Using a 2DST Waveguide for Usable, Physically Constrained Out-of-Band Wi-Fi Authentication

Matthias Budde, Marcel Köpke, Matthias Berning, Till Riedel, and Michael Beigl

{budde, koepke, berning, riedel, michael}@teco.edu
TECO, Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany

Abstract. This paper proposes using a 2D waveguide for a novel means of authentication in public Wi-Fi infrastructures. The design of the system is presented, and its practicability and usability is comparatively discussed with that of five other tag and context based authentication schemes, two of which have not been previously realized. In accordance with the presented application scenarios, all of the schemes were implemented in a platform-independent fashion built on web technology.

Keywords: Practical Security, Waveguide, Wi-Fi, 802.11, Usability, Device Association, Authentication, Smart Environments.

ACM Classification Terms: H.5.2 User interfaces: Interaction styles.

General Terms: Human Factors; Design; Reliability; Security

1 Introduction

Publicly accessible Wi-Fi hotspots are used for corporate guest networks, in hotels and at airports, as well as in cafés or restaurants that offer their customers Wi-Fi access at their venues. They are also increasingly recognized as an essential part of our mobile computing infrastructure, complementing mobile broadband: Recently, German carrier *Deutsche Telekom* announced a long-term Wi-Fi offloading project. A partnership with *Fon*, a Wi-Fi crowdsourcing provider, will extend the Telekom's network by 12,000 access points, and the ambitious plan is to "provide nationwide WLAN To Go at more than 2.5 million additional hotspots" by 2016 [16]. As providing a good wireless network service is not only about network quality but also about user experience, ease of access and attractiveness are important factors. For providers of free services, open hotspots create the implication of legal liability, which is why access control often remains mandatory. This adds an extra burden on many users, especially when systems use complicated user/password schemes. We therefore present and discuss alternative techniques suited for authentication of mobile devices in Wi-Fi networks. The focus lies on implementation and practical feasibility as well as usability. A completely novel approach that addresses these challenges is presented and relevant other Out-of-Band (OOB) authentication techniques are adapted to our use case. In total, we

implemented six different means of authenticating mobile devices to a guest Wi-Fi network. Our selection of relevant techniques was based on the following constraints that are relevant in the presented scenarios:

- *Non-mediated*, i.e. users can log on themselves at any time.
- *Intuitive*, as hotspots are broadly used by non-experts.
- *Platform-independent*, as the spectrum of mobile devices and operating systems is diverse and volatile.

Since from an operator's point of view, authentication must be available to as many users as possible, we selected methods that can be implemented using solely web technology.

2 Related Work

A number of schemes have been proposed in the past to pair mobile devices for spontaneous interaction, many of which could in principle be applied for the authentication to public Wi-Fi hotspot as well. A general solution proposed in earlier work is the use of OOB information to establish or verify a shared secret between the two communication parties. A good overview on possible OOB channels is given by Kainda et al. [6] and Kobsa et al. [7]. In addition both conducted extensive comparative user studies on the usability of the proposed methods, which could be flawed or at least biased as argued by Ion et al. [5]. The latter does not only take a more varied participant background into account but showed that the results of the usability evaluation and user preference depend on the context of the pairing situation.

An approach to provide location constrained access to a Wi-Fi network is implemented by Sheth et al. [11]: *Wi-Fi geofencing*. By using several APs with steerable directed antennas, they were able to constrain the network reception to an arbitrarily shaped area the size of an office desk. Although this approach seems promising and does not require anything beyond Wi-Fi capability on the device side, it is prohibitively expensive in terms of hardware and installation costs. *Amigo* [17] is another OOB approach that solely requires wireless radio capability to enable proximity-based device pairing. The approach leverages the similarity of dynamic characteristics of the common radio environment observed by co-located devices in close physical proximity. An extension of *Amigo* that offers a series of improvements was presented by Mathur et al. [8]. While not requiring special device features or user involvement, the general approach demands that a device can overhear a public source of radio waves, which entails the installation of software on the device.

The constraints imposed by our scenario also restrict the use of several others of the mentioned OOB channels. For example Holmquist et al. [4] as well as Mayrhofer et al. [9] propose the use of acceleration sensors embedded in the devices. When shaken simultaneously by a single user, both devices can synchronize using the common sensor-values. While robust, this technique is not applicable in our scenario, since the access point is usually fixed to a location. This is also a concern with the results found by Chong et al. [2] in his explorative study on natural device interactions employed by users to pair different devices. Most of the suggested procedures would require physical access to the access point, which is usually not possible or at least not favorable by the network operator. Other proven approaches need to be adapted and might require a modification of the central device.

Fig. 1. Prototypical 2DST sheet used for spatially confined Wi-Fi.

In the work of McCune et al. [10] a video channel is used to transmit information encoded in a barcode between two devices. Similarly Goodrich et al. [3] generate audio output on one device which can be verified on the other. The concept of using sound as the OOB channel was later researched by Sigg et al. [15] to generate a shared secret from ambient audio. The latter work was used as basis for one of the techniques adopted to Wi-Fi authentication presented below.

3 Waveguide Authentication

We present a novel way of creating a spatially confined Wi-Fi network and show how this can be exploited for providing an easy context-based mode of authentication. We leverage the idea of location restricted Wi-Fi by using a 2D waveguide which is cheap and can be easily installed, e.g. in a shop's counter or registration desk, and allows distinguishing between devices on its surface and other devices in the room. We used the prototypical *Two-Dimensional Signal Transmission sheet* (2DST sheet) [12,13] from Shinoda Labs (see Figure 1). The sheet was initially developed for different applications: It can be used to induce power into objects placed on its surface, as well as for data transmissions trapped in two dimensions. The unique feature of the sheet is, that it emits a signal of about 2.4 GHz only up to a distance of several centimeters. We can therefore create a spatially confined Wi-Fi by (ab)using it as an antenna connected to a standard access point (AP). Because the signal injection into the sheet is done through an clip-on induction coupler which emits the signal too, we attenuated the signal strength by 60 dB (10dB in the AP firmware and another 50dB through a series of SMA attenuators). This is still sufficient to induce the signal into the sheet, while minimizing radiation from the coupler. Additionally, we shielded the AP through a metal enclosure in order to block the signal emitted from an internal antenna.

In principle, this configuration could be used stand-alone to provide localized Wi-Fi access. However, this would mean that

the device must remain on the surface at all times. We therefore devised a scheme which allows us to use the sheet to authenticate the device and then remove it without losing connectivity. For this, we set up a multiple-AP (roaming) 802.11 network with the following configuration: A standard Wi-Fi AP, subsequently named *main AP*, is used to supply the guest network. Additionally, a second AP which uses the 2DST sheet as antenna supplies another, spatially confined Wi-Fi with the same SSID and located in the same address space. We dub this the *sheet AP*. This approach is easily extensible to multiple APs of both kinds.

In order to authenticate to a guest Wi-Fi, a user first connects to the main AP. This AP optionally redirects any web request to a captive portal page (see Figure 2 ①) which prompts the user to place his device on the 2DST sheet for authentication. Triggered by an event, such as a button press or the detection of a new device by the sheet AP, the system de-authenticates the device association to the main AP (②). For our prototype, we use the WEP/WPA-cracking tool *aircrack-ng* for Wi-Fi monitoring and packet injection. We continuously inject de-authentication packets for the association between the main AP and the client into the Wi-Fi traffic. As the client will try to reconnect, eventually a handover to the sheet AP is forced (③). Since the whole network lies within a single address space, working TCP/IP connections are kept alive. The sheet AP is monitored and devices that come into its proximity are authenticated (④), after which the system de-authenticates the association between the sheet AP and the device, forcing it to roam back to the main AP with full network access (⑤).

We evaluated our approach by placing devices in different distances above the

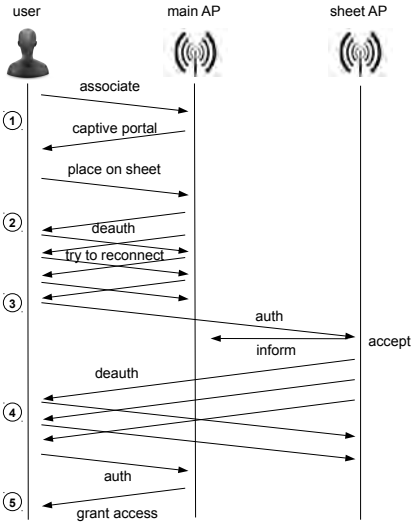

Fig. 2. Novel mode of authentication using the 2DST sheet.

sheet and sending ping messages (1000 packets, 64 byte, timeout 10s, no waiting time between packets). This was done for different intensities of the induced Wi-Fi signal as well as for different devices, two phones and a laptop: A *Huawei U8815*, a *Samsung Galaxy SIII*, and a *Lenovo X220t*. Table 1 shows the results: In direct contact to the surface, the devices all showed a stable connection. Depending on the respective antenna quality, the connection either gradually degraded with increasing distance or suddenly broke off. At a distance of 10cm, none of the devices was able to connect anymore.

When using even stronger attenuation (65dB), we started to observe packet loss already in direct contact to the sheet (*Galaxy SIII*). Less attenuation (45dB) lead to the inductive coupler starting to interfere, which may be a problem of our prototype. These initial experiments show that the Wi-Fi signal can be spatially confined and exploited for the outlined ap-

Device	Distance	*Attenuation: 60dB* Paket loss	RTT [ms] (min/avg/max/mdev)				*Attenuation: 55dB* Paket loss	RTT [ms] (min/avg/max/mdev)			
U8815	0 cm	0%	1.5	5.2	108.2	13.9	0%	1.5	7.4	236.2	23.7
	1 cm	0%	2.5	3.9	18.6	1.9	0%	2.1	7.3	226.7	25.7
	2 cm	100%	(dest. unreachable)				0%	2.5	9.6	135.5	19.2
	5 cm	100%	(dest. unreachable)				100%	(dest. unreachable)			
SIII	0 cm	0%	1.5	2.2	47.8	1.8	0%	1.5	4.4	253.1	18.7
	1 cm	62%†	3.2	12.6	108.7	16.9	40%	2.5	335.8	3571.7	818.7
	2 cm	100%	(dest. unreachable)				85%	21.6	666.9	3400.8	777.1
	5 cm	100%	(dest. unreachable)				100%	(dest. unreachable)			
X220t	0 cm	0%	1.4	2.0	37.6	18.0	0%	1.3	1.9	24.2	1.4
	1 cm	0%	1.5	1.8	5.9	0.4	0%	1.4	1.8	11.4	0.6
	2 cm	0%	1.3	2.0	7.1	0.5	0%	1.6	2.0	10.7	0.8
	5 cm	100%	(dest. unreachable)				0%	4.1	835.4	1555.7	357.6
	10 cm	100%	(dest. unreachable)				100%	(dest. unreachable)			

† Frequent connect/disconnect observed.

Table 1. Packet loss and RTT of ping packets for different devices, distances from the 2DST sheet and attenuation of the induced Wi-Fi signal.

plication scenario. In order to support devices that have their antenna in the third dimension, such as laptop computers, multiple sheets may be employed.

4 Discussion

Today, the standard mode to authenticate to a guest Wi-Fi network still is a combination of a login name and a password. Though broadly supported and easy to provide, this can be cumbersome on mobile devices. However, there are methods that can be used to enter these credentials, two examples being *QR-Codes* and *Near Field Communication (NFC)*. Since the standard *username:passwd* mode basically comes down to logging on to a password protected web interface, all necessary information can be encoded into a URL, which in turn can be stored in a tag. We implemented a platform-independent solution that captures the image with web technology (*HTML5*) and decodes the QR-Code with a JavaScript library (*jsqrcode*). For NFC, the approach worked out-of-the box, the URL was opened without need for further applications other than a browser. In addition to these credential-based methods, we implemented two more context-based login techniques aside from the 2DST sheet. The first one makes use of the *Microsoft Kinect* to identify a login attempt. We adapted it from a smart home project in which we use smartphones as universal remotes and the Kinect to identify which device a user wants to control [1]. In the same way, we can check on the server whether a user performs a specific gesture, e.g. raising his hand over his head. If the user stands within the Kinect's field of vision while trying to log on to the Wi-Fi network, access will be granted. As last method, we used ambient audio in

Method	off-the-shelf	Requires			Supports	
		device features	infrastructure	special software	individual login	context-based login
Login: passwd	yes	*none* ⊕⊕	login printer ⊕	standard browser ⊕	×	
QR-code	no	camera ⊕	login printer ⊕	HTML5 browser ◯	×	
NFC	yes	NFC ⊖	tags/writer ◯	standard browser ⊕	×	×
Kinect	no	*none* ⊕⊕	Kinect ⊖⊖	standard browser ⊕		×
Audio context	no	microphone ⊕	microphone ⊖	HTML5 browser ⊖		×
2DST sheet	no	*none* ⊕⊕	2DSTsheet ◯	*none* ⊕⊕		×

Table 2. Benefits and drawbacks of different authentication methods.

order to establish whether the user is in the correct context. Microphones are naturally present in phones and – as with camera access for the QR-codes – the readout can be implemented in *HTML5*. In order to log in, a user presses a button on the captive portal site and both the phone and the server start recording. The phone transmits its recording to the server, which calculates fingerprints from the audio and compares them. If they are sufficiently similar, access is granted. For creation of the audio fingerprints we used the algorithm proposed in [15].

Each of the presented modes of authentication has different strengths and weaknesses by design. Some require the authenticated device to have certain sensors or other technological features, others rely on additional infrastructure besides the mandatory access point. We rated the features with respect to their implementation complexity and general requirements on a scale ranging from 1 to 5 (⊖⊖, ⊖, ◯, ⊕, ⊕⊕). In addition, a comparative user study was conducted, which is currently being evaluated. Table 2 shows whether the approach requires the device to have certain *technological features*, special *infrastructure* (except Wi-Fi APs), or requires certain *software*. Furthermore, it shows whether the method supports *individual login* through credentials and/or *context-based login*, i.e. anyone being in a certain context can log on.

For the standard *Login:passwd* technique, only some kind of printer for account provisioning is needed beyond the APs that provide the Wi-Fi network in terms of infrastructure (⊕) and the de-

vices need no other technological features than Wi-Fi support (⊕⊕) and a standard browser (⊕). While the *QR-Code* method also does not rely on additional infrastructure (⊕), it requires the device to have a built-in camera, which today is present in most mobile devices (⊕). The platform-independent implementation of the scheme requires a browser that supports the `GetUserMedia()`-API of *HTML5*, which on mobile devices is currently only available in selected browsers (◯).

Near Field Communication (NFC) is the most recent of the employed technologies, which also means that it is currently only supported by very recent devices (⊖). While we used a passive solution, active solutions are also possible. However, the ease of use may turn out to have a downside as well, since in our experience, a device with NFC will read any tag and open the URL that is programmed, without prior confirmation or knowledge of the URL. Users might feel reluctant to use this technology in an environment they do not completely trust.

The *Kinect* solution does not require any device features on the phone (⊕⊕) and runs using a standard browser (⊕). However, the infrastructure overhead is rather high (⊖⊖). Concerning the security of this method, we emphasize that in its current implementation, it is less secure than the other methods, since an attacker could attempt to exploit a race condition during the login process, by syncing a login attempt while a different user performs a gesture in the Kinect's field of view. We are currently examining to alleviate this vulnerability by comparing the performed gestures to the accelerometer data of a phone, which also can be read out via *HTML5*. For the last context-based method, ambient audio was chosen because microphones are present in basically any mobile device today (⊕). Similar to the QR-Code implementation, audio readout is only supported by a few capable browsers, none of which currently run on mobile devices (⊖). However, getting the scheme to work reliably and user friendly at the same time is quite a challenge, as hardware differences, especially different microphones, have a strong impact on the fingerprints. Furthermore, time synchronization is very important. In order to reach reasonably reliable authentication, we needed to record relatively long samples (8s), which lead to quite long authentication times. Another issue may be that the level of security that fingerprints based on ambient audio can provide is relatively unexplored. While some work regarding the entropy of the employed algorithm has been done [14], a comprehensive analysis is not available yet.

The beauty of the 2DST sheet solution is that it can be implemented completely software-free on the client side and thus truly device independent (⊕⊕). In principle, the only thing this solution requires is the ability to log on to a Wi-Fi network and support to re-log on once the connectivity breaks. On the infrastructure side, this approach requires a bit more effort (◯). Still, it seems well suited for certain scenarios, e.g. the integration into a check-out counter.

5 Conclusion and Future Work

This work presents and discusses novel methods for authenticating mobile devices in a Wi-Fi network. We show a way of providing a spatially confined Wi-Fi using a 2D waveguide sheet as well as an authentication scheme leveraging it. The approach performs very well and requires no additional technology or software on

the device side and only little infrastructure. As part of our work, we have implemented platform-independent solutions based on *HTML5* for six different authentication techniques and share the code with the community. In our future work, we will present the results of a comparative user study with 22 participants that has been conducted and is currently being evaluated. We also intend to refine the systems, e.g. increase the security of the *Kinect*-based scheme by sampling the accelerometer using *HTML5* and comparing the data to the performed gestures.

References

1. Budde, M., Berning, M. et al. Point&Control - Interaction in Smart Environments: You Only Click Twice. In *Adj. Ubicomp 2013* (2013).
2. Chong, M. K., and Gellersen, H. How users associate wireless devices. In *CHI'11* (2011).
3. Goodrich, M., Sirivianos, M., Solis, J., Tsudik, G., and Uzun, E. Loud and Clear: Human-Verifiable Authentication Based on Audio. In *ICDCS'06* (2006).
4. Holmquist, L., Mattern, F., Schiele, B., Alahuhta, P., Beigl, M., and Gellersen, H. Smart-Its Friends: A Technique for Users to Easily Establish Connection Between Smart Artefacts. In *Ubicomp'01* (2001).
5. Ion, I., Langheinrich, M., Kumaraguru, P., and Čapkun, S. Influence of User Perception, Security Needs, and Social Factors on Device Pairing Method Choices. In *SOUPS'10*, ACM (2010).
6. Kainda, R., Flechais, I., and Roscoe, A. W. Usability and security of out-of-band channels in secure device pairing protocols. In *SOUPS'09* (2009).
7. Kobsa, A., Sonawalla, R., and Tsudik, G. Serial hook-ups: a comparative usability study of secure device pairing methods. In *SOUPS'09* (2009).
8. Mathur, S., Miller, R., Varshavsky, A., Trappe, W., and Mandayam, N. Proximate: proximity-based secure pairing using ambient wireless signals. In *MobiSys'11* (2011).
9. Mayrhofer, R., and Gellersen, H. Shake well before use: Authentication based on accelerometer data. In *Pervasive computing* (2007).
10. McCune, J., Perrig, A., and Reiter, M. Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication. In *SP'05* (2005).
11. Sheth, A., Seshan, S., and Wetherall, D. Geo-fencing: Confining Wi-Fi coverage to physical boundaries. In *Pervasive'09* (2009).
12. Shinoda, H., Asamura, N., Hakozaki, M., and Wang, X. Two-dimensio- nal Signal Transmission Technology for Robotics. In *ICRA'03.* (2003).
13. Shinoda, H., Makino, Y., Yamahira, N., and Itai, H. Surface Sensor Network Using Inductive Signal Transmission Layer. In *INSS'07.* (2007).
14. Sigg, S., Budde, M., Ji, Y., and Beigl, M. Entropy of Audio Fingerprints for Unobtrusive Device Authentication. In *Context 2011*, LNCS (2011).
15. Sigg, S., Schuermann, D., and Ji, Y. PINtext: A Framework for Secure Communication Based on Context. In *MobiQuitous 2011* (2011).
16. Sottek, T. Deutsche Telekom partners with Fon for crowdsourced Wi-Fi, plans to cover Germany in hotspots. **http://www.theverge.com/2013/3/4/4062748/deutsche-telekom-fon-wifi-hotspots**, March 2013.
17. Varshavsky, A., Scannell, A., LaMarca, A., and De Lara, E. Amigo: proximity-based authentication of mobile devices. In *UbiComp'07* (2007).