community operator* is in charge of deciding which guests should be allowed to access the Internet. In all previous approaches the operator does so either by online authentication or by issuing certificates. Thus, the host is not even in charge of the authentication and thus cannot even decide *whose* traffic she is taking the responsibility for.

Finally, authentication towards the community operator poses another problem: to authenticate the guest, the community operator needs to identify the guest. This kind of authentication means a serious threat to the guest's privacy, since it provides the community operator with full knowledge about when the guest accessed the Internet and from which access point. Keeping the commercial motivation of most community operators in mind, this is surely not desirable. Moreover, in many approaches, the (untrusted) host can either learn about the guest's identity, too, or she can at least recognize guests who have already connected before based on identification attributes visible to the access point during the transport of authentication traffic, exposing the guest to both community operator *and* host.

At a closer look, all those weaknesses of existing WiFi sharing approaches result from their centralized structure—especially from the existence of and the dependency on a community operator. And this central instance is not only a danger to the members' security and privacy—the dependency of the community on a central operator seems even more absurd when we recall that a WiFi sharing community is inherently based on the peer-to-peer concept: equal members share resources by providing Internet access to each other. Consequently, we tackle those security issues by removing the community operator entirely and decentralizing the community structure.

II. Decentralized WiFi Sharing

The goal of the decentralization of the community is to provide freedom of decision for the host—and thereby the opportunity to share her Internet connection without risk and without having to trust an operator, her guests, or any other party. At the same time, it provides anonymity and privacy as well as data traffic protection for the guests. The following is a brief sketch of how we accomplish these seemingly contradictory goals in our *radioActive WiFi* sharing approach, which is described in more detail in [2].

First, to relieve the host from the liability for her guests' traffic, we need to shift this liability to an instance that can take it without concerns. The most consequential target for this shift is the guest herself. In order to burden the guest with the responsibility for her own traffic, another instance is introduced in the community structure: the *remote station*. The remote station generally shares a trust relation with the guest. The most common setup will be similar to approaches like [3] or [4]: the access point at the guest's own Internet connection at home acts both as her remote station and as a host access point for other community members at the same time. While [3], [4] still required a central operator, though, we can do without any such instance.

As shown in Fig. 1, by forwarding a guest's traffic exclusively to this particular guest's own remote station, the host hands over the liability for this traffic to this remote station. The remote station can then act as a trusted relay for the guest's

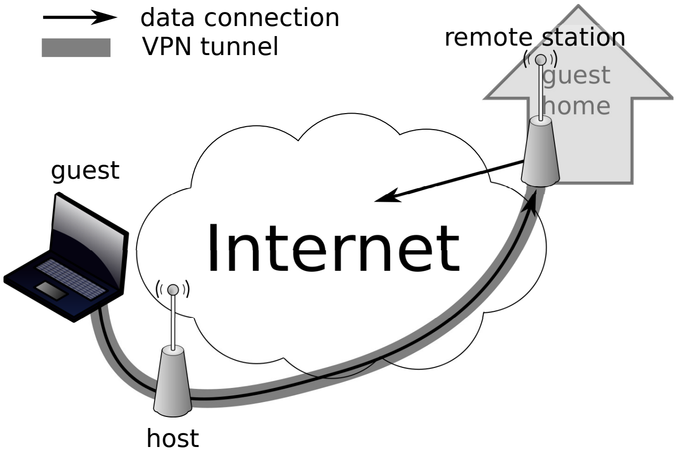
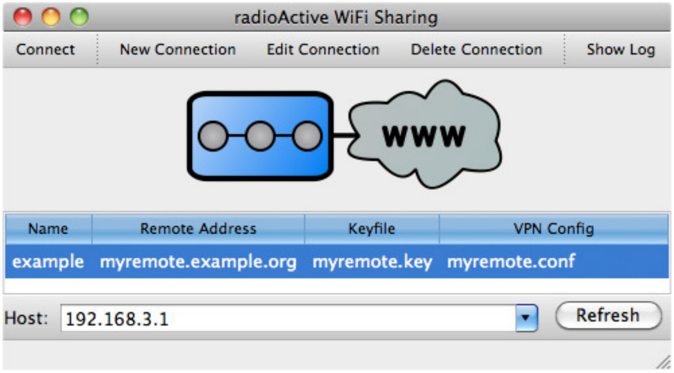


Fig. 1. Connection in a decentral WiFi sharing community.



Name	Remote Address	Keyfile	VPN Config
example	myremote.example.org	myremote.key	myremote.conf

Host: 192.168.3.1

Fig. 2. Screen shot of the client's graphical user interface (Mac OS X).

traffic, forwarding it on to the Internet. The host does not need to worry about transporting potentially malicious traffic, as the remote station explicitly agrees to receive this guest's traffic. From there on, towards other Internet nodes, the remote station itself appears as the origin of the traffic. Thus, the host may forward any kind of traffic between guest and remote station. By encrypting the exchanged data on the path between guest and remote station, we can also leverage this redirection to protect the guest's traffic from the host.

A host must of course not forward any guest's traffic to any arbitrary remote station—thus, a central question remains: how can a host verify that it is safe to forward traffic between a guest and an IP address on the Internet which this guest claims to be her remote station? Or, simpler: how to prevent guests from naming an incorrect remote station? Clearly, some form of authentication is necessary.

We are the first to propose a system that accomplishes this authentication without a central entity in the system, not even on the organizational level. Certificate-based authentication schemes can therefore be ruled out: certificates which confirm that guest and remote station belong together would require the host to trust the authority issuing these certificates, which would again mean that the host needs to accept the decision of an external instance of whether to share her Internet connection with a guest or not. Moreover, certificate-based authentication also means a threat to the guest's privacy as the certificate uniquely identifies the guest towards the host, making the guest recognizable whenever she returns to the same host. The hosts therefore need other means to verify that the remote station is ready and willing to accept traffic from a particular guest. Our solution to this problem is what we call the *remote station approval* handshake.

During this handshake, guest and remote station prove to the host that they belong together, not only without the need for any central instance or authority, but also without the need of direct communication between guest and remote station. To prove their trust relationship, guest and remote station share a secret in form of a symmetric cryptographic key s. If a guest requests to connect to a particular remote station, this remote station provides a temporary secret t to the host. In order to obtain this temporary secret, the guest must have the symmetric key s. The subsequent authentication towards the host with t proves the guest's possession of s and consequently the trust relationship between guest and remote station. With the trust relation between guest and remote station proven and the guest thus only being able to connect to this remote station, the host is free of any liability concerns when granting the guest access to her Internet connection. Moreover, the whole authentication scheme is accomplished using symmetric cryptography only—this avoids the risk of denial-of-service attacks even on low-end hardware. A detailed description of the remote station approval handshake can be found in [2].

Our implementation of the system is designed to run on low-cost access point hardware with the open source embedded firmware OpenWRT [5] and is thus suitable for home deployment. Client (guest) software with a Qt-based graphical user interface, as shown in Fig. 2, exists for all major operating systems. Guest, host, and remote station software run completely in user space and do not require any modification of the network stack or operating system. For the encryption and authentication operations, the well-proved VPN platform OpenVPN [6] is used as a basis. Further information about the project and software releases can be found on the project website [7].

References

[1] "Fon," web site. [Online]. Available: http://www.fon.com

[2] W. Kiess, T. Elsner, B. Scheuermann, and M. Mauve, "Global grassroots WiFi sharing," in *WCNC '10: Proceedings of the IEEE Wireless Communications and Networking Conference*, Apr. 2010.

[3] N. Sastry, J. Crowcroft, and K. Sollins, "Architecting citywide ubiquitous Wi-Fi access," in *HotNets '07: Proceedings of the 6th Workshop on Hot Topics in Networks*, Nov. 2007.

[4] T. Heer, S. Götz, E. Weingärtner, and K. Wehrle, "Secure Wi-Fi sharing on global scales," in *ICT '08: Proceedings of the 15th International Conference on Telecommunication*, June 2008.

[5] "OpenWRT," web site. [Online]. Available: http://www.openwrt.org

[6] "OpenVPN," web site. [Online]. Available: http://openvpn.net

[7] "radioActive WiFi project," web site. [Online]. Available: http://radioactive-wifi.net