
# REPLICATE: Countering Concurrent Login Attacks in "Just Tap" Push-based Authentication

## A Redesign and Usability Evaluation

**Jay Prakash**

Clarice Chua, Tanvi Thombre , Andrei Bytes , Mohammed Jubur , Nitesh Saxena , Lucienne Blessing , Jianying Zhou , and Tony Q.S Quek

Silence Laboratories

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

TEXAS A&M UNIVERSITY

SUTD-MIT INTERNATIONAL DESIGN CENTRE (IDC)

Innovation Ready Design

# This paper highlights issues and proposes a solution for usable push notification based 2FA.

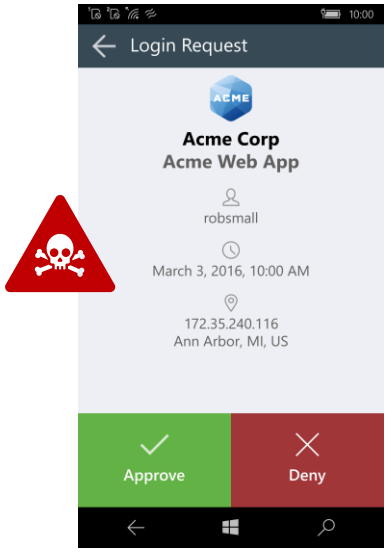
1. The current 2FAs, especially Just Tap to authenticate, are not secure enough.


2. Proposes usable methods to fix the Vulnerabilities.

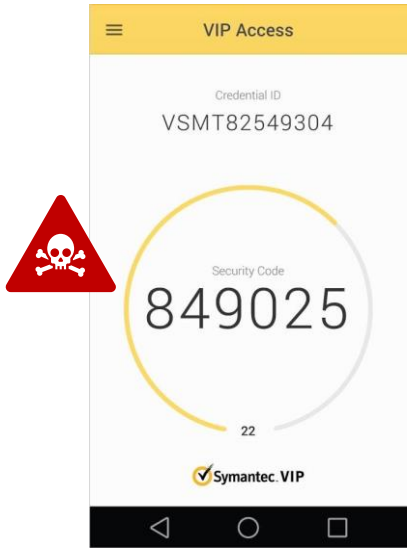
Our method:
**REPLICATE to Authenticate.**

# The Bigger Problem on Target?

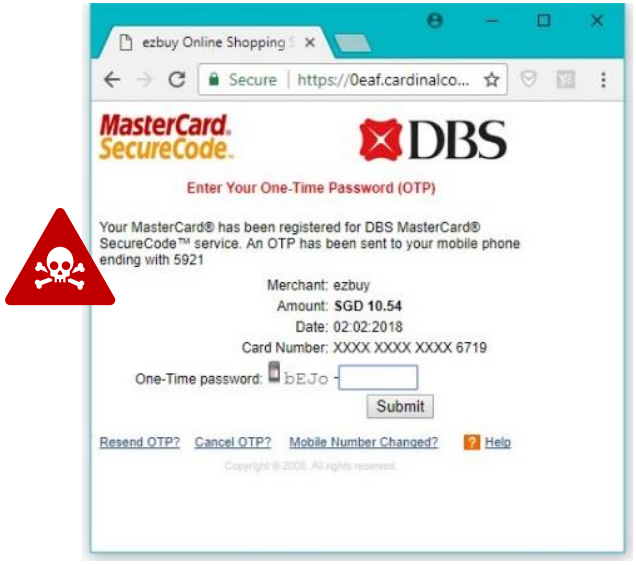
## Current solutions do not have balance between Usability and Security.




Tap to Auth




In-app generator

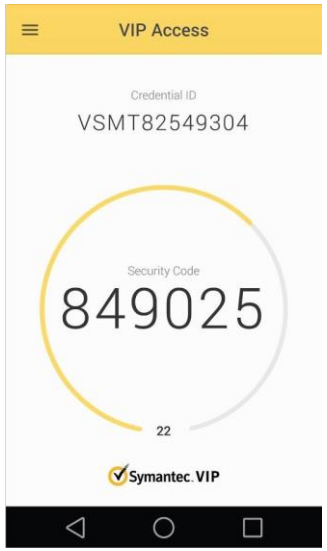


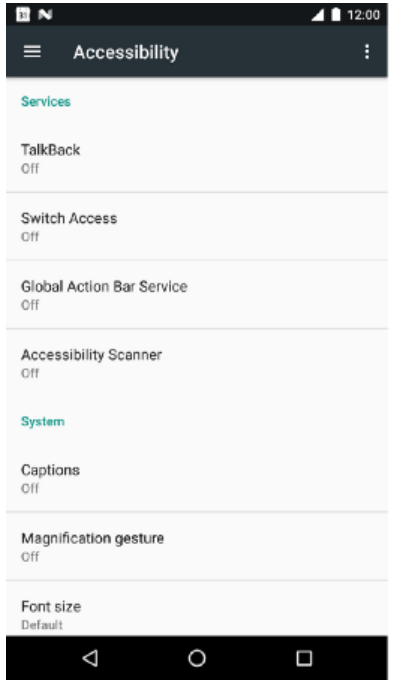

SMS OTPs

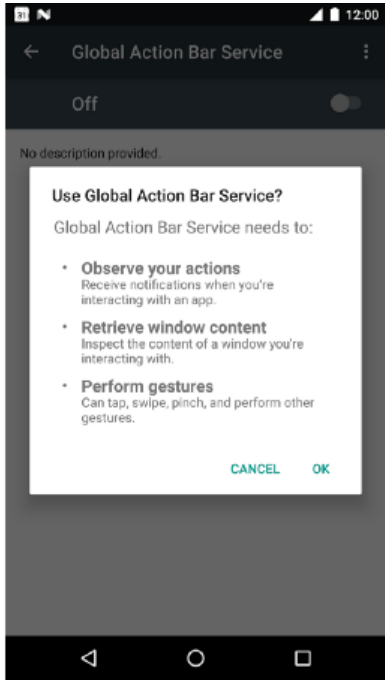
# Why?

# Problem: State of TOTP 2FA

## TOTPs apps are vulnerable to screen overlays and Accessibility based attacks



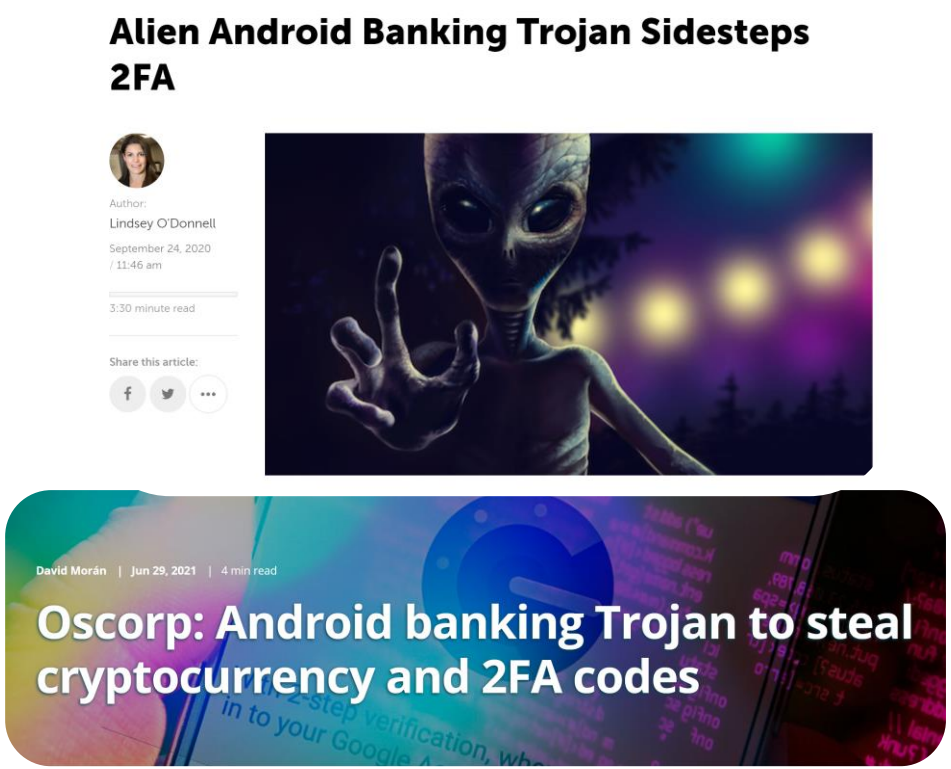




**In-app generator** requires effort, **takes time to auth** and in **vulnerable to remote login** attempts.

- Malware with accessibility permissions can **capture credentials** entered by the user on mobile banking apps**, read or generate** SMS messages, and **even read Two-Factor Authentication (2FA) codes** generated by authenticator apps!

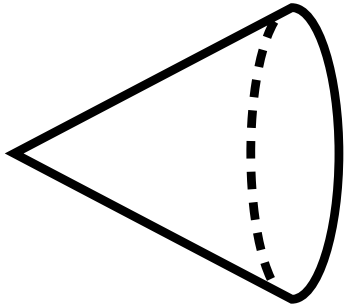
# Problem: State of TOTP 2FA

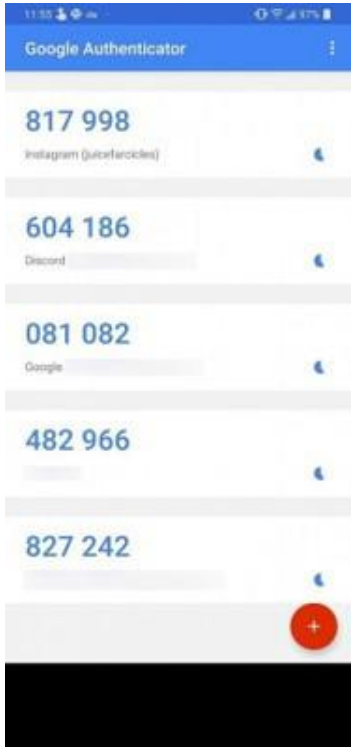
## TOTPs apps are vulnerable to screen overlays and Accessibility based attacks




**Malware Apps:**

- Cerberus
- TrickBot,
- DEFENSOR ID,
- TeaBot,
- Oscorp,
- Toddler.



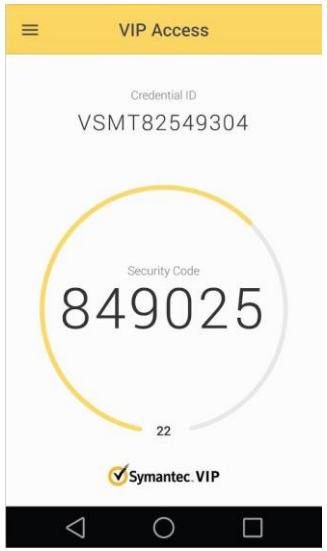


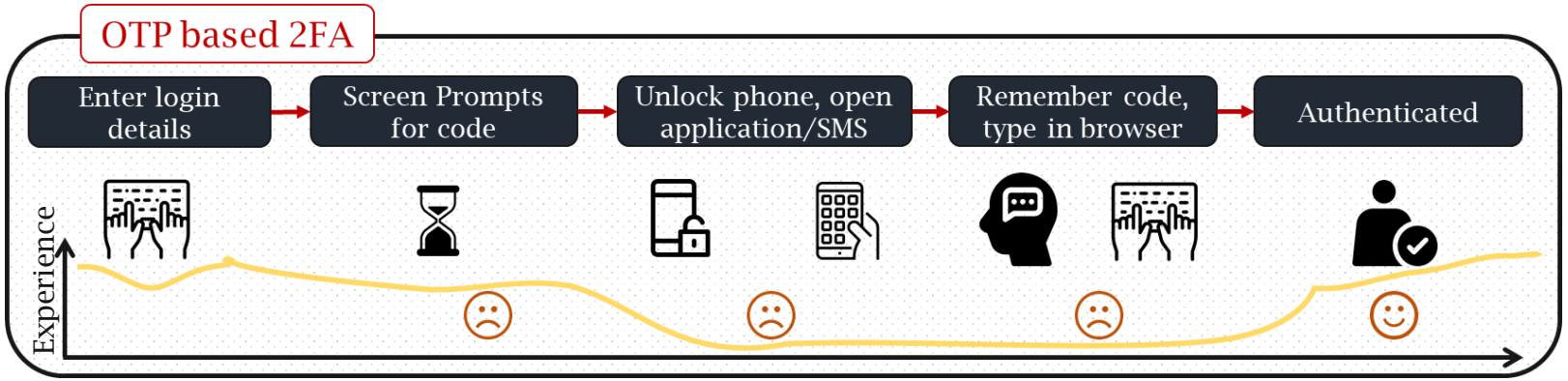


1. https://medium.com/axdb/%EF%B8%8F-dissecting-defensor-a-stealthy-android-banking-malware-6610b0468256
2. https://www.secureauth.com/blog/hijacking-2fa-a-look-at-mobile-malware-through-an-identity-lens/
3. https://labs.f-secure.com/blog/how-are-we-doing-with-androids-overlay-attacks-in-2020/

# Problem: State of TOTP 2FA

## TOTPs apps have high friction in use and adoption

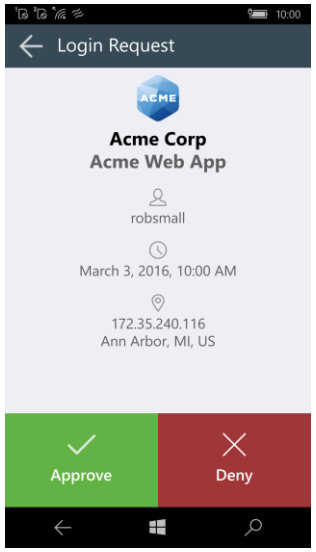



- User experience is affected due to time, distraction and errors while performing copying and typing of the OTP codes.

# Problem: State of Push based 2FA

## Push based 2FAs are vulnerable to concurrency and overlays attacks.




If an attacker & user logs in at the same time, the token device receives two pushes.

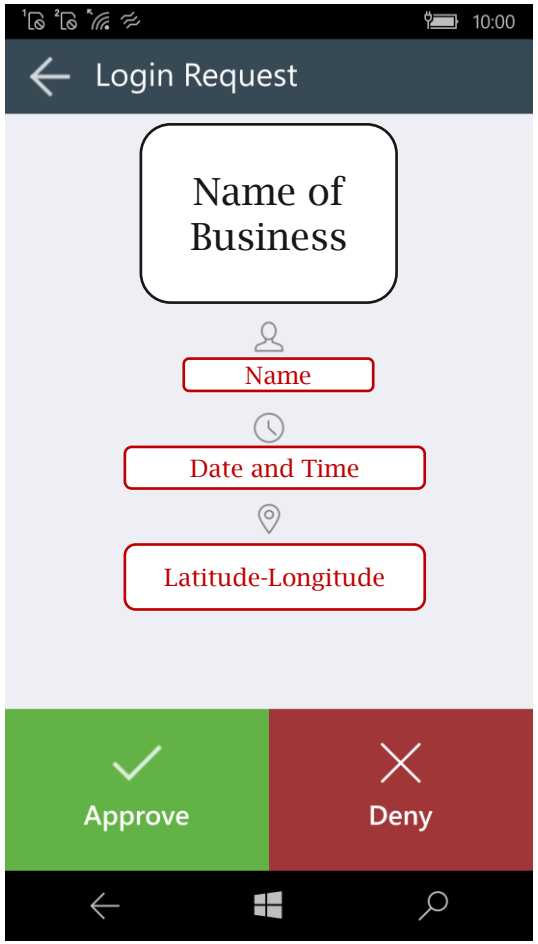
User tends to approve either or attacker's push (sophisticated attack) [1, Asia CCS 2021]

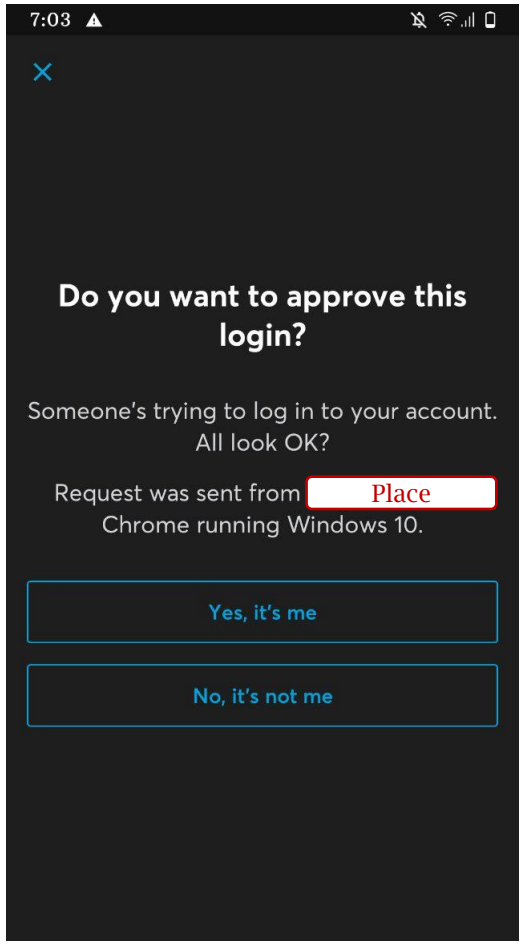
**Tap to Auth** is vulnerable to **concurrency attacks**

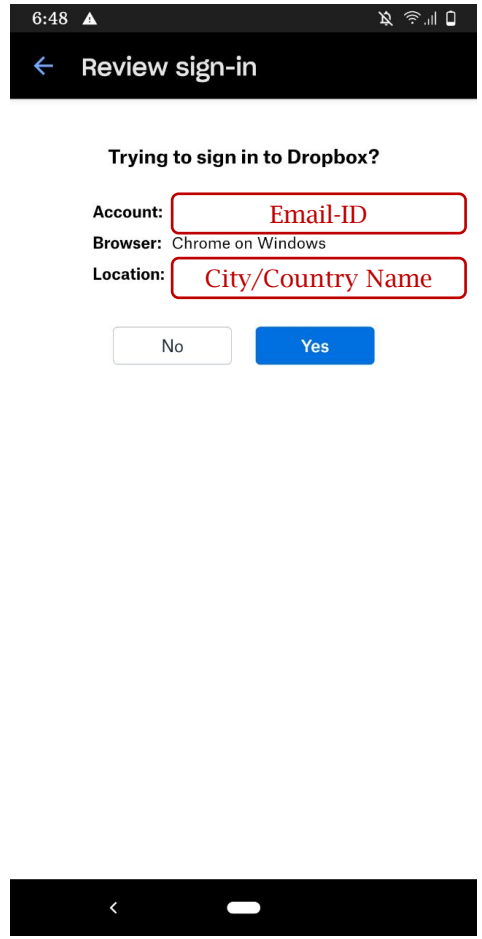

1. Mohammed Jubur, Prakash Shrestha, Nitesh Saxena, Jay Prakash, *Bypassing Push-based Second Factor and Passwordless Authentication with Human-Indistinguishable Notifications, ASIA CCS 2021*

# Problem: State of Push based 2FA

## Push to Approve Notifications are not differentiable



# Problem: State of Push based 2FA

Push to Approve Notifications are not differentiable

# Solution?

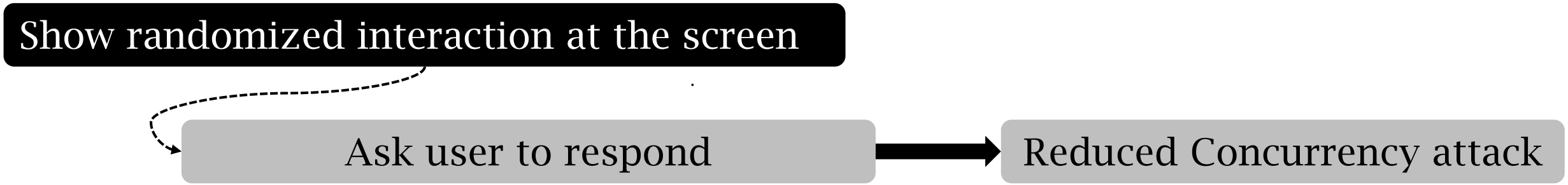
## Key Idea:

Remove static and fixed responses to Push

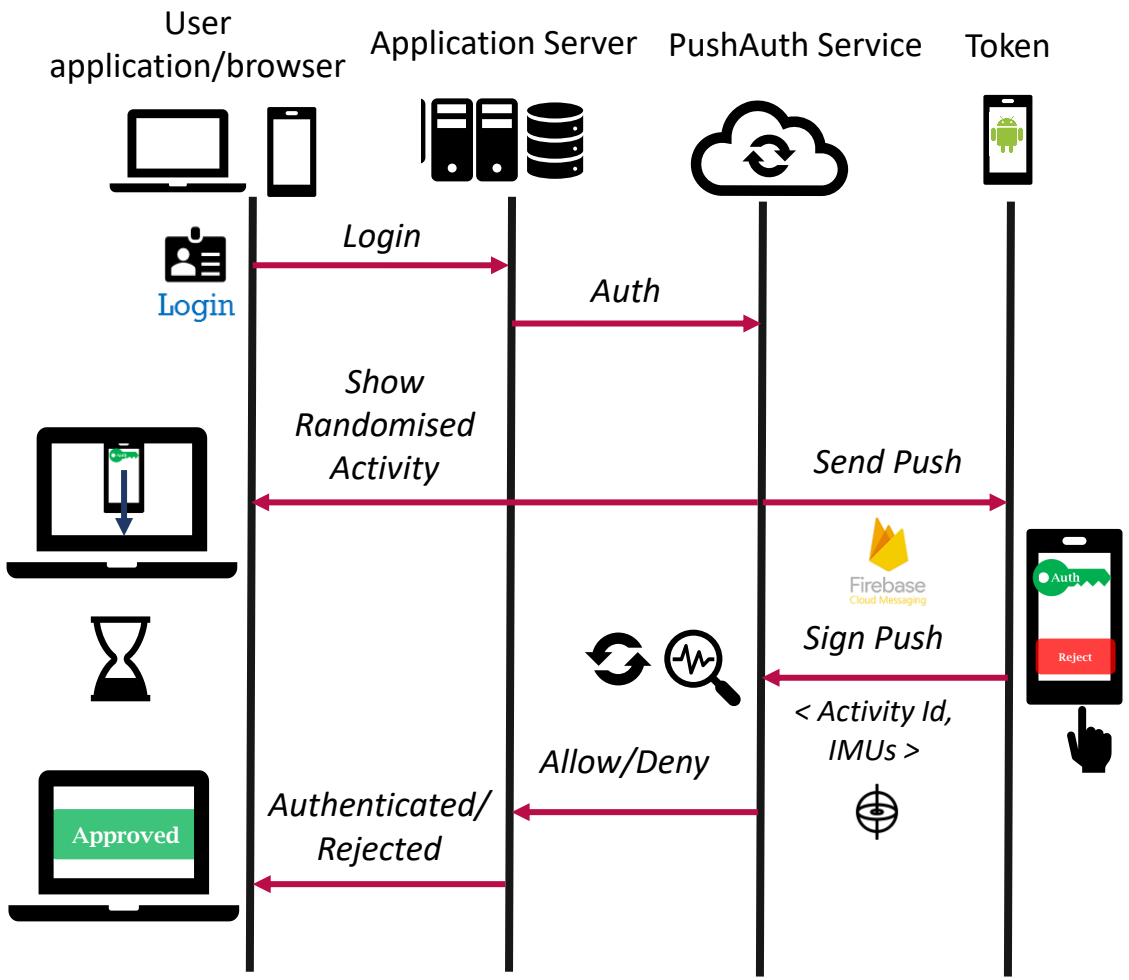
Random Interaction at login prompt → Replicate using token device

# Our Solution: REPLICATE to Prove and Auth

## Key Idea: REPLICATE



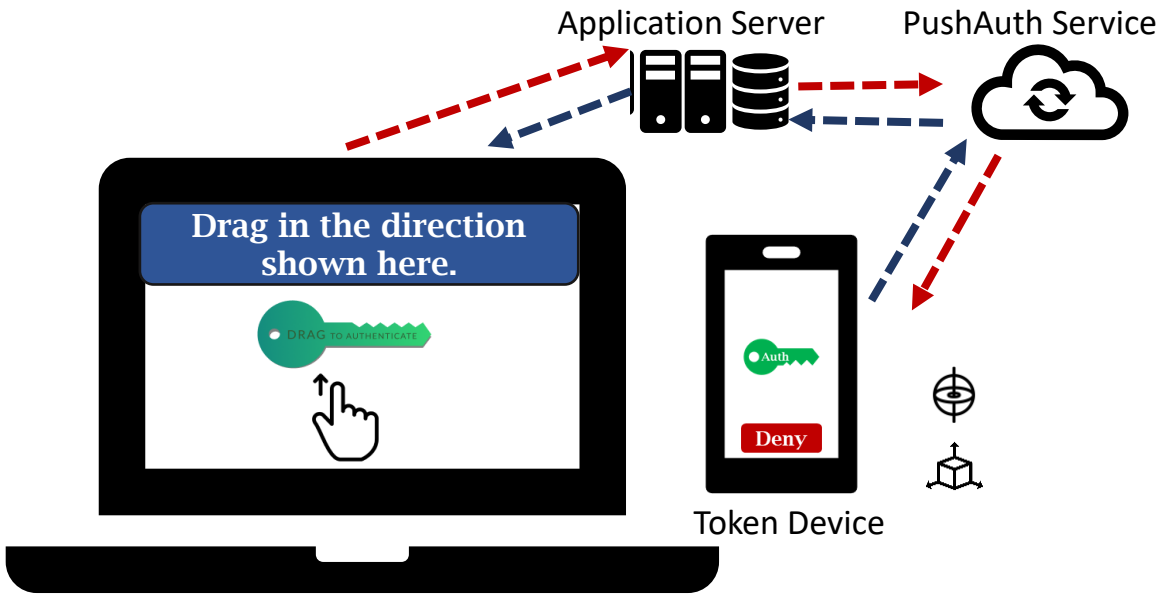
# REPLICATE: System Architecture

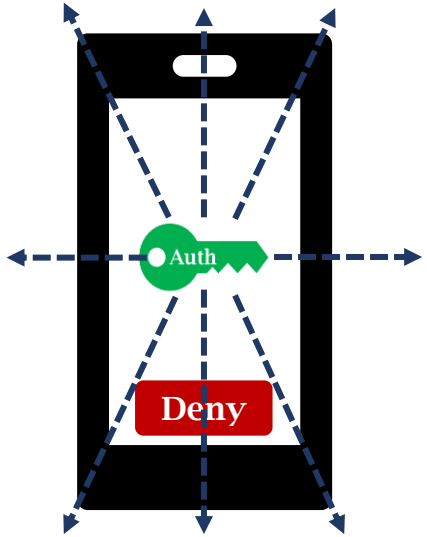


# REPLICATE: Forms for Study

Show randomized interaction at the screen

## Key Drag

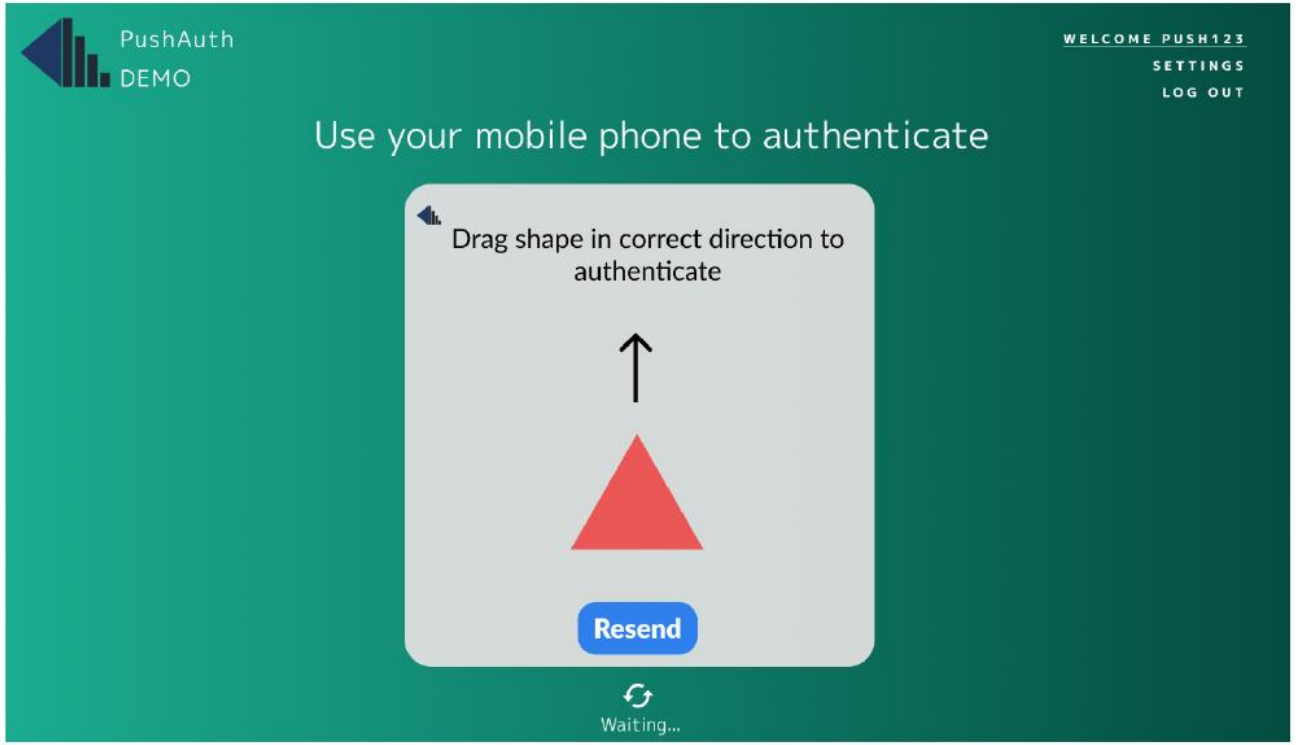


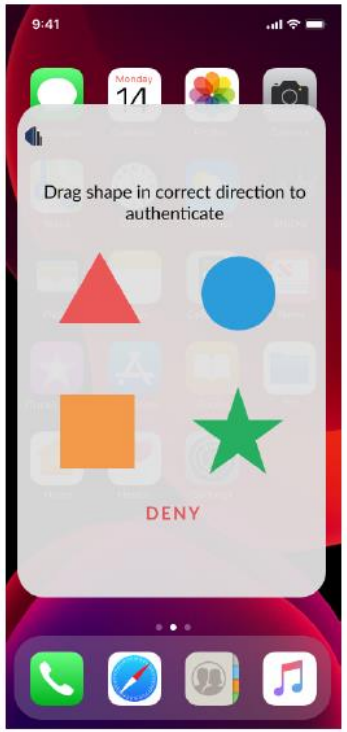



# REPLICATE: Forms for Study

Show randomized interaction at the screen

## Move a Shape



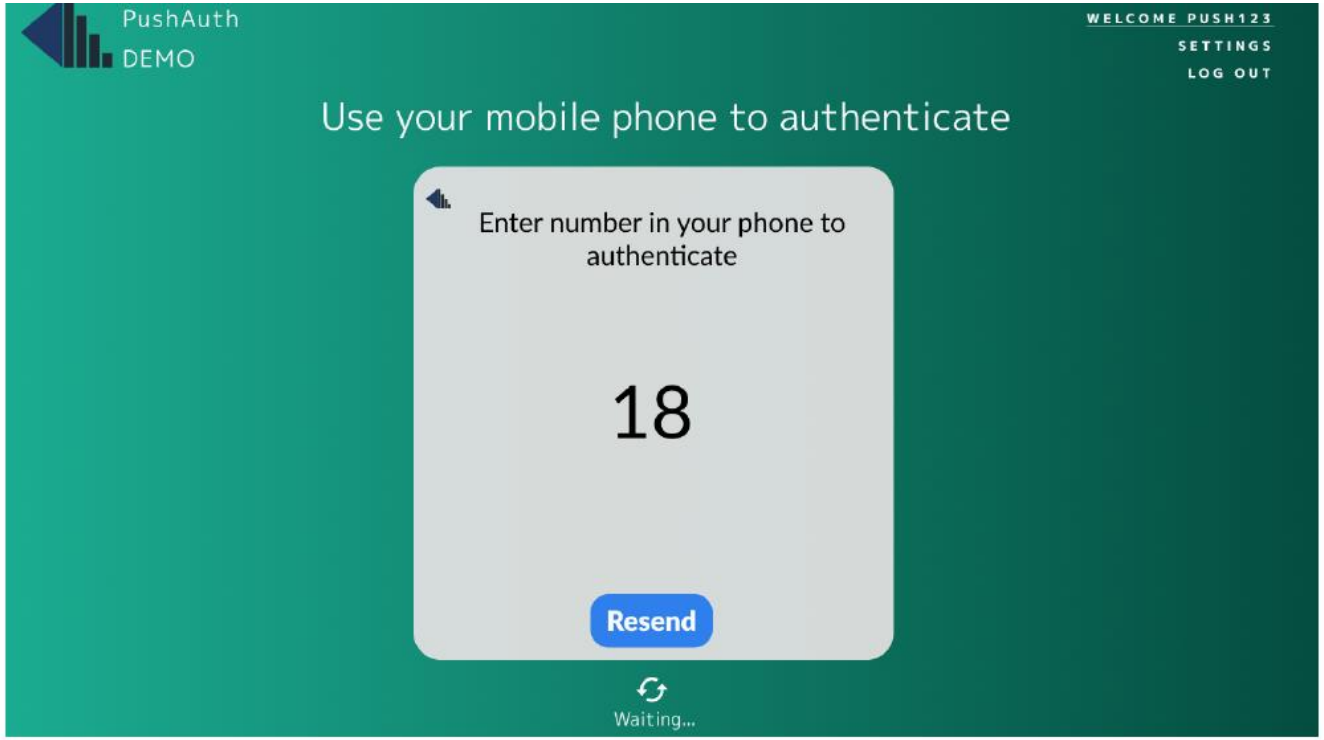



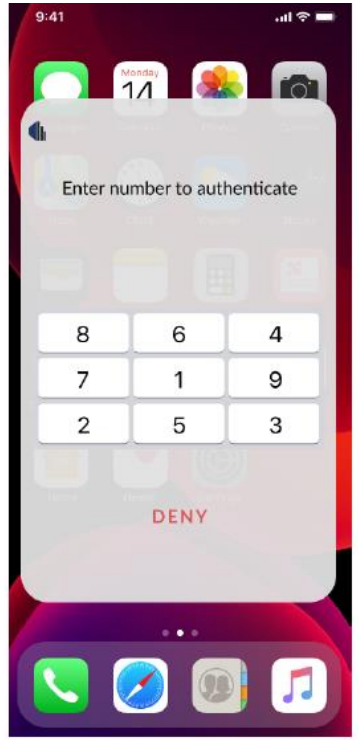

Move a Shape to Auth (a) Login window display and (b) Phone authentication push screen overlay.

# REPLICATE: Forms for Study

Show randomized interaction at the screen

## Randomized Keypad



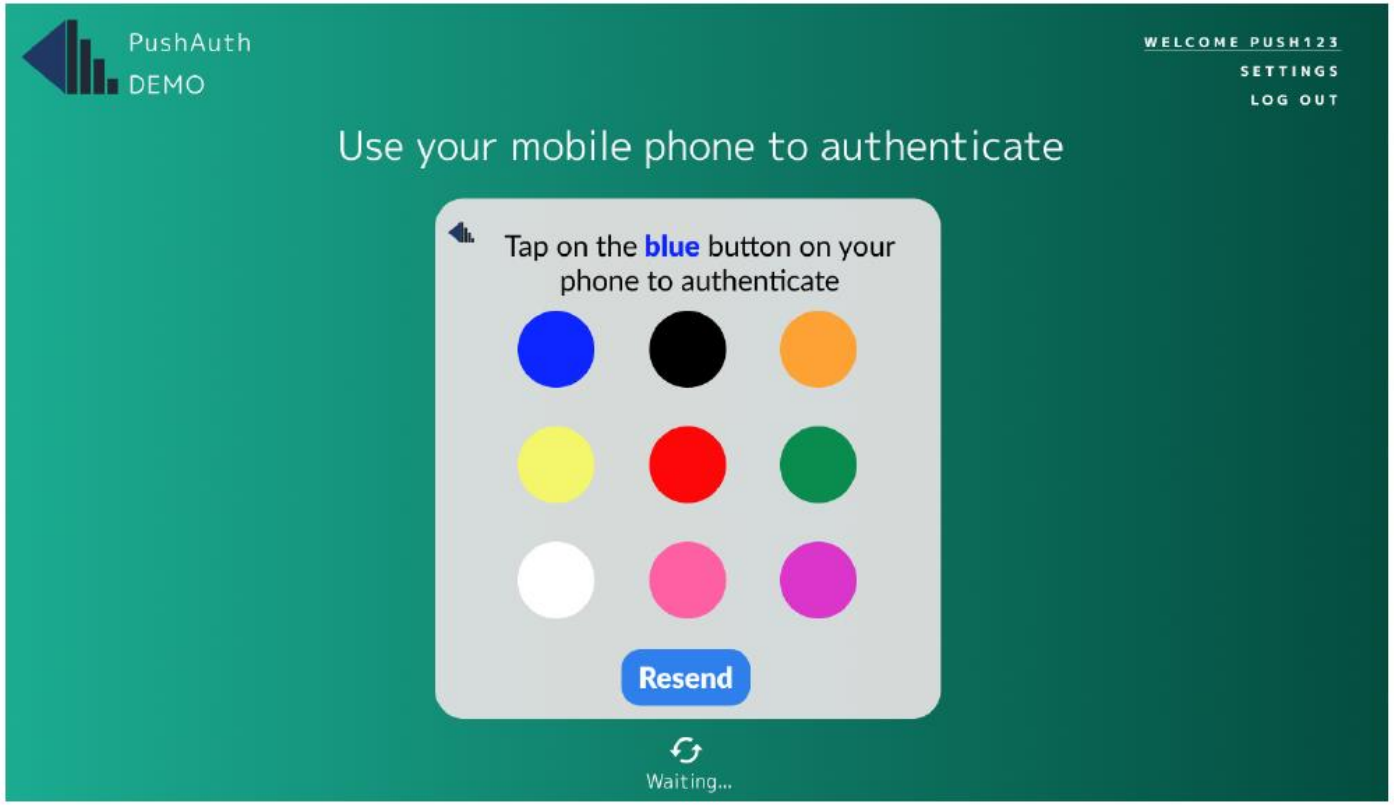



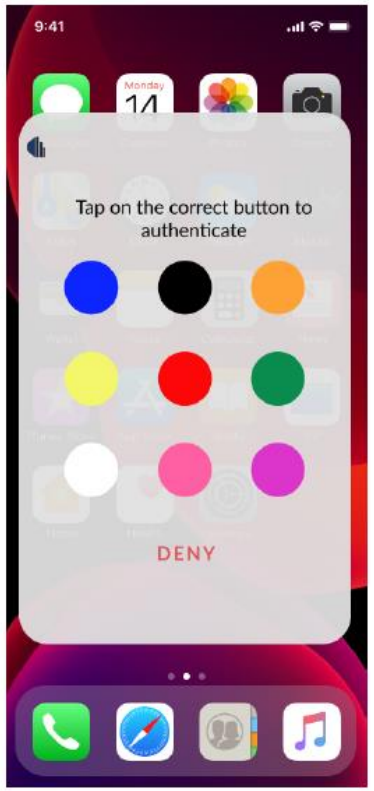

Randomized Keypad to Auth (a) Login window display and (b) Phone authentication push screen overlay

# REPLICATE: Forms for Study

Show randomized interaction at the screen

## Choose a Colored Button



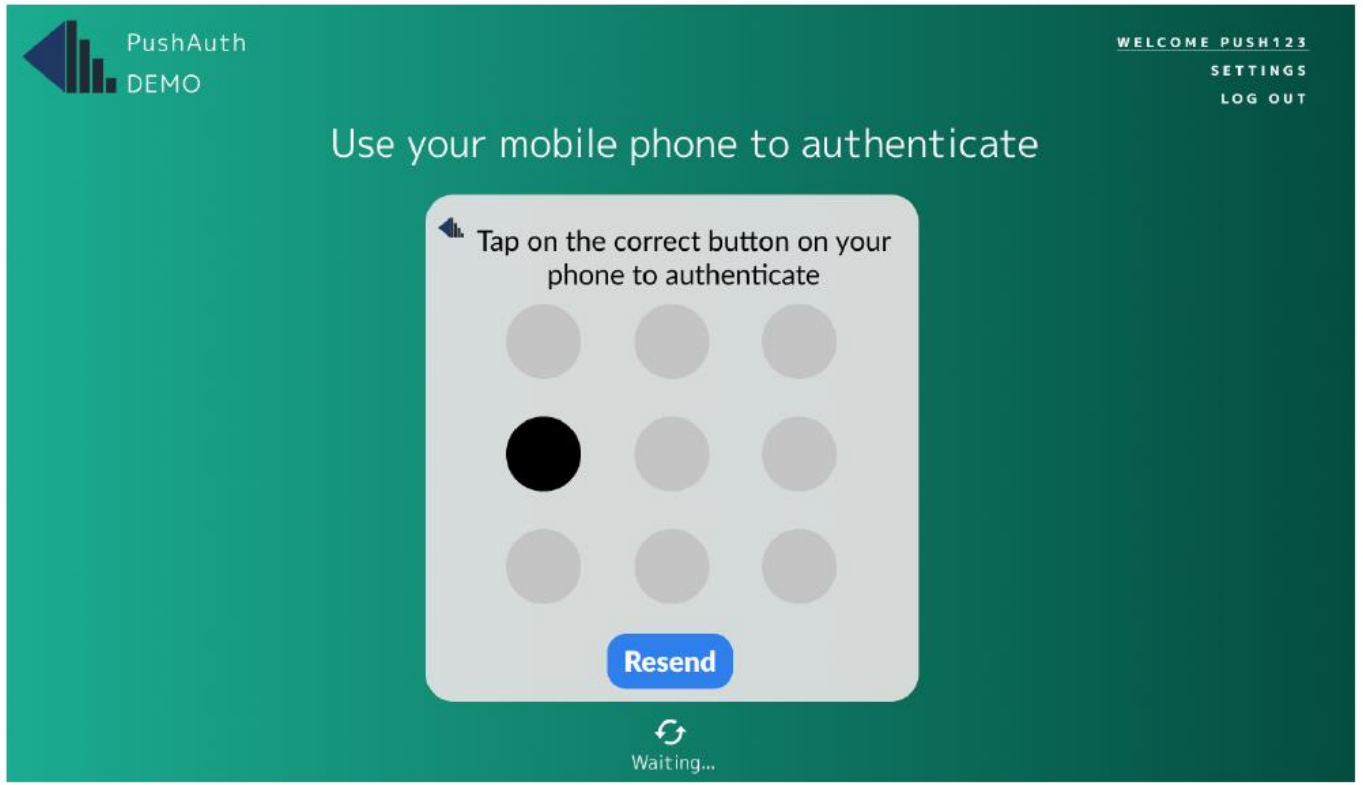




Choose a Colored Button to Auth (a) Login window display and (b) Phone authentication push screen overlay

# REPLICATE: Forms for Study

Show randomized interaction at the screen

## Tap on Black Button



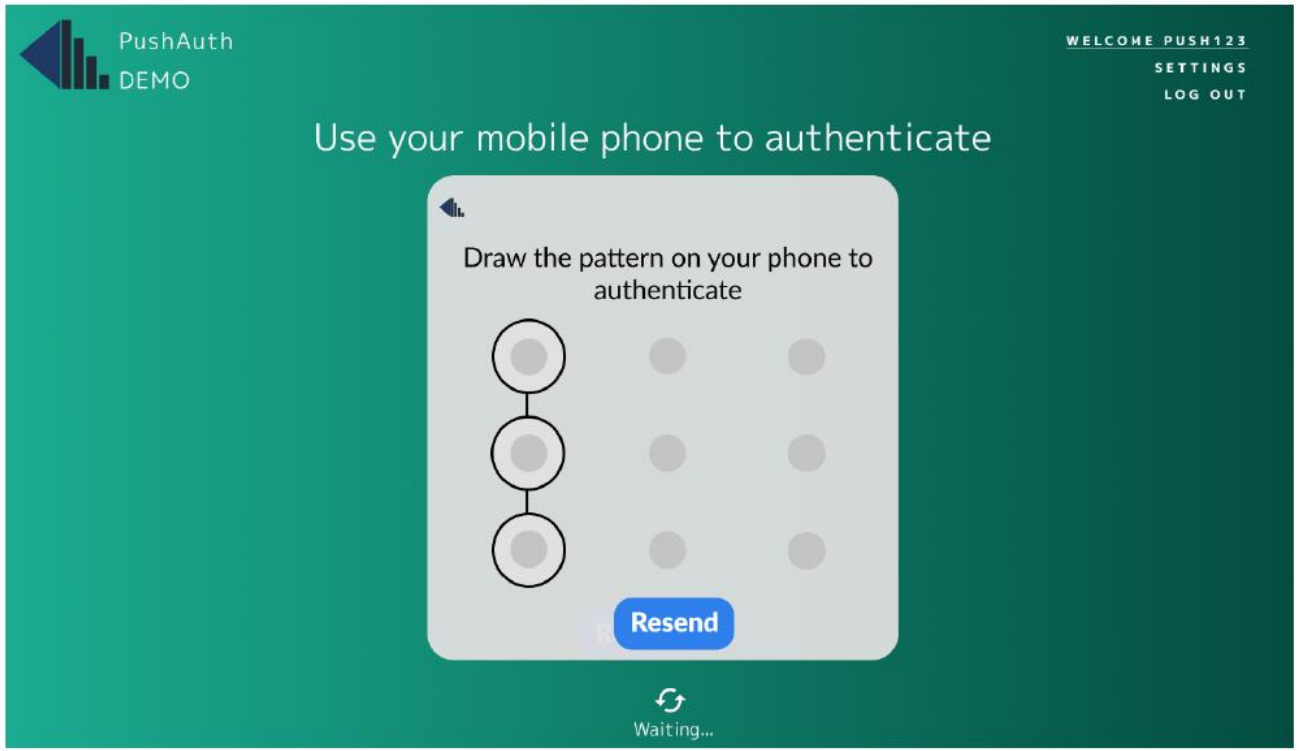


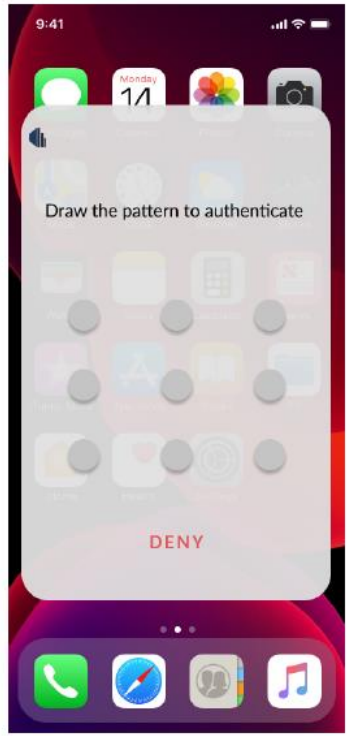
Tap on Black Button (a) Login window display and (b) Phone authentication push screen overlay

# REPLICATE: Forms for Study

Show randomized interaction at the screen

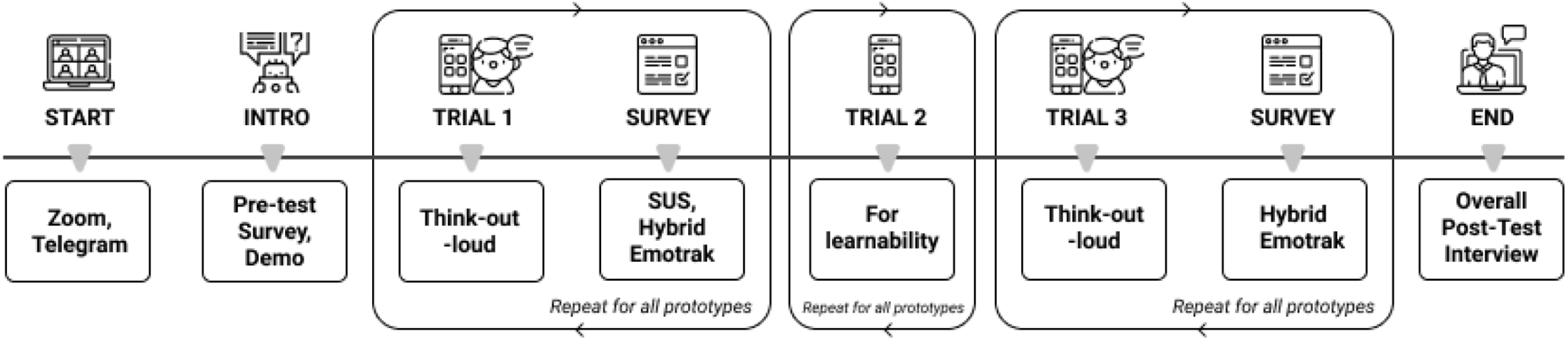
## Draw Pattern




Draw Unlock Pattern (a) Login window display and (b) Phone authentication push screen overlay

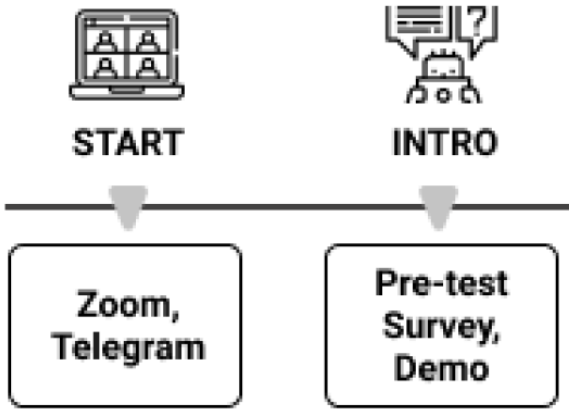
# REPLICATE: Study Design





Figma was used a base for the remote study.

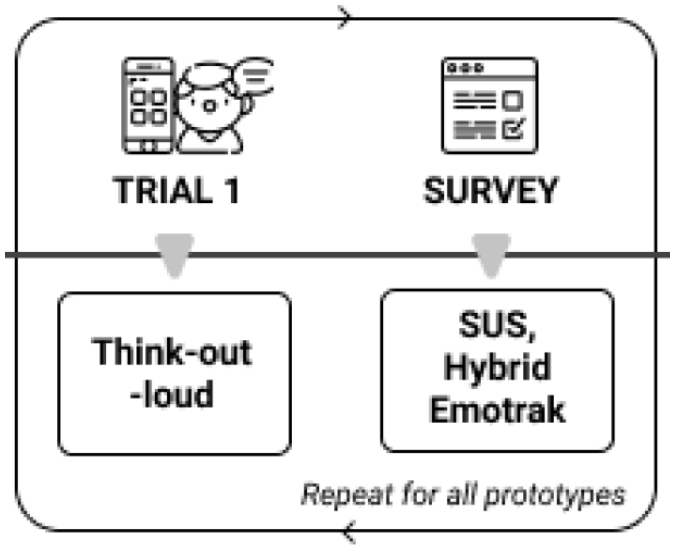
# REPLICATE: Study Design




## Pre-Test Survey

- What is your age group? a) 20 and below b) 21-30 c) 31-40 d) 41-50 e) 51 and above.
- On a scale of 0 to 4, how would you rate your level of familiarity in using your laptop? (0 being the least familiar and 4 being the most familiar).
- On a scale of 0 to 4, how would you rate your level of familiarity in using your phone? (0 being the least familiar and 4 being the most familiar.)
- Do you know what second-factor authentication is? a) Yes or b) No.
- In which of the following areas have you used a two-factor authentication? You can select more than one option. a) I have not done a two-factor authentication before, b) Banking, c) Email, d) Social Media, and e) Others.
- Have you come across a push-based TFA? Some examples are shown in the image below. a) Yes b) No

# REPLICATE: Study Design



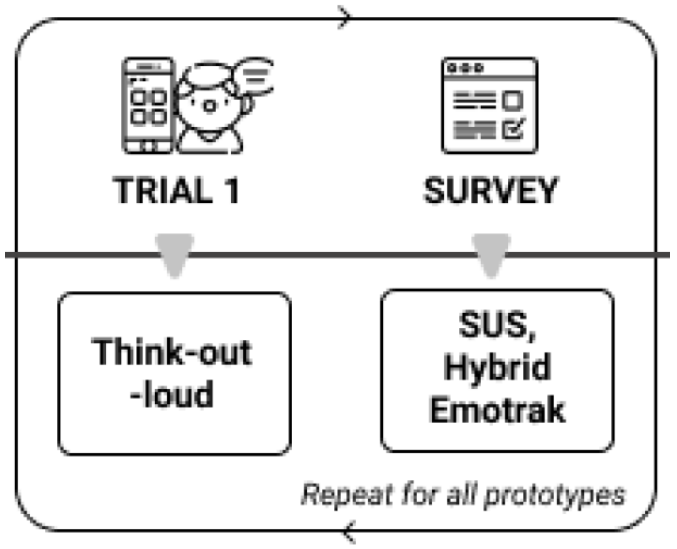

**Quantitative**

All positive SUS Survey

**Qualitative**

User Journey Mapping

# REPLICATE: Study Design

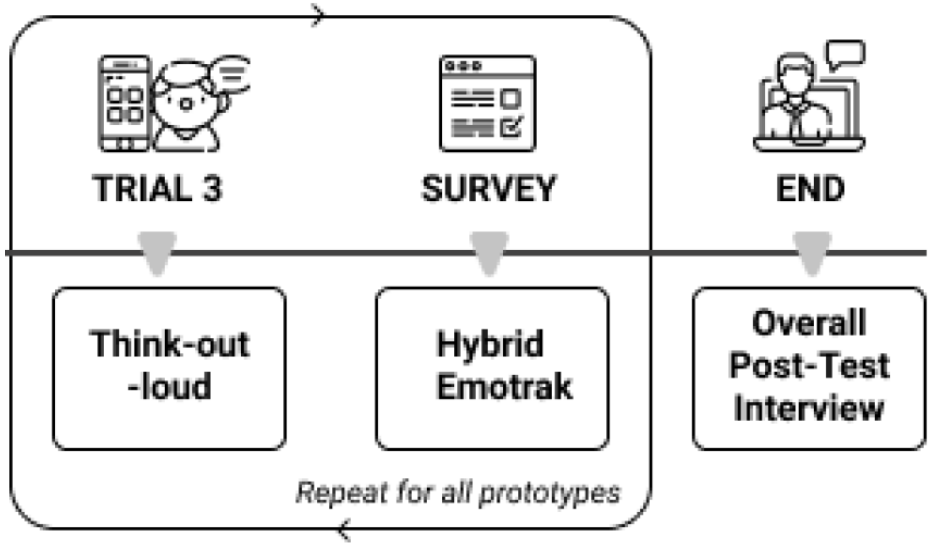



Quantitative

Qualitative

All positive SUS Survey

User Journey Mapping(UJM)

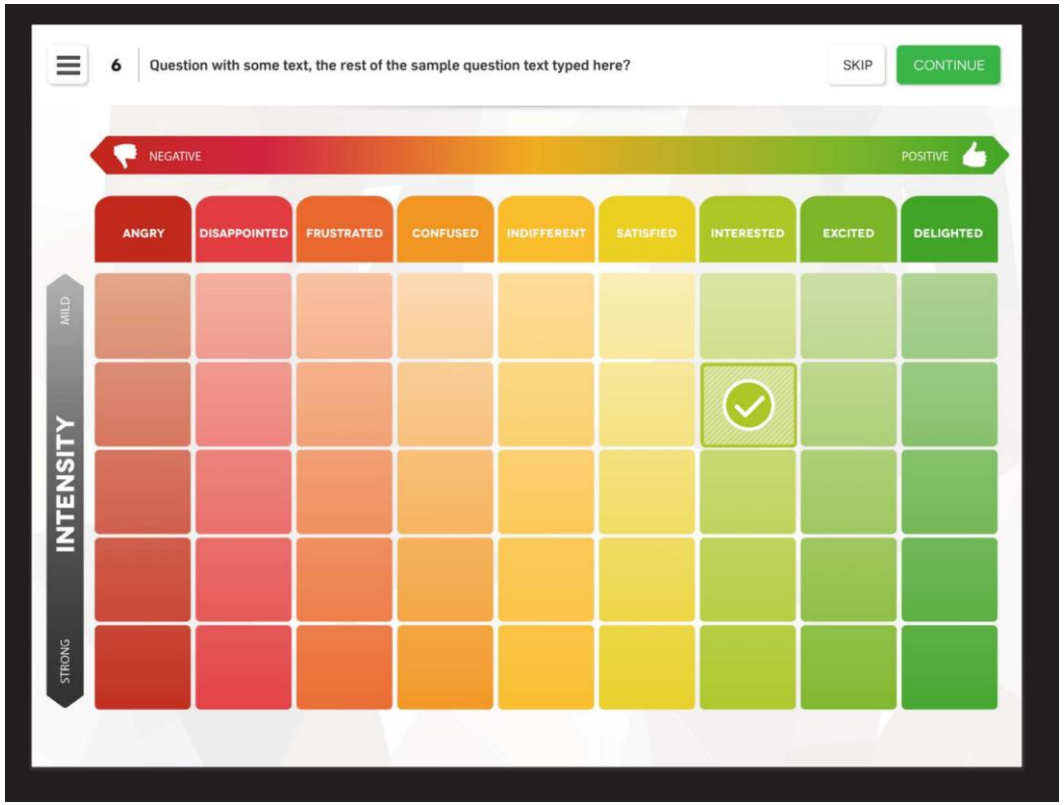



Trial 2 and 3, UJM and overall post test interview.

# Qualitative Study: Generating UJM

We proposed Hybrid Emotrack: Inspired from Plutchik Emotion Wheel and Emotrak


Plutchik Emotion Wheel [1]

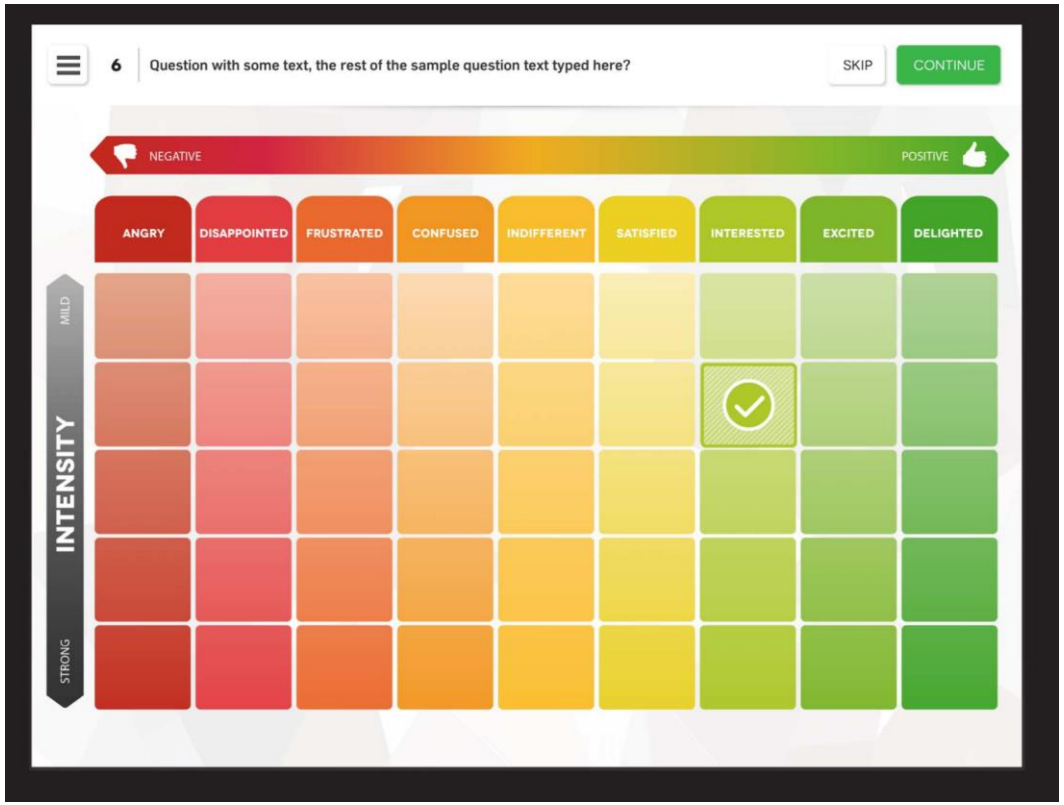



Emotrak by UEGroup [1]

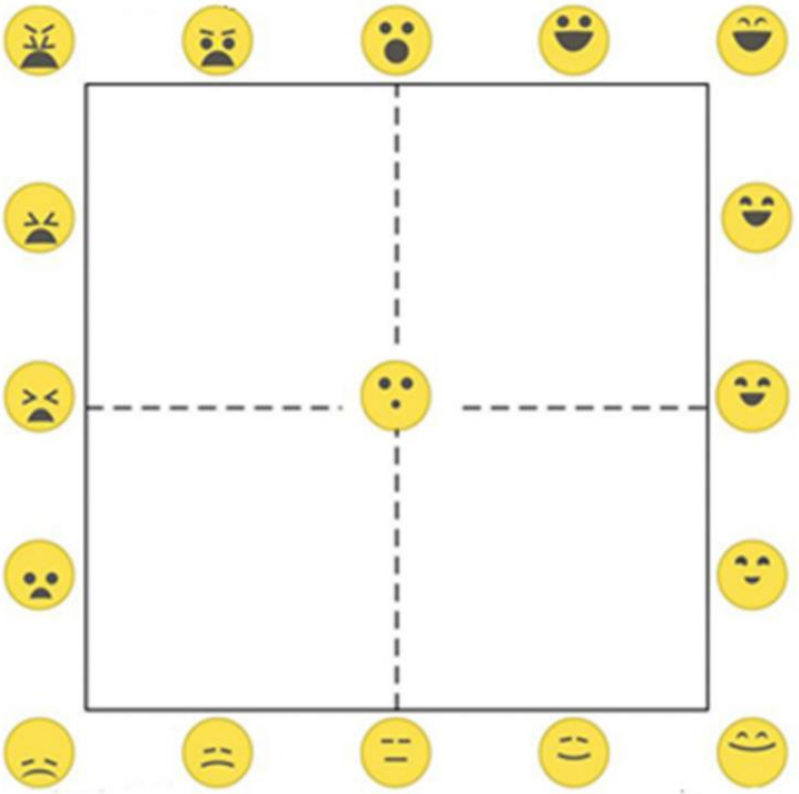
1. Capturing & Measuring Emotions in UX, CHI4Good, CHI 2016

# Qualitative Study: Generating UJM

We proposed Hybrid Emotrack: Inspired from Plutchik Emotion Wheel and Emotrak



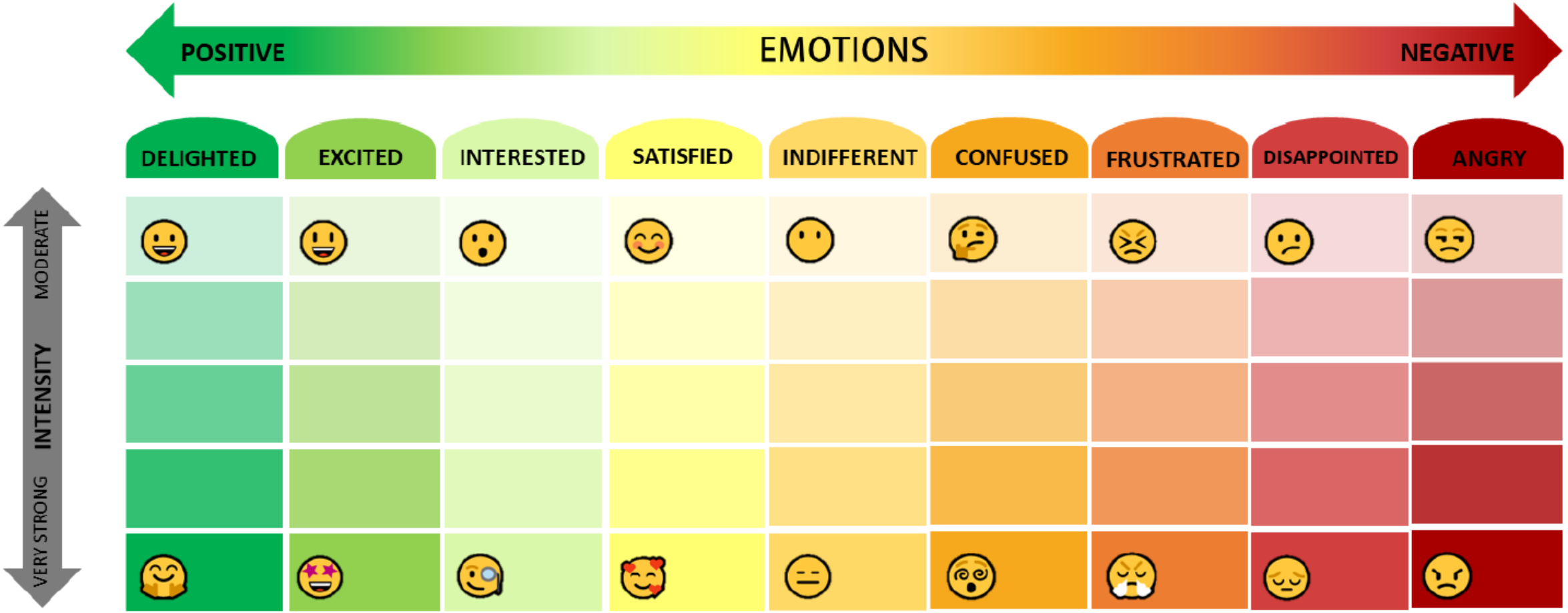

Emotrak by UEGroup [1]



EmojiGrid: Emoji Affect Grid [2]

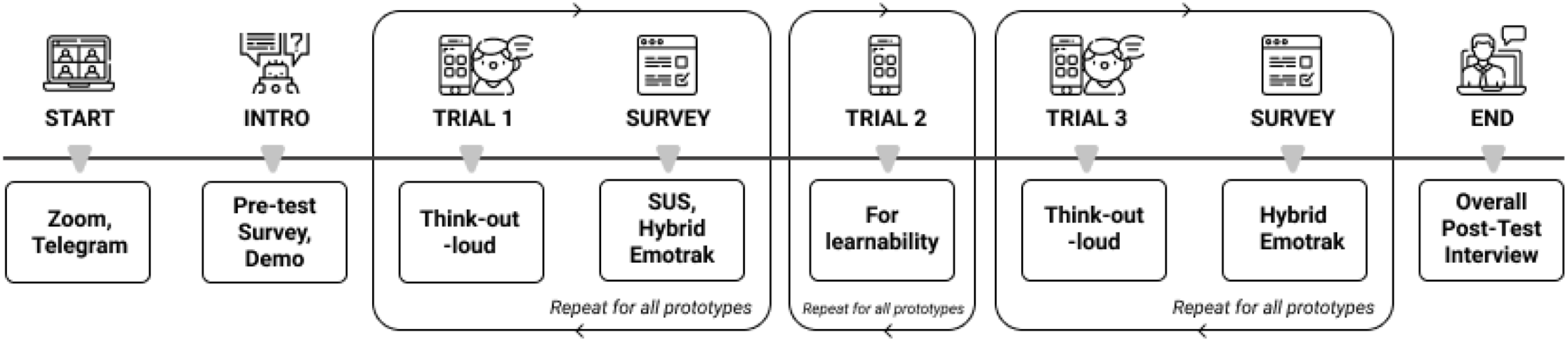

1. Capturing & Measuring Emotions in UX, CHI4Good, CHI 2016
2. EmojiGrid: A 2D Pictorial Scale for the Assessment of Food Elicited Emotions, Front. Psychol., 28 November 2018.

# Qualitative Study: Generating UJM




Hybrid Emotrak with emojis as hint for emotions

# REPLICATE: Study Design




Just Tap to Authenticate

VS

REPLICATE

1. Laptop as login device & Phone as a token

+

2. Both login and authentication on a phone

# Quantitative Analysis

## Task Success

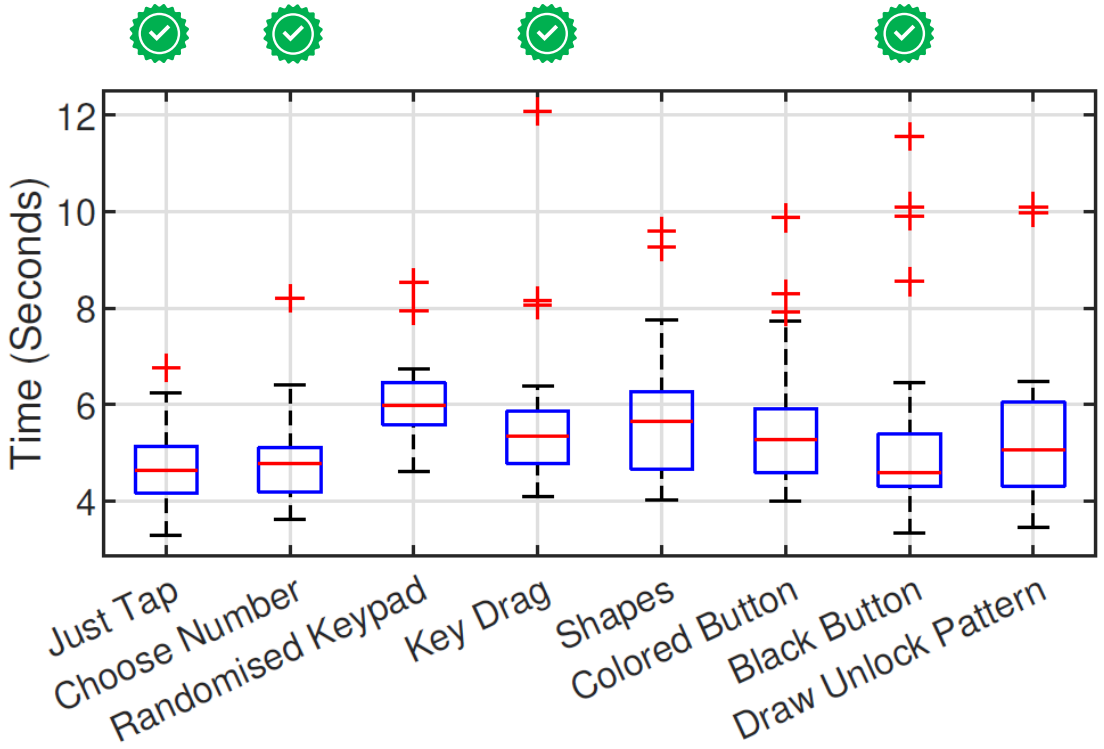
| Authentication Method | Task Success Rate ( in %) | 95% Confidence Interval (Adjusted Wald Method) |
|---|---|---|
| Just Tap | 100 | (90,100) |
| Choose Number | 100 | (90,100) |
| Randomized Keypad | 93 | (76,99) |
| Key Drag | 100 | (90,100) |
| Shapes | 100 | (90,100) |
| Colored Button | 97 | (82,100) |
| Black Button | 100 | (90,100) |
| Draw Unlock Pattern | 100 | (89,100) |

TABLE 1. TASK SUCCESS RATES WITH 95% CI (L2P)

- If participant managed to reach “Unlocked”/ “ Authenticated” in one try without external helps gets 1 score, 0 otherwise.

# Quantitative Analysis

## Task Time




- The time taken (in seconds) for the participant to authenticate successfully; task time = end time - start time.

# Quantitative Analysis

## Task Time

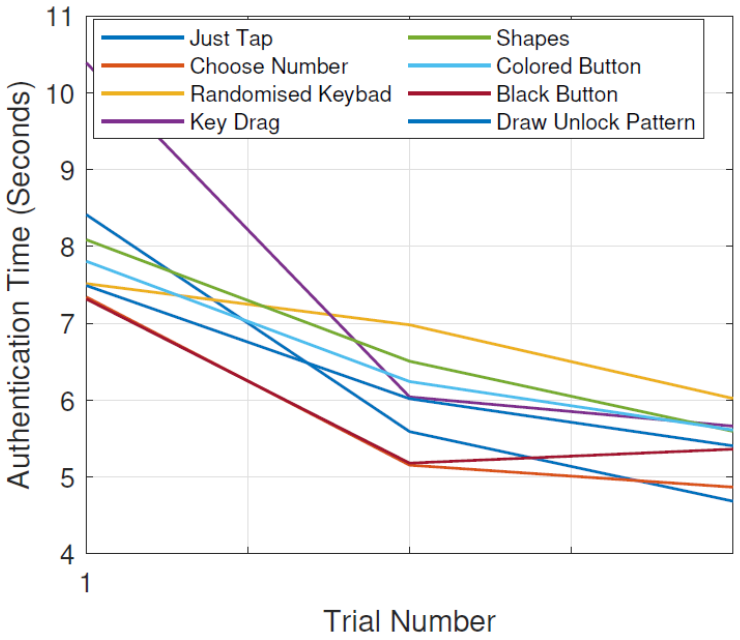
| Authentication Method | Q1 | Mean | Median | Q3 | 95% Confidence Interval |
|---|---|---|---|---|---|
| Just Tap | 4.19 | 4.69 | 4.65 | 5.12 | (4.37,5.01) |
| Choose Number | 4.24 | 4.87 | 4.78 | 5.08 | (4.50, 5.24) |
| Randomized Keypad | 5.60 | 6.02 | 5.98 | 6.44 | (5.69, 6.35) |
| Key Drag | 4.82 | 5.66 | 5.35 | 5.86 | (5.07, 6.25) |
| Shapes | 4.67 | 5.73 | 5.66 | 6.27 | (5.25, 6.21) |
| Colored Button | 4.60 | 5.61 | 5.27 | 5.89 | (5.09,6.13) |
| Black Button | 4.31 | 5.36 | 4.59 | 5.36 | (4.61, 6.11) |
| Draw Unlock Pattern | 4.35 | 5.41 | 5.06 | 5.99 | (4.82, 6.00) |

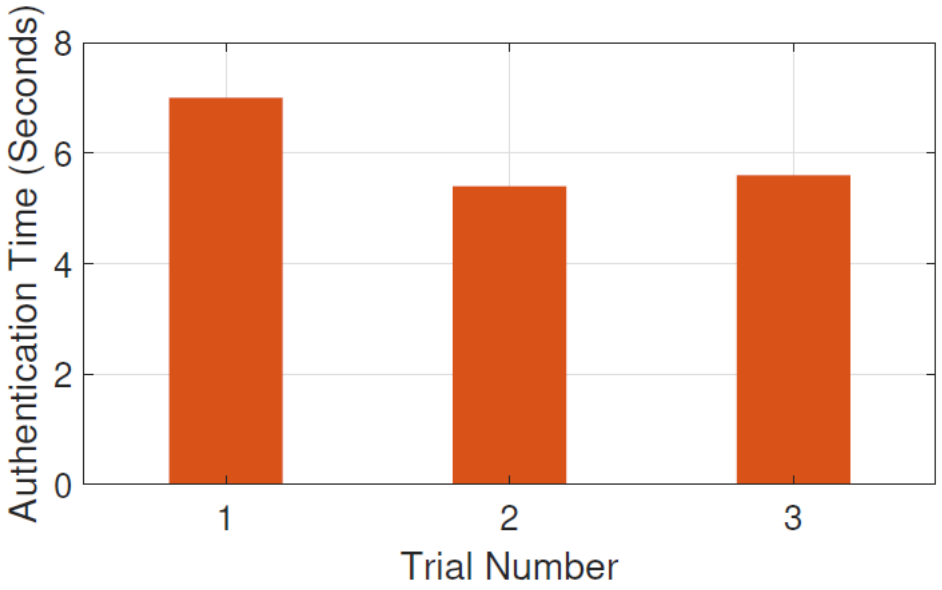
TABLE 2. STATISTICS OF AUTHENTICATION TIME (IN SECONDS)

- Just Tap and Black button method seem to be competitive.

# Quantitative Analysis

## Task Time

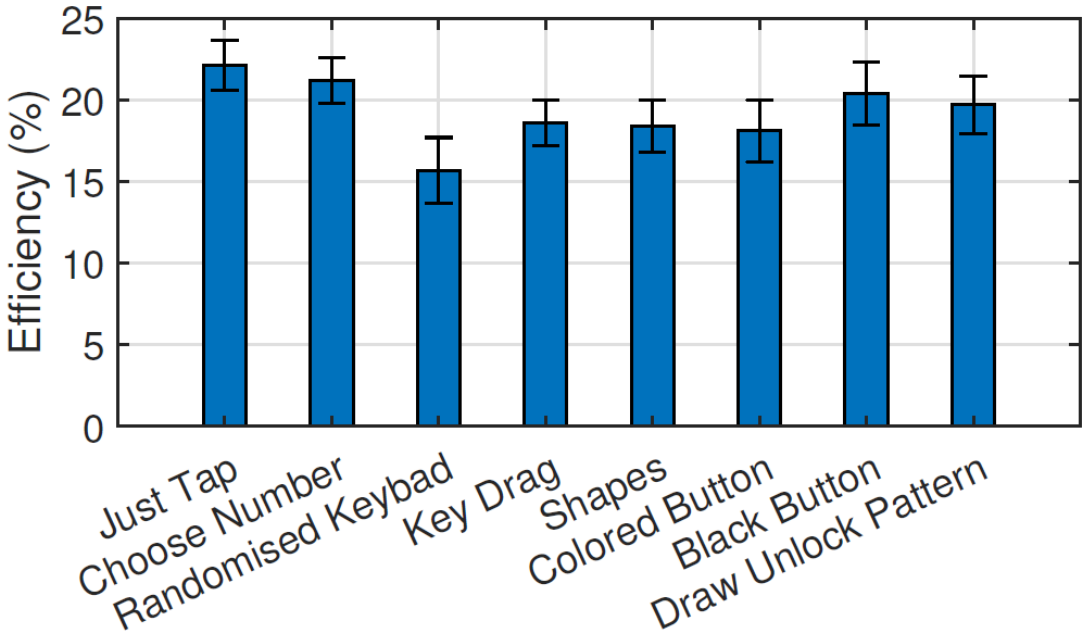



- User got familiarized with the trials and time plateaued.

# Quantitative Analysis

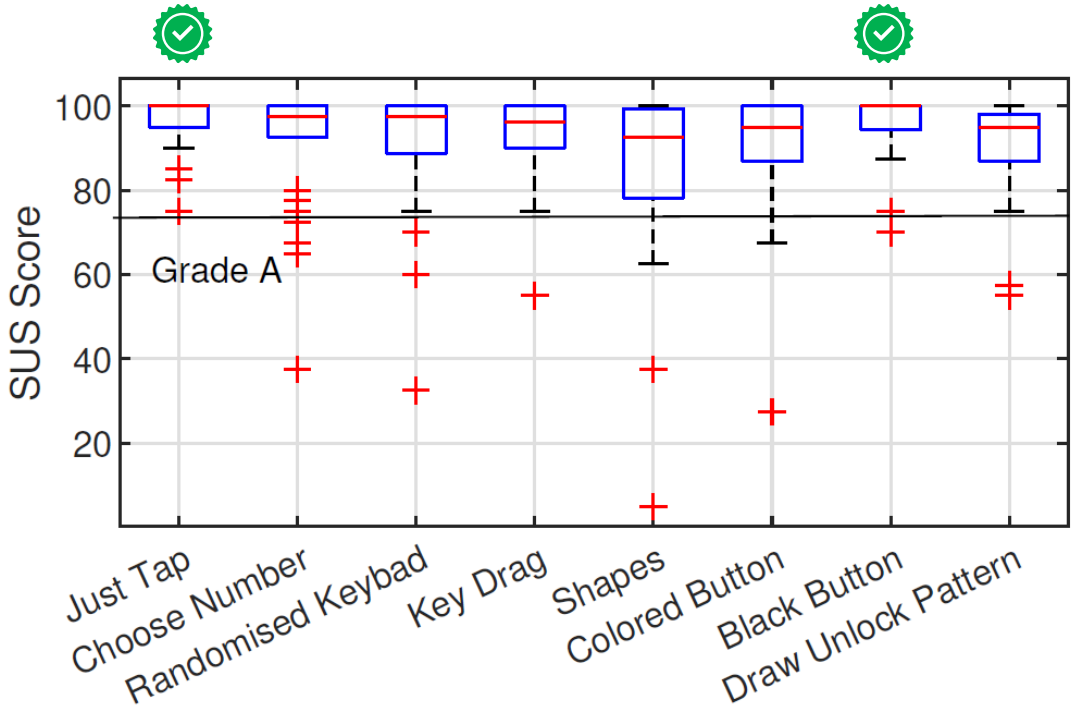
## Efficiency




- Efficiency: Task success/ task time.
- Black Button and Draw Unlock Pattern's task efficiency were comparable to existing solutions.

# Quantitative Analysis

## SUS Score




| Authentication Method | Q1 | Mean | Median | Q3 | 95% Confidence Interval |
|---|---|---|---|---|---|
| Just Tap | 95.6 | 95.7 | 100.0 | 100.0 | (93.0,98.4) |
| Choose Number | 92.5 | 91.8 | 97.5 | 100.0 | (86.7, 96.9) |
| Randomized Keypad | 89.4 | 90.5 | 97.5 | 100.0 | (84.5, 96.5) |
| Key Drag | 90.0 | 91.8 | 96.3 | 100.0 | (87.9, 95.7) |
| Shapes | 78.8 | 84.7 | 93.0 | 98.8 | (76.1, 93.3) |
| Colored Button | 87.5 | 90.1 | 95.0 | 100.0 | (84.5, 95.7) |
| Black Button | 95.0 | 95.0 | 100.0 | 100.0 | (91.6, 98.4) |
| Draw Unlock Pattern | 87.5 | 90.3 | 95.0 | 97.5 | (85.8, 94.8) |

- Tap on Black Button fairs similar to Just Tap method and better than the rest

# Quantitative Analysis

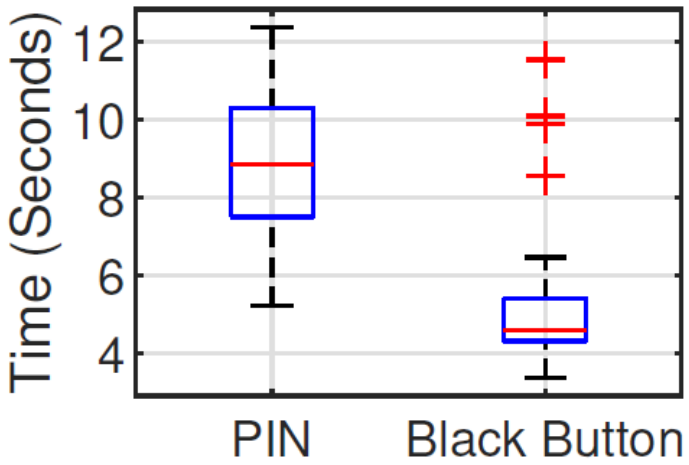
## Combined Analysis

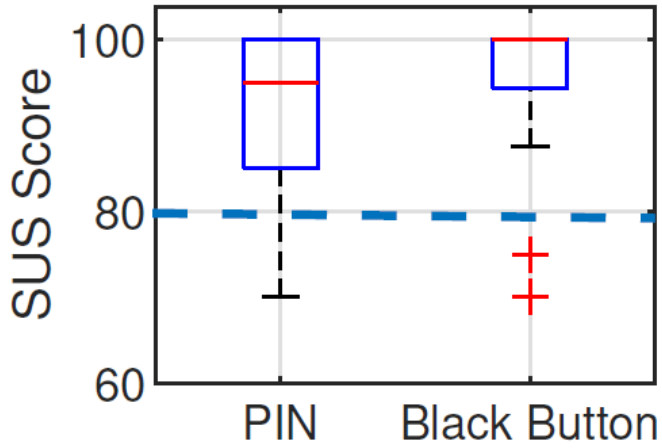
| Authentication Method | Task Success | Time | Task Efficiency | SUS Score | Favourite Count | Less Favourite Count | Score |
|---|---|---|---|---|---|---|---|
| Just Tap | 1 | 2 | 1 | 1 | 1 | 4 | 10 |
| Choose Number | 1 | 3 | 2 | 3 | 4 | 1 | 14 |
| Randomised Keypad | 8 | 8 | 8 | 3 | 4 | 8 | 39 |
| Key Drag | 1 | 6 | 5 | 5 | 4 | 5 | 26 |
| Shapes | 1 | 7 | 6 | 8 | 7 | 7 | 36 |
| Coloured Button | 7 | 5 | 7 | 6 | 3 | 6 | 34 |
| Black Button | 1 | 1 | 3 | 1 | 2 | 2 | 10 |
| Draw Pattern | 1 | 4 | 4 | 6 | 7 | 2 | 24 |

- Based on ranking 1 to 8.
- Tap on Black Button fairs similar to Just Tap method and better than the rest.

# Quantitative Analysis

## Compared to PIN 2FA




- REPLICATE fairs better than PIN based 2FAs across all dimensions including time and SUS scores.

# Qualitative Analysis

## Ease of Execution and Cognitive Effort

- Black button method faired much well compared to others in the usability ranking.

**P3:** *"I prefer the Black Button method. For PIN-based method, I had to look at the screen at least 3 times to ensure I was doing it right. For Black button, I didn't have to refer back."*

**P14:** *"It is easy enough for you to just press 1 time. The rest requires dragging and more actions. This is the fastest."*

**P11:** *"This is the easiest to understand. By far the best for understanding and carrying out."*

**P30:** *"The buttons were all grey, and only the one I had to press was in black. The difference in the coloring was fun and helped me easily identify which button to press. Also, after I pressed the correct button, then the exact color in the instructions showed on my phone, which helped me to recognize that I did it correctly."*

# Qualitative Analysis

## Perception of Security

- 13/40 cited lack of security in Just Tap to authenticate method.

**P9:** *"It is easy but secure. Just Tap is easy but not secure. For Black Button you only have 1/9 chance to randomly click on it. Easiest and more safe."*

- Participants appreciated forcing to think method of REPLICATE.

**P34:** *"Simple but makes you think twice. Thinking twice is important because I want to be aware of what I am doing."*

**P25:** *"I like that it is fairly simple but relatively much more secure than current simple TFA methods."*

# Qualitative Analysis

## Inclusivity

- Colored Button noticed concerns over color blindness.

**P12:** *"In consideration of a minority of people that are colorblind, this method won't be feasible."*

- Drawing patterns witnesses issues about unfamiliarity.

**P37:** *"Troublesome, especially for old people. This is okay for unlocking phone because we are used to the same pattern, but in this case, it is always a different pattern."*

# Qualitative Analysis

## Level of Engagements

- Participants felt encouraged to try out 2FAs as PIN based methods are boring.

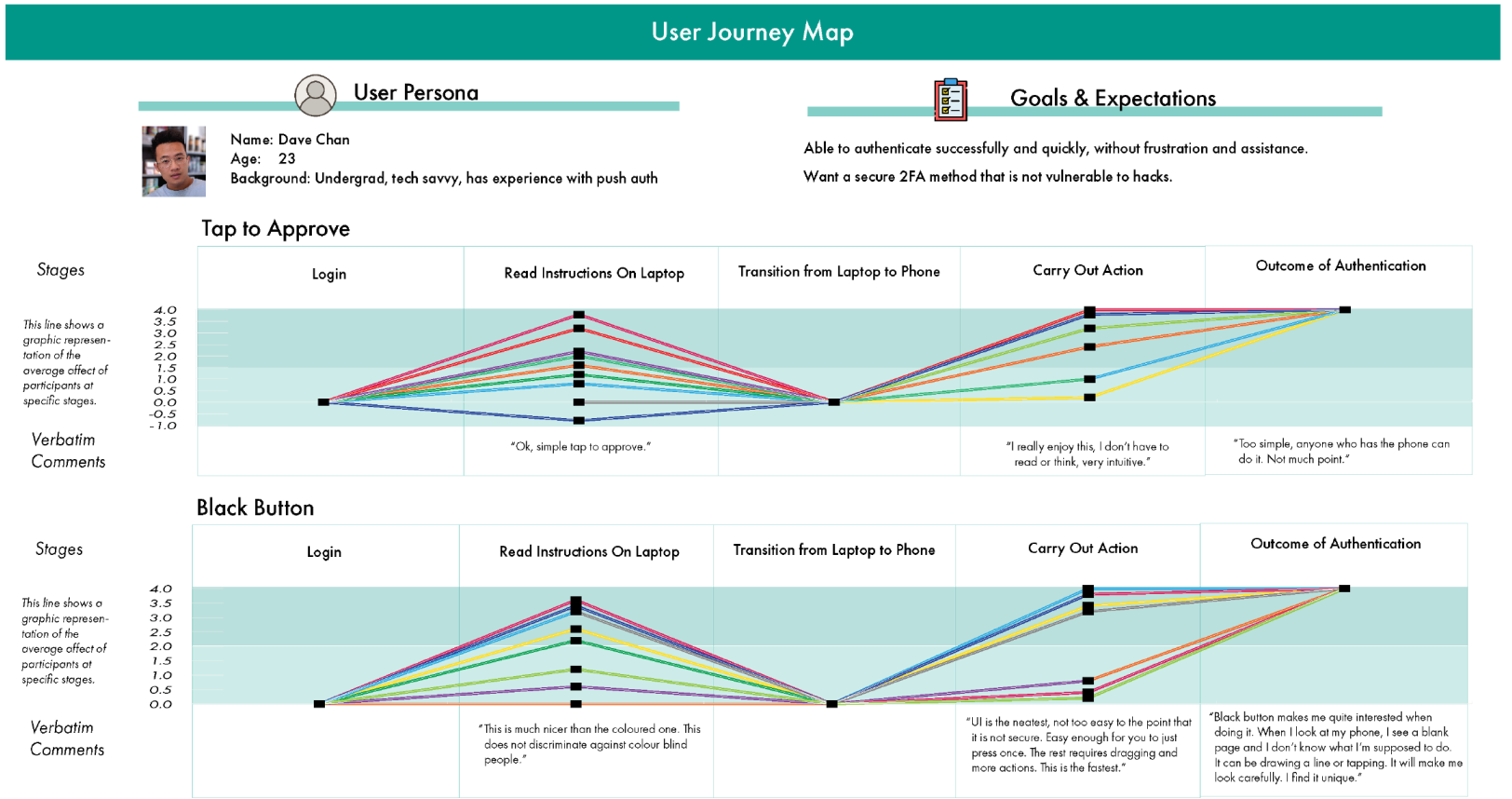
**P33:** *"I like this. Usual OTP methods are very boring. This method is like a small puzzle. Nice shapes. More fun and less boring, I like this."*

- Participants prefer the more engaging or fun method if everything else is comparable. Key Drag, Shapes and Colored Button were deemed fun by some participants.

**P13:** *"Once in a while, it will be a very fun way. Looking at the key was more fun. The shapes look simple, but the key has a nicer display. It is a unique way to unlock because it literally has a key to unlock."*

# Qualitative Analysis

## User Journey Map




- Tap on Black Button fairs similar to Just Tap method and better than the rest

# Comparisons with other 2FAs

| Schemes | Usability | | | | | | | | Deployability | | | | | | Security | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Memorywise-Effortless | Scalable-for-Users | Nothing-to-Carry | Physically Effortless | Easy-to-Learn | Efficient-to-Use | Infrequent-Errors | Easy-Recovery-from-Loss | Accessible | Negligible-Cost-per-User | Server-Compatible | Browser-Compatible | Mature | Non-Proprietary | Resilient-to-Physical-Observation | Resilient-to-Targeted-Impersonation | Resilient-to-Throttled-Guessing | Resilient-to-Unthrottled-Guessing | Resilient-to-Internal-Observation | Resilient-to-Leaks-from-Other-Verifiers | Resilient-to-Phishing | Resilient-to-Theft | No-Trusted-Third-Party | Requiring-Explicit-Consent | Unlinkable |
| **PIN** | | | + | | * | + | + | + | + | * | | * | * | * | + | + | * | * | | * | * | * | * | * | |
| **Just Tap** | | | + | | * | * | | + | * | * | | * | * | * | * | | * | * | | * | * | * | * | * | |
| **REPLICATE** | | | + | | * | * | | + | * | * | | * | | * | * | + | * | * | | * | * | * | * | * | |

TABLE 5. COMPARING REPLICATE AGAINST PIN AND TAP-TO-AUTHENTICATE USING THE FRAMEWORK OF BONNEAU ET AL. [26]. '*' REPRESENTS THAT THE SCHEME "OFFERS" THE BENEFIT AND '+' REPRESENTS THAT THE SCHEME "SOMEWHAT OFFER" THE BENEFIT.

- REPLICATE fairs better than PIN based 2FAs across all dimensions including time and SUS scores.

# Demo

# Much more in the paper …

# Thanks.

## Countering Concurrent Login Attacks in "Just Tap" Push-based Authentication: A Redesign and Usability Evaluations

Jay Prakash[1,2], Clarice Chua Qing Yu [1,2], Tanvi Ravindra Thombre[2], Andrei Bytes[2], Mohammed Jubur[3], Nitesh Saxena[3], Lucienne Blessing[2], Jianying Zhou[2], and Tony Q.S Quek[2]

[1] Silence Laboratories, Singapore
[2] Singapore University of Technology and Design, Singapore
[3]University of Alabama at Birmingham, USA

***Abstract*—In this paper, we highlight a fundamental vulnerability associated with the widely adopted "Just Tap" push-based authentication in the face of a concurrency attack, and propose the method REPLICATE , a redesign to counter this vulnerability. In the concurrency attack, the attacker launches the login session at the same time the user initiates a session, and the user may be fooled, with high likelihood, into accepting the push notification which corresponds to the attacker's session, thinking it is their own. The attack stems from the fact that the login notification is not explicitly mapped to the login session running on the browser in the Just Tap approach. REPLICATE attempts to address this fundamental flaw by having the user approve the login attempt by replicating the information presented on the browser session over to the login notification, such as by moving a key in a particular direction, choosing a particular shape, etc. We report on the design and a systematic usability study of REPLICATE. Even without being aware of the vulnerability, in general, participants placed multiple variants of REPLICATE in competition to the Just Tap and fairly above PIN-based authentication.**

### 1. Introduction

Push notification based authentication, such as seen in solutions like, Duo-Push [1] or Authy [2], has witnessed a sharp rise in adoption in the past few years. It has been deployed as second-factor authentication (TFA) or password-less authentication. A device is first enrolled as a token device and associated with an *(account, service)* pair. Next, whenever a user attempts to log in to an application or web-service, and enters the correct credentials, the token device receives a push notification. When the user opens/taps on the notification, a screen overlay requests if the user wants to approve or deny the login attempt (Figure 1). The usability pain point is well relieved by this "Just Tap" push-based authentication compared to traditional one-time PIN (OTP) based TFA as there is no need to copy the PIN code from the device to the login terminal/browser. Hence, being more usable than OTP-based TFA, push notification assisted authentication has witnessed growing user adoption as reflected in the success of Duo Security and commercial adoption by software and service giants like Twitter, Yahoo, Google [1], [3], [4] and academic entities.

However, Just Tap push-based authentication has a fundamental and easy-to-exploit vulnerability, which we

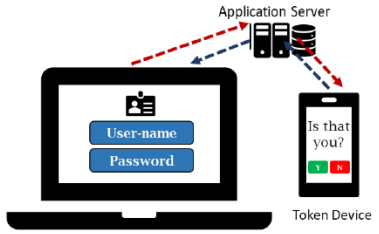



Figure 1. Conventional push-based, Just Tap to authenticate, TFA

call the "concurrency attack." In this attack, the malicious actor launches the login session at the same time as the user. The user may then be fooled, with high likelihood, into accepting the push notification corresponding to the attacker's session, allowing the attacker to successfully access the user's account. This will break the second-factor security offered by Just Tap TFA, assuming the attacker has already compromised the first factor, the password (e.g. via hacked password databases). In the case of Just Tap password-less authentication, the attacker does not need to compromise the user's password. In the concurrency attack, the attacker's goal is to confuse the legitimate user with two or more similar push notifications. As represented in Figure 3, the push notification prompts ask the user to tap on the "Yes" or "No" button. The only differentiating information from login attempt of an attacker is the location name, usually given as coordinates. However, this information is too coarse and gives ample scope of the attack. Also, the attacker can spoof the location. The legitimate user would have no definite way to identify the correct push notification or even the possibility of an adversarial login, and they will most likely approve the attacker's notification.

To better understand this attack context, we simulated the situation of concurrent logins with 75 pairs of legitimate users and the attacker. The study set consisted of diverse personas, including undergraduate students of different streams, faculties, corporate employees from both business and information technology(IT) domains, and retired and old users. Statistically, only 5% of people (mostly comprising of IT employees and a few university students) raised doubts when receiving such notifications in the concurrency attack. Most of the people approved