Josef Ressel Center for User-friendly Secure Mobile Environments (u‘smile)
University of Applied Sciences Upper Austria
FH OÖ Forschungs&Entwicklungs GmbH

Master's Thesis: Mobile Device-to-User Authentication

Contact
Rainhard Findling
Mobile Authentication, Biometrics, and Machine Learning
Softwarepark 11
A-4232 Hagenberg/Austria
+43 (0)50804-27188
rainhard.findling@fh-hagenberg.at
www.usmile.at
www.fh-ooe.at

Motivation

To prevent malicious interaction with mobile devices, users typically authenticate before using them (PIN, pattern, etc). In contrast, devices usually do not authenticate to users before being used. This enables hardware phishing attacks: attackers exchanges users' devices with malicious devices, which e.g. forward whatever information they receive to the attackers. If users take the phishing hardware for their own devices and authenticate with their credentials, these get forwarded to the attackers and the attack was successful.
One approach to avoid such attacks is mutual authentication (both parties authenticate against each other). Mutual authentication is widely used in machine-to-machine (M2M) communication, e.g. with TLS. In contrast, it is not widely used with humans, due to human factors (limitations in cognitive load, channel bandwidth and calculation power) – although some researched M2M channels could be used for human-machine information exchange as well (cf. [2,3,4,5]). Consequently, there is room for device-to-user authentication suitable for everyday tasks. Previous research [1] has shown e.g. vibration to possibly be suitable for unobstrusive and hard-to-eavesdrop mobile device-to-user authentication. The goal of this thesis is to extent these approaches and evaluate different channels and protocols (cf. Interlock [6]) of device-to-user information transportation. To do so, conceptually all human senses can be employed to sense information from devices.


[wikipedia.org]

Goals

- Different approaches to device-to-user approaches should be identified and compared against each other (all human senses can possibly be used).
- Different protocols to transport device-to-user information on these channels should be identified and compared against each other.
- Combinations of device-to-user channels and channel protocols should be analyzed (properties, attacks, etc), and a number of them should be implemented prototypically on Android. These prototypes should be used to evaluate the corresponding combinations in their performance and effectiveness in user studies.
- The final, selected approach should be implemented as Android application.

Research questions

- Which device-to-user channels are suitable for authentication information? What are their properties, including channel bandwidth and possible attacks?
- Which are suitable protocols to efficiently transport authentication information on these channels?
- Which bandwidth can be expected from evaluation data per channel and protocol? What is the corresponding rate of users recognizing the transported information correctly?

Literature

[1] Towards Device-to-User Authentication: Protecting Against Phishing Hardware by Ensuring Mobile Device Authenticity using Vibration Patterns. 14th International Conference on Mobile and Ubiquitous Multimedia (MUM'15), ACM, 2015, 131-136.
[2] C. Soriente and G. Tsudik and E. Uzun. HAPADEP: Human-Assisted Pure Audio Device Pairing. Information Security, Springer, Berlin Heidelberg, 2008, 5222, 385-400.
[3] N. Roy, M. Gowda and R. R. Choudhury.. Ripple: Communicating through Physical Vibration. 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15), USENIX Association, 2015, 265-278.
[4] P. Roberts, L. Benofsky, W. Holt, L. Johnson, B. Willman and M. Bryant. Systems and methods for determining if applications executing on a computer system are trusted. US Patent 7,721,094, 2010.
[5] M. Long and D. Durham. Human Perceivable Authentication: An Economical Solution for Security Associations in Short-Distance Wireless Networking. Proceedings of 16th International Conference on Computer Communications and Networks (ICCCN), 2007, 257-264.
[6] T. Kindberg, C. Bevan, E. O'Neill, J. Mitchell, J. Grimmett and D. Woodgate. Authenticating Ubiquitous Services: A Study of Wireless Hotspot Access. Proceedings of the 11th International Conference on Ubiquitous Computing, ACM, 2009, 115-124.