

Poster: Preliminary Investigation of an NFC-Unlock Mechanism for Android

[SOUPS 2013 Poster Abstract]

Sandra Flügge, Hannes Scharf, Sascha Fahl, Matthew Smith
Distributed Systems and Security Group, Dept. of Computer Science
Leibniz Universität Hannover, Germany

1. INTRODUCTION

Protecting mobile phones with password, pins, gestures and other types of authentication mechanisms is a hot topic, since ever more sensitive information is stored on peoples' phones and the usability of current systems still leaves much to be desired[3]. New techniques of authentication to a phone - unlocking it - which are fast, easy to use and secure are needed [1]. In this poster we present a preliminary study of a new unlock method which uses NFC tags as authentication tokens. The NFC based unlocking mechanism was developed by a student of the DCSec group at the University of Hannover [4] and will be described in the next section. To evaluate which features of this system need to be improved and how to proceed with the further development, we designed and conducted a user study. The results of this study will be presented in this poster.

2. NFC-UNLOCK

NFC-Unlock [4] is an Android application that allows users to unlock their smartphone with a NFC tag in addition to a PIN based unlock. The prototype NFC-Unlock software was implemented as an app to offer easy deployability. Once the app was installed on the smartphone, the user is guided through a setup phase, during which a PIN is set and an NFC tag is bound to the app. The binding of the NFC tag is accomplished simply by holding the NFC tag next to the phone when prompted, which completes the setup phase. The app registers for screen-on events and goes into the foreground when such an event occurs, presenting a lock screen, which becomes visible after a short lag.

The unlock screen offers the user two alternative means of unlocking the device. The user can either unlock the phone by holding it next to the NFC tag or by entering the PIN. After either holding the NFC tag close to the phone or entering the PIN, the user must press the OK button. If the correct PIN or NFC tag was provided, the software grants the user access to the home screen. However, that the prototype was implemented as an app leads to two drawbacks: Firstly, the app cannot override the recently-used apps quick-change feature and thus it is possible to circumvent the unlocking mechanism using this feature. While this is of course a serious security issue, the trade-off was made to have better deployability for the prototype testing phase. Secondly, the NFC feature of Android does not run when the phone is in sleep mode, thus the user must manually wake the phone from sleep mode by pressing a button before the unlocking the phone with the NFC tag. This is certainly due to battery preservation measures of Android. While a custom Android

image could change this behaviour, it would also impact the battery life. Since unlocking the phone with a PIN also requires the phone to be woken from sleep by a button press, one issue that our study wanted to evaluate was whether this battery/usability trade-off was desirable or not.

3. EXPLORATORY STUDY

To evaluate the usability of NFC-Unlock, we conducted an exploratory study. For the study the NFC-unlock app was modified to log when the phone is unlocked and which method for unlocking was used. To reduce the negative impact on ecological validity we wanted the participants to use their real phones during the study, instead of handing out pre-prepared study devices. The down-side of this decision was that this introduced a tech-bias, since the participants needed a current Android phone capable of NFC. We were able to recruit 5 participants (4 male, 1 female, average age 25.4) all of whom had an IT-background. However, since the NFC-unlock app is still and we were interested in getting expert feedback, we believe this bias is actually beneficial. All participants got an introduction to the software, including a warning that the app is a prototype and that using the recent-app switching feature of Android the unlock could be circumvented. The participants were then asked to use the NFC-unlock app for one week on their main mobile phone. After this period the participants were invited to an interview and debriefing. As mentioned in the previous section, the NFC-unlock app logged the unlock method and a timestamp of the unlock event. In figure 3 we show the results of the log files where 'NFC' and 'PIN' stand for the unlock method respectively and 'FAIL' for a failed unlock attempt. As can be seen two of the five participants used the NFC unlock more than the PIN, but none did so exclusively.

To evaluate the usability of the software we asked the participants to fill out a system usability scale (SUS) for us. The results are shown in figure 1 for every participant respectively. Since this was an early prototype we did not expect a great result and we believe the result of an average SUS score of 47 reflects the early stage of the prototype more than the method itself.

During the interview the main issue we found was that our participants were annoyed by the fact that they still had to click OK after using the NFC tag, although carrying the token as a second factor was also mentioned as a down side. There were also some instances of the NFC-unlock feature activated at inconvenient moments.

We also asked the participants to rate how secure they felt the different unlock methods PIN, Pattern and NFC were on

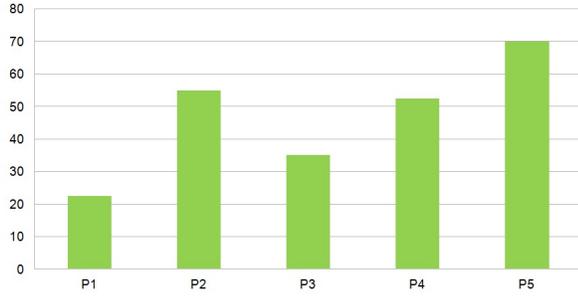


Figure 1: SUS Score of NFC

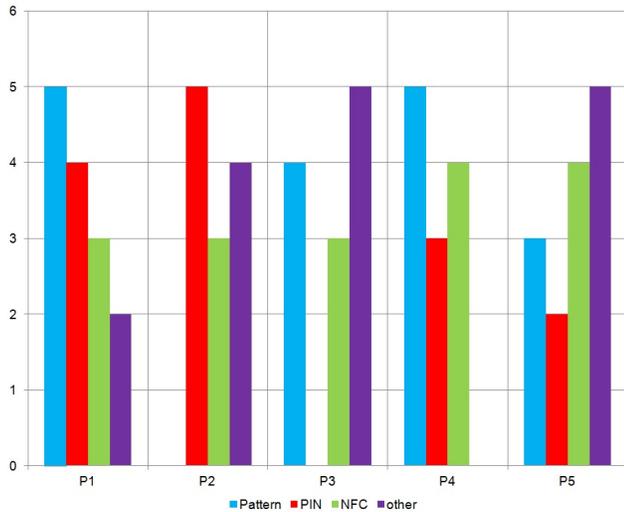


Figure 2: Ranking of NFC, Pattern and PIN Unlock

a 5 point Likert scale. Figure 2 shows this ranking, where 'other' stands for other unlock methods mentioned by the participants during the interview such as face-unlock and password. We want to remind the reader at this point, that although we asked the participants to discount the recent-app issue, it is fairly likely to have subconsciously biased their security perception.

The following shows some notable quotes of our participants¹.

"Without the OK button NFC-Unlock would be a good alternative to unlock my smartphone."

"During a call I wanted to check a telephone number on my smartphone but the NFC-Unlock blocked my screen, that's not good."

"Although I had to press the OK button, the method was fast anyway"

"The tag is an additional thing that I have to take with me all the time."

"It was good to be able to fall back on the PIN entry, for the times when I did not have the tag with me."

¹Quotes were translated from German to English

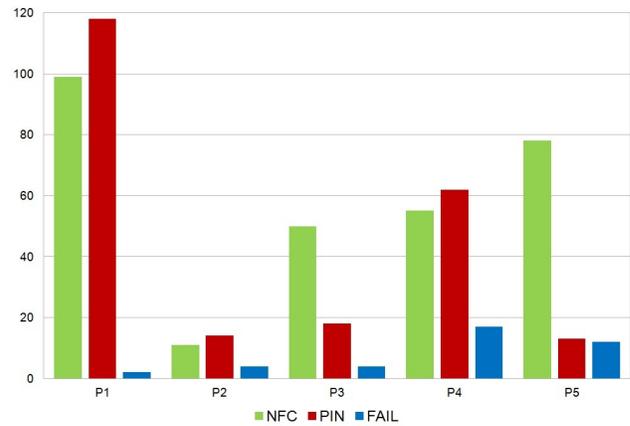


Figure 3: Number of unlocks per participant

4. CONCLUSION AND FUTURE WORK

The preliminary study fulfilled its main goal of field testing the prototype to get feedback for the next design phase. Based on the results of the study we are planning the following steps: While it seriously hampers deployability, the next version of the prototype will be integrated into the core Android OS to fix the recent-app and lag issues and to be able to experiment with an always-on NFC system. The following suggestions of our study participants will also be adopted:

"I wish I could use more tags to unlock my smartphone."

"A good feature would be multi-user in NFC-Unlock."

"I would use the software if it allowed me to combine NFC-Unlock with pattern unlock."

While there were a number of issues which hampered the usability of our prototype, we believe the above changes will alleviate these issues and create an interesting alternative to traditional authentication mechanisms for smart phones.

5. REFERENCES

- [1] N Asokan and Cynthia Kuo. Usable mobile security. In *Distributed Computing and Internet Technology*, pages 1–6. Springer, 2012.
- [2] A Malm. Handset connectivity technologies. Technical report, Berg Insight, Tech. Rep, 2011.
- [3] Xiaoyuan Suo, Ying Zhu, and G Scott Owen. Graphical passwords: A survey. In *Computer Security Applications Conference, 21st Annual*, pages 10–pp. IEEE, 2005.
- [4] Marcus Wobig. Entsperren von Android Smartphones mit Hilfe von NFC. 2012.