User Perceptions of Usability and Security of Authentication Methods for Mobile Banking on Smartphones

Lenka Knapová, Agáta Kružíková, Lenka Dědková & David Šmahel

Cyberspace 2019 Presentation (Usable Security & Privacy Track)
30. 11. 2019, Brno, Czech Republic
Project Introduction

• *Innovation and adaptation of authentication technologies for secure digital environment*

• 2/2018-2/2020

• Supported by Technological Agency of Czech Republic

• Cooperation between Centre for Research on Cryptography and Security at the Faculty of Informatics Masaryk University, Interdisciplinary Research Team on Internet and Society at the Faculty of Social Studies MU, and AHEAD iTec, s.r.o./Monet+
Background

• Mandatory 2FA since September 2019
• Widely used SMS code
• Need for a different authentication method that is
  • Easy to use
  • Secure
  • Well-accepted

• Qualitiative User Study → Large-Scale User Study
Large-Scale User Study

• Goal: To evaluate usability, perceived security, and preference of various authentication methods
  • Token vs. card-reader
  • PIN, fingerprint
• N = 250 (aged <55) + 250 (aged 55+)
• Preliminary results
Study Design

- **Scenario Evaluation**
  - **TOKEN**
  - **CARD-READER**

- **Questionnaire**
  - Demographics
  - Security Attitudes
  - Smartphone Security Behavior

- **Scenario Evaluation Questionnaire**

- **Questionnaire**
  - Authentication Method Evaluation
  - Authentication Method Usage
  - Online Banking Usage
Scenarios

• NFC token
• Card-reader and card PIN
• + PIN code and fingerprint

• 2 applications
  • IDport authentication application
  • YourBank MBanking application

• 2 tasks
  • Activate IDport
  • Pay for a vacation (money transfer)
Sample

**Age group <55**
- N = 250 (238)
- Data collected by a professional survey agency
- Representative sample

• Age $M = 38.76$, $SD = 9.16$
• Males 45%, females 55%
• Education
  - Primary 4.2%
  - Secondary 62.6%
  - Tertiary 33.2%
• Work status
  - Full-time 69.3%
  - Part-time 9.2%
  - Maternity leave 11.8%
Results

- Perceptions of „tested“ authentication methods: PIN, fingerprint, token, card-reader
  - Easy to use, practical, secure
  - Predictors of usability and security

- Preferences for specific authentication methods and their combinations
AGE <55

<table>
<thead>
<tr>
<th>Method</th>
<th>Easy to use</th>
<th>Practical</th>
<th>Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>M</td>
<td>SD</td>
<td>M</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>1.60</td>
<td>1.33</td>
<td>1.65</td>
</tr>
<tr>
<td>PIN</td>
<td>2.11</td>
<td>1.46</td>
<td>2.17</td>
</tr>
<tr>
<td>Token</td>
<td>2.10</td>
<td>1.67</td>
<td>2.86</td>
</tr>
<tr>
<td>Card-reader</td>
<td>2.64</td>
<td>1.90</td>
<td>3.43</td>
</tr>
</tbody>
</table>
How EASY TO USE do you find these methods?

- **fingerprint**: 74% easy, 14% somewhat easy, 4% neither, 1% somewhat difficult, 4% difficult
- **PIN**: 47% easy, 26% somewhat easy, 12% neither, 6% somewhat difficult, 5% difficult
- **token**: 56% easy, 19% somewhat easy, 9% neither, 4% somewhat difficult, 4% difficult
- **card-reader**: 40% easy, 20% somewhat easy, 13% neither, 8% somewhat difficult, 6% difficult
How PRACTICAL do you find these methods?

- **fingerprint**: 72, 12, 7, 3, 21, 3
- **PIN**: 46, 23, 14, 8, 3, 4, 1
- **token**: 35, 18, 10, 7, 7, 7
- **card-reader**: 24, 19, 10, 10, 7, 14
How SECURE do you find these methods?

- **fingerprint**: 63, 14, 7, 6, 4, 1, 4
- **PIN**: 26, 28, 19, 18, 6, 4, 3
- **token**: 26, 22, 20, 16, 6, 7, 3
- **card-reader**: 28, 24, 23, 11, 6, 6, 2
Usability & Security DV

• Easy to use + practical → **Perceived usability**
  • Cronbach’s $\alpha$.862 (fingerprint), .729 (PIN), .792 (token), .820 (card-reader)
• Secure → **Perceived security**

• **Predictors**
  • Demographics: age, gender, education
  • Smartphone security behavior scale Cronbach’s $\alpha$ = .751
  • General security orientation .687, Perceived vulnerability .731, Perceived seriousness .883, Smartphone Self-Efficacy .833
Regression Analyses

• 4 (fingerprint, PIN, token, card-reader) x 2 (usability, security) DV

• 1: demographics

• 2: smartphone security behavior and attitude scales
  → no consistent relationships emerged for usability or security
  → Card-reader
    • Age: the older the more usable/secure
    • Smartphone Secure behavior: the more secure they behave, the more usable/secure
Regression Analyses (continued)

Token & card-reader X usability & security
• 1: demographics
• 2: smartphone security behavior and attitude scales
• 3: scenario evaluation – easy to complete, time, instructions

• + 4: objective data from screen recordings
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Token</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Card-reader</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Token</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card-reader</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

- Fingerprint: +
- PIN: +
- Token: +
- Card-reader: +

- Task: Simple: +
- Task: Time: -
- Task: Instructions: -
• USABLE
• SECURE

• Which methods would participants actually use for online banking?
Preferences for AUTHENTICATION METHODS for online banking

- **Simple confirmation**: Would NEVER use: 38, For LOW amount only: 37, For LOW & HIGH amount: 19, For HIGH amount only: 6
- **PIN code**: Would NEVER use: 11, For LOW amount only: 38, For LOW & HIGH amount: 35, For HIGH amount only: 16
- **Password**: Would NEVER use: 17, For LOW amount only: 43, For LOW & HIGH amount: 28, For HIGH amount only: 12
- **Fingerprint**: Would NEVER use: 14, For LOW amount only: 21, For LOW & HIGH amount: 46, For HIGH amount only: 20
- **Token**: Would NEVER use: 29, For LOW amount only: 25, For LOW & HIGH amount: 27, For HIGH amount only: 19
- **PIN + token**: Would NEVER use: 24, For LOW amount only: 15, For LOW & HIGH amount: 33, For HIGH amount only: 28
- **Fingerprint + token**: Would NEVER use: 25, For LOW amount only: 6, For LOW & HIGH amount: 39, For HIGH amount only: 31
- **Card-reader + card PIN**: Would NEVER use: 27, For LOW amount only: 11, For LOW & HIGH amount: 34, For HIGH amount only: 28
Implications

• Perceptions of usability, practicality, and security of the four authentication methods generally positive

• *Fingerprint wins the game*: security perceptions vs. reality

• Card-reader vs. Token: token slightly easier to use and more practical

• Preferences for 2FA combinations
  • Not a clearly preferred or unpopular combination
  • Offer a choice?

• Predictors of usability and security need further exploration
  • validation on the second sample
Limitations and Future Steps

• Preliminary analyses
• Evaluation of methods affected by performed tasks on smartphone
• Finish data collection + data cleaning
• Evaluate predictors in more detail
  • Include objective data from tasks
Thank you for Your attention.

Questions?