Poster: User preferences for biometric authentication methods and graded security on mobile phones

Poster abstract SOUPS 2010

Hanul Sieger
Quality and Usability Lab
Deutsche Telekom Laboratories
Technische Universität Berlin
Ernst-Reuter-Platz 7, 10587 Berlin
hanul.sieger@telekom.de

Niklas Kirschnick
Quality and Usability Lab
Deutsche Telekom Laboratories
Technische Universität Berlin
Ernst-Reuter-Platz 7, 10587 Berlin
niklas.kirschnick@telekom.de

Sebastian Möller
Quality and Usability Lab
Deutsche Telekom Laboratories
Technische Universität Berlin
Ernst-Reuter-Platz 7, 10587 Berlin
sebastian.moeller@telekom.de

1. INTRODUCTION

Conventional protection on mobile phones provides only a one-time verification system upon switch-on: unless locked, the device is always open; and automatic locking of the device is usually not the default setup on the phones of the top 5 vendors [4]. Many users use to keep their devices unsecured as they perceive the usage of a phone PIN (not the SIM PIN) as inconvenient [1] [9].

Our research aims to get an insight into user preferences for graded (multi-level) security mechanisms and alternative (biometric) authentication methods. Graded security is the concept of assigning different levels of security to different applications and data, and to combine these levels with different authentication methods; for example, securing the SMS application with a simple visual code.

2. AUTHENTICATION METHODS ON MOBILE PHONES

While knowledge-based and token-based authentication are used on a regular basis by many people around the world (think ATM cards (token, PIN) and mobile phones (PIN)), biometric authentication methods are at least known to exist (fingerprint and iris recognition in movies etc.) by a part of the users.

Biometric authentication methods are often seen as having advantages over other methods, because no password has to be remembered, no token or written-down note can be lost or stolen, and biometric methods are harder to "crack" [3].

Some biometric methods are less suited for mobile devices, if we consider usability and hardware constraints [3]. For example, palm-print, hand vascular, and hand or ear geometry recognition cannot be implemented due to size requirements. Gait recognition by camera or accelerometer requires motion. 3D object recognition either depends on considerable hardware or would be hard to use alone.

Therefore, we focused on fingerprint; face; iris; speaker; 2D; and 3D gesture recognition; and continuous verification (e.g. typing pattern).

There were and are very few mobile phones available offering other security methods than a 4-digit PIN. Examples of commercially available devices are several models by Fujitsu, e.g. FOMA F905i (released in 2008) with a fingerprint swipe-sensor on the backside, and Sharp 904SH (released in 2006), which uses its front-facing camera for face recognition. Both example devices were released on the Japanese market only. Looking at the U.S. and European market, only the following device was found offering alternative authentication methods: LG eXpo GW820, a Windows Mobile 6.5-based model with a fingerprint sensor to secure access to the phone as well as individual applications and data [5].

3. GRADED SECURITY

Graded security can be seen as either a role-based hierarchical system to provide access to certain areas of the secured device (e.g. from guest-user to super-user); or as a data-based system, where access to specific data is secured by access to this data alone. The user has to provide authentication to get access to data, but there is no overlap to other data, it has to be accessed individually. This is in contrast to the super-user, who can access everything on the system once authentication is passed.

On mobile computers the user may need to provide a BIOS password or fingerprint scan, and then further authentication when to log into his or her user account. People are used to provide authentication to access an e-mail account, a web shop, or a banking account. Thus, we can expect to a certain degree, that users are aware of the concepts of graded security.

4. RESULTS FROM FOCUS GROUP DISCUSSIONS

A focus group discussion with a total of 19 participants was conducted at our lab in Berlin in November 2009 [6]. During the focus group discussions the following authentication methods were demonstrated and discussed: fingerprint recognition with swipe sensor on a laptop computer; 2D gesture recognition using a touch-pad on a laptop computer with our own prototype software; 3D gesture recognition (in analogy to the Nintendo Wii's controller) using a mock-up; iris scan or face recognition with a phone's camera using a mock-up; activity-based verification through keyboard typing patterns using a laptop computer's keyboard with our own prototype software; recognition-based authentication by selecting points on a picture in a specific order using a mock-up; and speaker recognition using a mock-up.

The participants rated the different methods concerning the perceived security and possible use. The evaluations of the authentication methods and graded security levels were introduced with scenarios presented by the moderators. The results show a significant lead for fingerprint recognition as being *both* secure and usable (see Tables 1, 2).

Table 1: Focus groups – "I think this method is secure"

Iris recognition	100%
Fingerprint authentication	95%
Speaker recognition	68%
Face recognition	64%
Activity-based verification	63%
2D gestures	63%
3D gestures	42%
Recognition-based authentication	37%

Table 2: Focus groups – "I would use this method"

Fingerprint authentication	95%
2D gestures	63%
Recognition-based authentication	47%
Activity-based verification	42%
3D gestures	37%
Speaker recognition	37%
Face recognition	27%
Iris recognition	26%

This leads to an interesting preference for graded security, which we addressed in asking "How should security levels be combined with authentication methods?". Instead of assigning each security level a "matching" method (lower security levels match with less secure authentication methods) a "one size fits all" approach (fingerprint) was preferred [6].

5. RESULTS FROM WEB SURVEY

In the time as the focus group discussions took place we also conducted a web survey with a similar set of questions to cross-validate the findings of the focus group discussions. The survey consisted of 64 questions with closed answers on a 6-point Likert scale. It generated 308 individual responses in its run-time of two weeks.

Table 3: web survey – "perceived as high level of security by method"

Fingerprint recognition	75%
Face recognition	44%
Speaker recognition	30%
PIN	29%
Gesture recognition	14%
Iris recognition	6%

Table 4: web survey – "future use by method"

Fingerprint recognition	49%
PIN	35%
Face recognition	23%
Speaker recognition	23%
Iris recognition	21%
Gesture recognition	16%

The results support the trends found in the focus groups (see Table 3 and 4) [9]. The results are also in line with earlier findings, where fingerprint recognition got also the highest rating in a survey [7] [8].

6. CONCLUSIONS

The results show a significant lead for the finger-print method. Mobile phones are operated by using one or two fingers and fingerprint authentication fits this context of use. Speaker recognition would also fit, but is sometimes seen as awkward (especially in crowded places) as remarks in the focus groups revealed. An iris scan, for example, would interrupt the finger-driven work-flow. We can conclude, that authentication methods breaking the operating mode are considered as inconvenient. In this way, an "optimum" could be reached by combining a touch screen with a fingerprint reader (which is not commercially available yet). When the user tabs on an application icon, the phone would automatically authenticate the user, providing a seamless experience.

An additional layer of security to secure single applications or data would suffice for most participants. The findings in the focus groups revealed, that if an authentication method was perceived as convenient *and* secure, the consensus was to use it throughout for all security levels instead of combining low security levels with less secure authentication methods.

7. REFERENCES

[1] Tognazzini, B.: Design for Usability. In: Cranor, L.F., Garfinkel, S. (eds.): Security and Usability. Designing Secure Systems That People Can Use. O'Reilly (2005)

[2] Imperva Application Defense Center: Consumer Password Worst Practices. Imperva 2010 at `www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf`

[3] Jain, A.K., Flynn, P., Ross, A.A. (eds.): Handbook of Biometrics. Springer (2008)

[4] IDC press release from 28 Jan 2010 at `www.idc.com/getdoc.jsp?containerId=prUS22186410`

[5] Examined websites (as of early February 2010): Apple, Inc.: `www.apple.com`, LG Electronics, Inc.: `www.lge.com`, Motorola, Inc.: `www.motorola.com`, Nokia Corp.: `www.nokia.com`, Research in Motion Ltd.: `www.rim.com`, Samsung Electronics Co. Ltd.: `www.samsumg.com`, Sony Ericsson Mobile Communications AB: `www.sonyericsson.com`

[6] Dörflinger, T., Voth, A., Krämer, J.: "My Smartphone is a Safe!" The user's point of view regarding novel authentication methods and gradual security levels on smartphones. SECRYPT 2010

[7] Clarke, N., Furnell, S., Reynolds, P.: Biometric authentication for mobile devices. In: Proceedings of the 3rd Australian Information Warfare and Security Conference, Perth, Western Australia, 28-29 Nov 2002

[8] Clarke, N., Furnell, S.: Authentication of users on mobile telephones. A survey of attitudes and practices, In: Computers & Security, Volume 24, Issue 7, October 2005, Pages 519-527

[9] Ben-Asher, N., Ben-Oved, A., Meyer, J.: Preliminary survey results - project "Graded Security for Mobiles". Deutsche Telekom Laboratories 2009