Demonstrating OpenUAT, the Open Source Ubiquitous Authentication Toolkit

Rene Mayrhofer[1] and Iulia Ion[2]

[1] Faculty for Computer Science, Vienna University, AT
[2] ETH Zurich, Switzerland
rene@mayrhofer.eu.org, iulia.ion@inf.ethz.ch

Abstract. Establishing secure communication channels between devices that share no a priori context, also known as the device-pairing problem, is the first step towards the realization of mobile, interoperable applications interacting across several devices. One approach that promises to be both secure and usable relies on so-called auxiliary or out-of-band channels for authentication. Although many such solutions have been independently suggested, open, easily usable implementations are unfortunately missing so far. In this demonstration, we present *OpenUAT*, an open source toolkit for establishing secure ad-hoc connections. OpenUAT implements many of the auxiliary channels proposed in the past few years on top of a unified, common cryptographic protocol for key exchange and runs on a variety of mobile phones and desktop/laptop computers. By giving users the chance to directly compare different device pairing alternatives in a real-life security prototype, OpenUAT fosters usability research and shortens the gap between research prototypes and real-world applications.

1 Introduction

In mobile applications, authentication is required to secure any device interaction. For example, without being able to authenticate whom our smart phone is transmitting its access keys or credit card information to, no real security is possible. *Spontaneous authentication* can thus be seen as a necessary building block for many future applications in mobile and pervasive computing. Without relying on wired connections (which are impractical) or trusted third parties (which seem infeasible to secure and usable on a global scale), this is however not trivial: With potentially tens of different wireless networks and hundreds of unknown devices in these networks, even selecting the intended communication partner is a major challenge for users, and securely transmitting key material even more so. Specifically, mobile devices pose three novel challenges: (1) primary communication channels are wireless and thus inherently insecure; (2) mobile device often lack sufficiently capable user interfaces; and (3) user attention is a scarce resource.

To address these challenges in the context of secure device pairing, a number of proposals have recently emerged, all of which somehow involve the user in the

pairing process and partially rely on so-called *auxiliary* message channels. For example, "constrained channels" [1] and "location-limited channels" [2] propose general models of auxiliary channels for authentication purposes. Examples of specific auxiliary channels are *video* by using mobile phone cameras and 2D barcodes [3], blinking patterns [4], or laser channels [5], *audio* by comparing spoken sentences [6] or MIDI tunes [7], *ultrasound* [8], *motion* by common movement [9], gestures [10], or synchronised button presses [11], or *radio frequency* by measuring common environment [12].

To ensure consistency and provide standardized solutions, the already suggested options for auxiliary channels should be supported by a unified authentication protocol. Usability studies on device pairing protocols so far have been hindered by lack of available implementations, therefore often limited to mockups of very few methods that cannot discover issues in real-world deployment. In practice, interesting user behaviour and additional issues only surface when user studies are done with functional (but maybe prototypical) applications.

2 OpenUAT summary

OpenUAT brings together most of the proposed device pairing methods in an open source toolkit, based on a common, underlying cryptographic protocol. The toolkit is designed to be easily extendable and the provided auxiliary channels are easily interchangeable.

OpenUAT serves as a real-life framework for comparative usability testing of different pairing methods. Furthermore, by providing usable implementations, OpenUAT enables rapid application development, and thus helps push research results into real-world applications.

OpenUAT is mainly implemented in Java and verified to work on most Java virtual machines (JVMs) including Java Micro Edition (JavaME) as available on many off-the-shelf mobile devices. In particular, we have successfully tested the implemented channels on Nokia Series60 devices that implement all the required optional JSRs (e.g. N95, N82, 5500), on selected Windows Mobile devices (e.g. Samsung i900) and on appropriately equipped laptops.

3 Application scenarios and auxiliary channels

Three application scenarios have been chosen to be representative of a wide range of application areas:

1. **Pairing two phones to exchange vCards and PGP keys**: Alice and Bob meet at a conference and wish to exchange contact information (vCards) and PGP keys for future remote communication. The keys are ephemeral, as their mobile phones are unlikely to directly communicate again. A specific issue is spontaneous authentication with severely limited user interfaces and highly personal devices that users may not wish to hand over.

2. **Printing a confidential document on a Bluetooth printer**: Alice wishes to use the (partially) trusted printer in the waiting lounge to print multiple parts of the paper she's preparing for submission. Keys may be reused for printing separate documents after initial establishment. A specific issue is selecting the "correct" printer in a list of similar ones.
3. **Connecting a PDA to a Wi-Fi router**: While enjoying a coffee in a Coffee shop in Tokyo, Bob wishes to quickly check his email. He connects his PDA to the secure wireless LAN provided. The trusted access point is in free line of sight, but Bob is afraid of man-in-the-middle attacks.

In each of the scenarios, users can choose between different authentication methods and channels currently implemented by OpenUAT and limited only by the capabilities of the respective devices:

- **Manual entry**: A user enters the same (short) PIN code on two devices.
- **Manual comparison**: A user compares a (short) PIN code displayed on two devices and confirms or rejects the authentication.
- **Shake together**: Two mobile phones can be shaken together for a few seconds and subsequently use their common movement to authenticate their communication. Off-the-shelf mobile phones that come with embedded accelerometers can be used without modification (besides installing the application)
- **Push buttons synchronously**: The user presses buttons concomitantly on both devices and thus provides common input.
- **Capture 2D barcodes**: One device (either a laptop or a mobile phone) displays a 2D barcode, which the user captures with the camera of a mobile phone.
- **Audio transmission**: One device transmits key material as MIDI tunes, which the other device captures using its microphone.

Most combinations of application scenarios and channels are possible, offering a wide range for live experimentation. Users are expected to play with the technology and intuitively familiarize themselves with each of the options. A potential outcome from a research perspective might be an interesting set of user experiences — enabling spontaneity is one of the design principles of OpenUAT.

4 Outlook

During this demonstration, users have the chance to try the most promising device authentication methods for ubiquitous computing first-hand. They are expected to securely pair two devices (either two mobile phones or one mobile phone and one laptop emulating either the printer or the access point) using the auxiliary channel of their choice. We will record all user feedback concerning the perceived usability and security level and personal preference towards particular pairing methods.

Our demonstration has in particular the following purposes:

1. Give users a motivating scenario and allow them to easily pair two arbitrary devices.
2. Observe the user feedback with regards to the technology and collect data that will help estimate the usability of different methods.
3. Get feedback from researchers on the further improvements for the pairing methods.
4. Presenting the toolkit internals on posters and hand-outs and inviting more researchers to work together on the well-known secure device pairing problem in the common framework provided by OpenUAT.

Thanks to our implementation in the form of an open source toolkit, all these methods may immediately and freely be used by all research groups for creating additional applications or enriching their current prototypes with secure authentication. By providing OpenUAT, we hope to both foster future research and to shorten the gap between research prototypes and real-world applications. OpenUAT serves researchers to compare and analyse existing methods, to easily prototype new ones and conduct user studies with real implementations.

References

1. Kindberg, T., Zhang, K.: Context authentication using constrained channels. Technical Report HPL-2001-84, HP Laboratories (April 2001)
2. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: Talking to strangers: Authentication in ad-hoc wireless networks. In: Proc. NDSS'02, The Internet Society (February 2002)
3. McCune, J.M., Perrig, A., Reiter, M.K.: Seeing-is-believing: Using camera phones for human-verifiable authentication. In: Proc. IEEE Symp. on Security and Privacy, IEEE CS Press (2005) 110–124
4. Saxena, N., Ekberg, J.E., Kostiainen, K., Asokan, N.: Secure device pairing based on a visual channel. Cryptology ePrint Archive, Report 2006/050 (2006)
5. Mayrhofer, R., Welch, M.: A human-verifiable authentication protocol using visible laser light. In: Proc. ARES 2007, IEEE CS Press (April 2007) 1143–1147
6. Goodrich, M.T., Sirivianos, M., Solis, J., Tsudik, G., Uzun, E.: Loud and clear: Human verifiable authentication based on audio. In: Proc. ICDCS 2006, IEEE CS Press (July 2006) 10
7. Soriente, C., Tsudik, G., Uzun, E.: HAPADEP: Human asisted pure audio device pairing. Cryptology ePrint Archive, Report 2007/093 (March 2007)
8. Mayrhofer, R., Gellersen, H., Hazas, M.: Security by spatial reference: Using relative positioning to authenticate devices for spontaneous interaction. In: Proc. Ubicomp 2007. Volume 4717 of LNCS., Springer-Verlag (September 2007) 199–216
9. Mayrhofer, R., Gellersen, H.: Shake well before use: Authentication based on accelerometer data. In: Proc. Pervasive 2007. Volume 4480 of LNCS., Springer-Verlag (May 2007) 144–161
10. Patel, S.N., Pierce, J.S., Abowd, G.D.: A gesture-based authentication scheme for untrusted public terminals. In: Proc. UIST 2004, ACM Press (October 2004) 157–160
11. Soriente, C., Tsudik, G., Uzun, E.: BEDA: Button-enabled device pairing. In: Proc. IWSSI 2007. (September 2007) 443–449
12. Varshavsky, A., Scannell, A., LaMarca, A., de Lara, E.: Amigo: Proximity-based authentication of mobile devices. In: Proc. UbiComp 2007, Springer-Verlag (September 2007) 253–270