Investigating Re-authentication Schemes for IA-Enabled Applications

Lalit Agarwal and Urs Hengartner

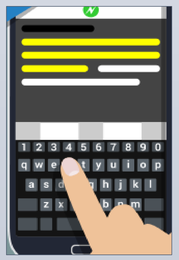
Cheriton School of Computer Science, University of Waterloo

IMPLICIT AUTHENTICATION (IA)

- IA schemes continuously and transparently authenticate users using their behavioral information such as their touch input, keystroke behavior etc.
- It prevents unauthorized access by an adversary to an application that implements an IA scheme.
- It provides security to users who do not use a traditional authentication scheme.
- At the same time, IA reduces the time to complete tasks by constantly monitoring users in the background instead of asking them to authenticate explicitly.
- Some of the current IA schemes being used are:

TOUCH-IA

GAIT-IA



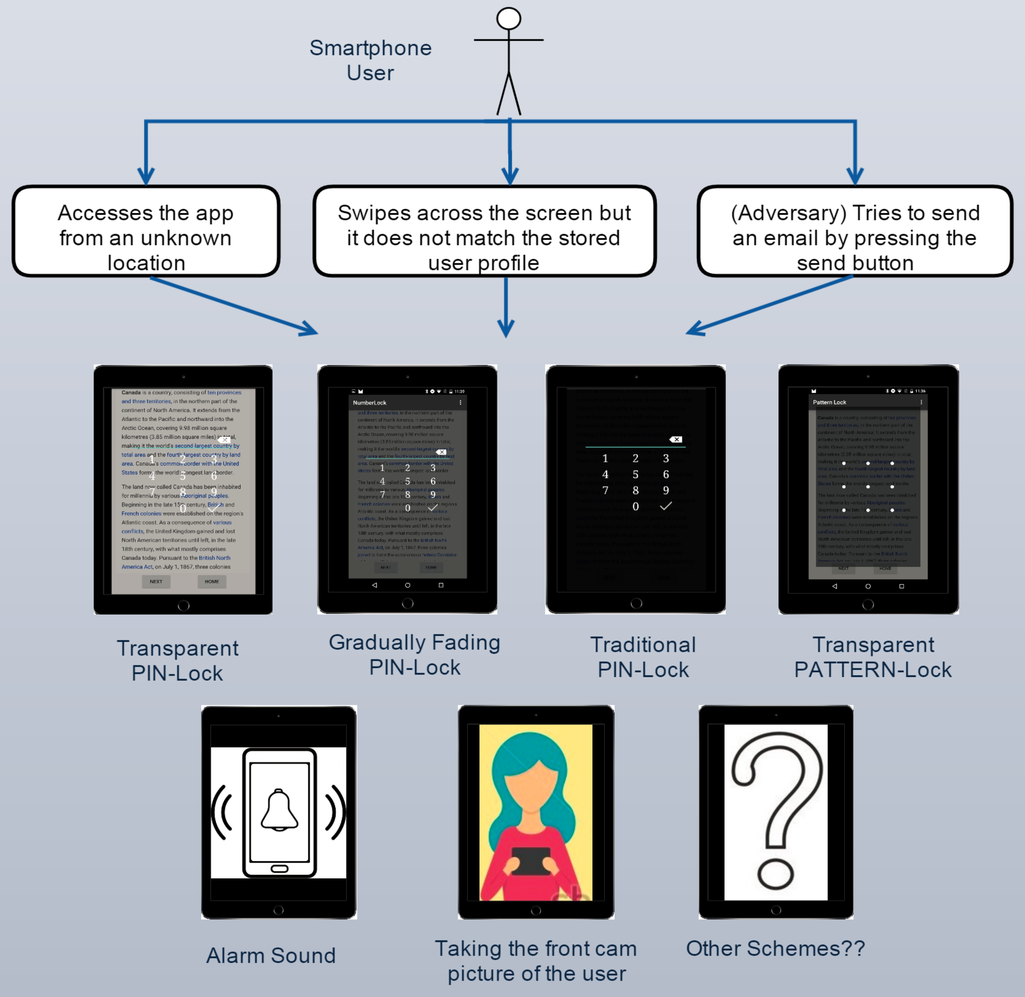
KEYSTROKE-IA

PROBLEMS WITH CURRENT IA SCHEMES

- Current IA schemes are subject to **false rejects (FRs)** and sometimes identify a legitimate user as an adversary.
- A recent study [1] has shown that frequent FRs lead to annoyance among the users due to unpredictable nature of these FRs.

SCHEMES FOR RE-AUTHENTICATING USERS

- We proposed few schemes to re-authenticate the users in case the system detects an anomalous behavior that meet the following goals:
- **USABILITY**
  - Allow a legitimate user to continue with his current task with least obstruction
  - Should be less annoying in case false rejects are frequent
  - Allow the users to easily set-up re-authentication scheme parameters for any application
- **SECURITY**
  - Prevent an adversary from accessing the app from thereon
  - Obscure as much information as possible from the screen
- **FLEXIBILITY**
  - Allow app developers to easily include these schemes with their applications



PLANNED WORK

- We plan to conduct an in-lab experiment to evaluate the usability of the schemes.
- During the experiment, the users will have to read and respond to a few emails using our email application on a Nexus 5 device. They will be shown one of these schemes at various intervals while they are completing the task.
- At the end of the task, we will ask the users to give their feedback and evaluate the schemes.
- Some of the research questions we will try to answer are:

R1) Do the re-authentication schemes reduce the annoyance caused among users due to frequent FRs?

R2) Do these schemes help in making IA more secure?

R3) Is there any particular scheme that users prefer more over other schemes?

R4) Is the preference of schemes consistent across a variety of apps such as messaging apps, utilities apps etc.?

REFERENCES

1. Khan, Hassan, Urs Hengartner, and Daniel Vogel. "Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying." Symposium on Usable Privacy and Security (SOUPS). 2015.
2. Khan, Hassan, Aaron Atwater, and Urs Hengartner. "Itus: an implicit authentication framework for android." Proceedings of the 20th annual international conference on Mobile computing and networking. ACM, 2014.