How Users Perceive Authentication of Choice on Mobile Devices

- **Akintunde Jeremiah Oluwafemi**
- **Jinjuan Heidi Feng**

Presenter

Akintunde Jeremiah Oluwafemi

Towson University
aoluwa2@students.towson.edu

Akintunde Jeremiah Oluwafemi is a Doctorate candidate in Towson University with research focus on usable security. In addition , he is also an Information Security Professional and Adjunct Faculty in Towson University

INTRODUCTION AND MOTIVATION

The goal of the authentication is to enable users to perform their primary tasks securely with minimal interference from the actions required to ensure security and privacy.

The goal of this study is to investigate user's perception of Authentication of Choice, which is a concept designed to find balance between usability and Security of system

AUTHENTICATION OF CHOICE

Authentication of choice concept was developed to improve the usability of the system without compromising the security. This allow users to choose their preferred authentication method(s), instead of system mandating a specific authentication method for users.

POTENTIAL BENEFIT OF AUTHENTICATION OF CHOICE

- ❑Increase in usability of the system : Freedom to select authentication method(s) of choice will make the system more usable to the users (Mayron et al, 2013).
- ❑Universal Accessibility : Users will be able to use the system regardless of their personal or environmental limitations (Mayron et al, 2013).
- ❑Increase in Security of the system: Users are known to be the weakest link in security of system, if the user choose authentication method, they are comfortable with, it will reduce possibility of compromising the security of the system

BACKGROUND OF THE STUDY

Previous studies confirmed the tradeoff between the security and usability of authentication methods currently in use.

A particular measure that improves the security of the authentication mechanism usually has a negative effect on the usability of the system [Yee, 2002].

To develop a system that is usable and secure, system developers need to adopt design techniques that allow users to make decisions (Cranor et. al ,2014).

BACKGROUND OF THE STUDY

There is no single authentication method that can accommodate all users. People have different preferences for the authentication method based on their cognitive skills or physical abilities (Belk M. et al, 2013).

The operating environment also affect the choice of authentication system. An authentication method that works perfectly in an environment may not work in another environment.

BACKGROUND OF THE STUDY

AUTHENTICATION METHODS

Knowledge-Based : This depends on what the user must know to verify his identity to the system e.g. Alphanumeric, PIN

Pro: It is relatively easy to implement and have lower operating cost (Lampson, 2002)

Con: Memorability problem impact its usability and security (Katsini, 2016)

Inherent Factors based: This is based on what the user is (Biometrics), this can use either physiological or behavioral traits of the user e.g. Fingerprint, Face recognition.

Pro: Relatively more usable and more secure (Cohen et al, 2011)

Con : Possibility of permanent compromising of the biometric feature (Cohen et al, 2011) Environment and situation may affect implementation (Stephanidis et al ,2013)

BACKGROUND OF THE STUDY

Possession-Based Authentication:

Pro: It is relatively more acceptable to users

Con : More difficult to manage

Can be lost, stolen or shared (Habtamu Abie, 2006)

Multifactor Authentication : Combination of two or more authentications factors

Pro

Provide higher level of security (Banyal, 2013)

Con

Multi factor authentication might make system more difficult to use (De Cristofaro et al. 2013)

METHODOLOGY

We developed an Android-based mobile device application called ‘Event Manager’. The Event Manager app supports five authentication methods and provides a calendar for managing daily schedule.

The five authentication methods supported are common Authentication methods on mobile devices:

- Alphanumeric username and password
- PIN
- Fingerprint authentication
- Facial recognition
- One-Time-Password (OTP)

METHODOLOGY

A within-group design was adopted with three conditions for authentication:

- Alphanumeric username and password
- One-factor AoC: In this condition, participants chose one authentication method out of five options provided
- Two-factor AoC: In this condition, participants chose two authentication methods out of the five options provided

After the participants completed the tasks under all conditions, they answered questionnaire via a Google Form. 75 participants completed the study

RESULT

- Login Time : The participants took significantly longer time to login under the alphanumeric username/password condition than the one-factor AoC condition and the two-factor AoC condition.

- Attitude toward security and usability

Level of Importance	Security	Ease of use
1 (Not at all)	0	0
2 (Slightly important)	0	0
3 (Important)	0	6
4 (Fairly important)	6	6
5 (Very important)	69	63

- User perception of authentication on mobile phones

Methods	Most Secure	Easiest of use
Alphanumeric password	2	2
PIN	2	6
Fingerprint	50	42
Facial authentication	18	23
Gesture/Pattern	1	2
Voice authentication	2	0

RESULT

Test conditions choice based on criterion

	Alphanumeric password as top preference	**One-factor AoC as top preference**	**Two-factor AoC as top preference**
Number of participants	3	63	9
Efficiency	2	34	3
Ease of use	2	51	3
Security	2	54	7
Memorability	0	28	1

User perceptions of Two- Factor AOC

Perceptions	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Improves Security	0	2	5	11	56
Takes too much time	17	25	11	13	8
Difficult to remember	29	29	11	5	0
Difficult to use	21	34	11	7	1

DISCUSSION

The results suggested that, on a mobile phone, both one-factor authentication of choice and the two-factor authentication choice are significantly more efficient than the alphanumeric password method.

The participants highly valued security and privacy both from the general perspective and in the specific context of mobile phone usage.

CONCLUSION AND FUTURE WORK

This study provided insights about user performance, preferences, and perception of the authentication of choice approach on mobile devices during their initial interaction with this approach.

The efficiency and the user subjective perception suggest that the AoC approach has the potential to serve as a usable and secure authentication solution on mobile devices.

Future research is needed to confirm the findings of this study on other platforms and longer period of user interaction.

THANK YOU

Acknowledge

We sincerely appreciate Edward Miklewski for his assistance in data collection and our appreciation goes to all the participants of this study.

For more information about the research you can reach out to :

- Akintunde Jeremiah Oluwafemi
  aoluwa2@students.towson.edu / tunnap@gmail.com
- Jinjuan Heidi Feng

  jfeng@towson.edu

QUESTIONS