In-Depth User Evaluation of m-Banking Authentication Application

AHEAD iTec workshop: New trends in combining high security and user experience of mobile applications

30. 11. 2019

Agáta Kružíková, Petr Doležal, Lenka Knapová

CROCS
Centre for Research on Cryptography and Security

Project Introduction

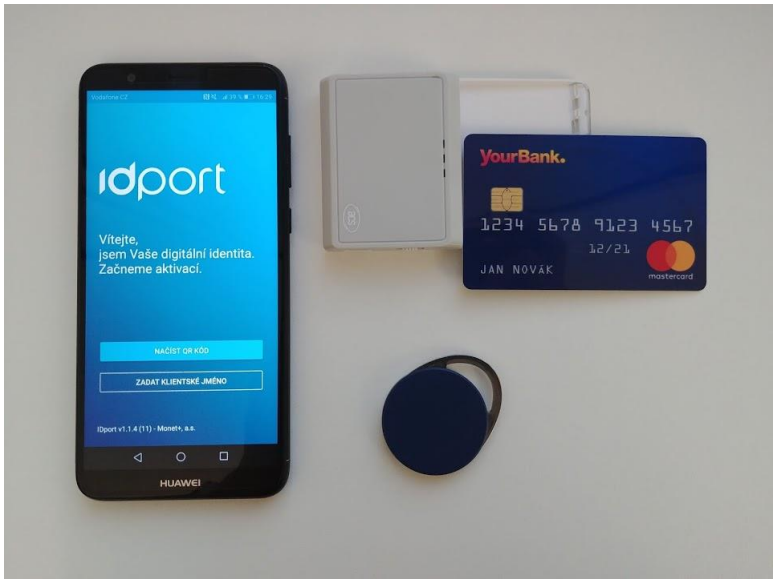
- ***Innovation and adaptation of authentication technologies for secure digital environment***
- 2/2018-2/2020
- Supported by Technological Agency of Czech Republic
- Cooperation between:
  - Centre for Research and Applied Cryptography
  - Interdisciplinary Research Team on Internet and Society
  - Monet+/AHEAD iTec

Motivation

- People do not want to use authentication method:
  - Which is not trustworthy for them
  - Nobody else uses it
  - It is not easy to use
- Secure solution != success in adoption
- Mandatory two factor authentication (2FA) for banking services in Czech Republic (from September 2019)

Investigated Authentication Methods

- One-time SMS code
- Numeric PIN code
- Hardware token (FIDO token, NFC token)
- Payment card with and without smartcard reader
- Fingerprint



User Study Design

- Study description
- Demographic questionnaire
- Getting familiar with the test smartphone
- Scenario description
- Fulfilment of the tasks
- Questionnaires and interviews based on the fulfilled tasks

Scenario Description

- IDport – application of digital identity recommended by participant bank
- Activation of IDport
  - QR code or user name and activation code
  - Choosing of personal PIN code and checking fingerprint
- Login to internet or mobile banking
- Payment of the bill(s)
- Checking of account balance

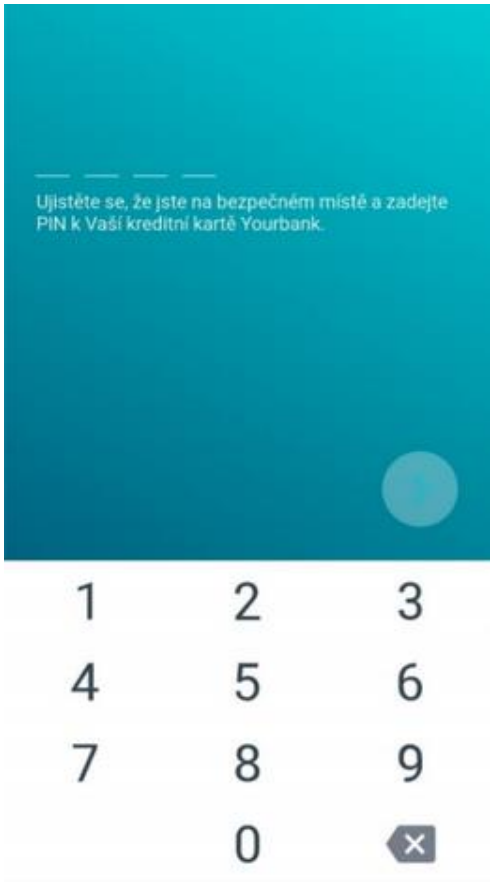
Iterative Process

- 1st round
  - One-time SMS code, FIDO token, payment card with smartcard reader
- 2nd round
  - FIDO token, payment card with smartcard reader
- 3rd round
  - payment card
- 4th round
  - NFC token, payment card with smartcard reader

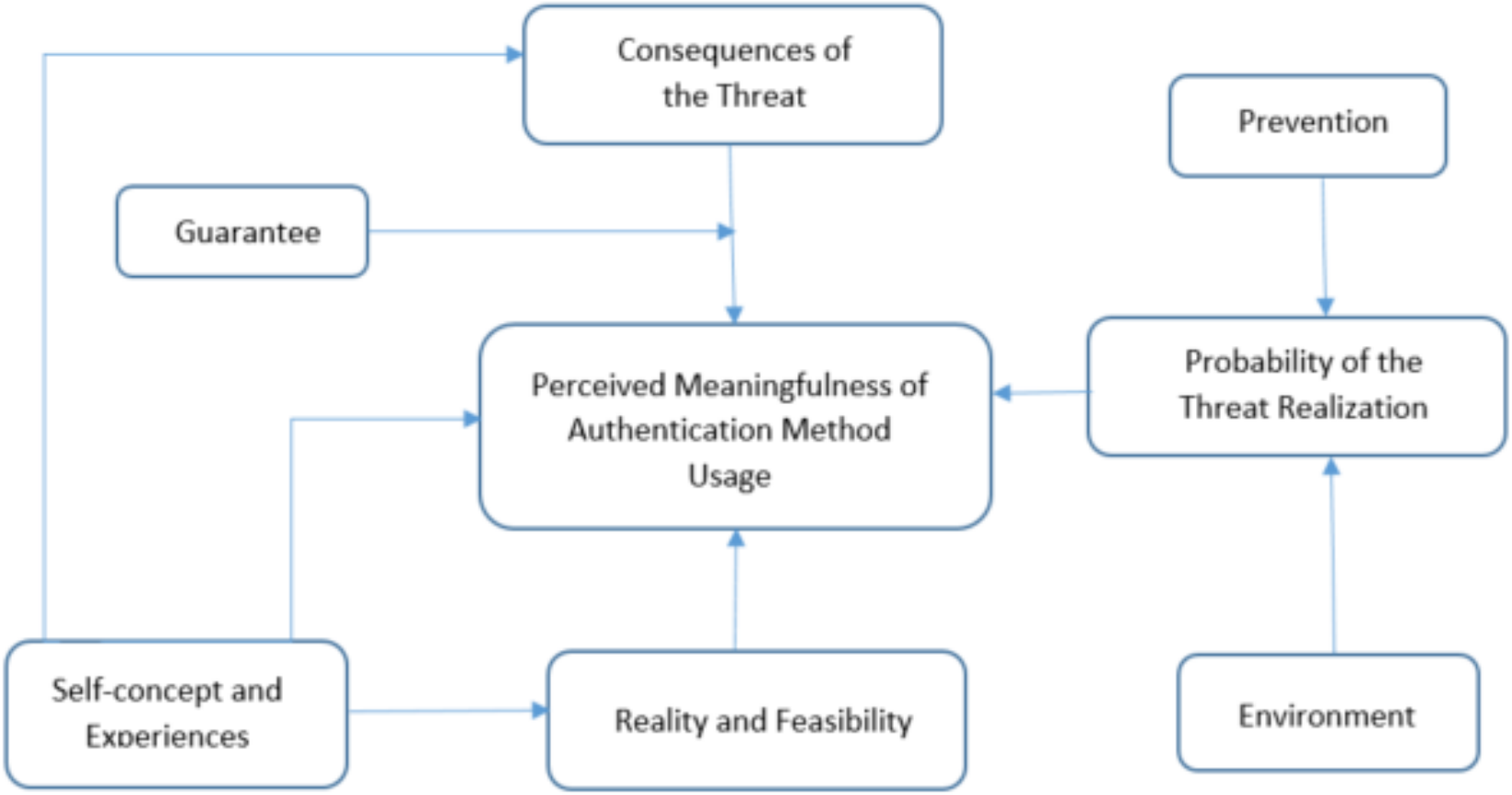
Changes According to the Results

Changes According to the Results

Changes According to the Results



Mental Model



Perceived Meaningfulness of Authentication Method Usage

- Need to see some benefit for an „extra work“
- Banking context – money protection
- Balance
  - Authentication method cannot be:
    - Too easy
    - Too complicated

Probability of the Threat Realization

- The threat is perceived as something
  - Materialized
  - Close
  - Present
- Theft (smartphone usually close to the wallet)
- Kidnapping (bank credentials are not a target)
- Type of an attacker
  - Industry espionage
  - Random person (with/without expert knowledge)

Probability of the Threat Realization Prevention and Environment

- To follow some basic security rules
- Possibility of prevention (fingerprint vs. PIN)
- Mistakes in prevention

- To be alone in a safe space vs. to be in a public place
- Large amount of money is usually transferred at home

Consequences of the Threat

- Money losts
- Physical injury (personal health)
- Stolen token
  - No access for the token owner to the banking application
- Stolen credentials (user name and password)
  - A bank account owner has still access
- Stolen payment card – shopping

Reality and Feasibility

- Technical feasibility (no science-fiction)
- Feasibility – how to fulfil some tasks without payment card?
- Denial of access to the authorized person
- Significant users' trust
- More important than security

Self-concept and Experience

- „I trust myself.“ – no need to confirm it again
- 2FA in general is ok, but should not impact users’ flexibility
- Feeling of control – „I know my needs best.“
- Transparency is more important than amount of screens/steps
- Illusion of understanding what is going on

Thank you for your attention!

Questions?