

# USER PERCEPTIONS OF SECURITY AND USABILITY OF MOBILE-BASED SINGLE PASSWORD AUTHENTICATION AND TWO- FACTOR AUTHENTICATION



**Devriş İşler**, imec-COSIC, KU Leuven, Leuven, Belgium

Alptekin Küpçü, Aykut Çoşkun, Koç University, Istanbul, Turkey

# CONTENT

- Introduction
- Two Factor Authentication
- Single Password Authentication (SPA)
  - Mobile-based SPA
- User Study Design
- Results
- Remarks
- Conclusion

# INTRODUCTION-TRADITIONAL AUTHENTICATION



*Alice*  
*(Alice, password)*



bank.com

Adds

*<Alice, Hash(password)>*  
to database

Alice, password

Alice, password

Accept/Reject

Checks the database  
if hashes match

*Registration*  
*Authentication*

# INTRODUCTION

## ***Traditional insecure approach:***

- **Insecure against offline dictionary, phishing, man-in-the-middle, and honeypot attacks**

Remembering **all passwords** is cumbersome for the user  
**Reuse** of the same password (Florencio et. al [5]) increases the damage of attack

**MOTHERBOARD**  
TECH BY VICE

## **Hacker Tries To Sell 427 Million Stolen MySpace Passwords For \$2,800**

A hacker and a paid search engine for hacked data claim to have a massive database stolen from MySpace at some point in the last few years.

User Perceptions of Security and Usability of Mobile-based SPA and 2FA

## **Hacker advertises details of 117 million LinkedIn users on darknet**

List of user IDs and passwords, allegedly sourced from cyber-attack in 2012, put on sale for around £1,500 as site says it is taking action



▲ LinkedIn's chief information security officer said the site is resetting the accounts of users it believes are affected. Photograph: Robert Galbraith/Reuters

A hacker claiming to have the log in details of millions of [LinkedIn](#) users is advertising the data for sale online.



# TWO FACTOR AUTHENTICATION (2FA)



Mobile-Device



Alice

(Alice, password, Tel)



bank.com

Alice, password, Tel

Adds  $\langle \text{Alice}, \text{Hash}(\text{password}), \text{Tel} \rangle$   
to database

*Registration*  
*Authentication*

Alice, password

Checks the database if  
hashes match

OTP code (e.g. via SMS)

Checks if OTP codes  
match

OTP code

OTP code

Accept/Reject

# TWO FACTOR AUTHENTICATION

## Attacks on 2FA?

[Home](#) > [Looking](#) > [Phishing](#)

INSIDER

Ph  
aut

Resea  
that c

### NIST EXPLAINS PROPOSED BAN ON SMS FOR 2FA



[Pindrop](#) > [Blog](#) > NIST Explains Proposed Ban on SMS for 2FA

A few days after releasing draft authentication guidelines that propose deprecating SMS as a second factor for authentication, NIST officials provided more context on the move, saying it's a result of advances in attacks and shifts in the threat landscape.

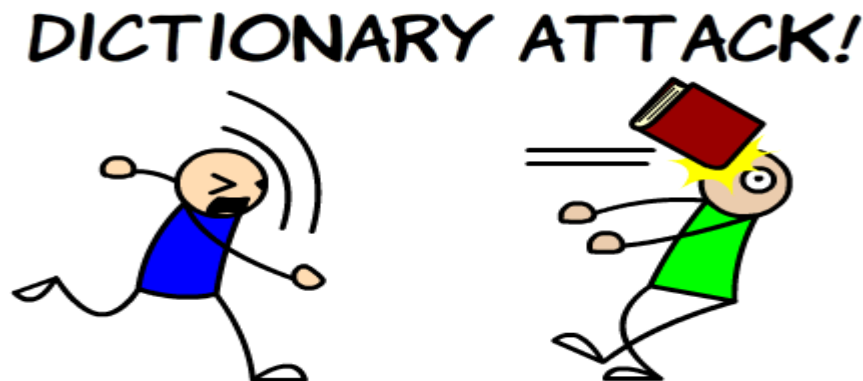
Factor  
execute

Automate phishing attacks



# SINGLE PASSWORD AUTHENTICATION

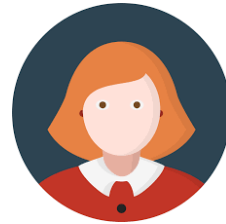
- **Acar et. al [1]**, and also by Jarecki et. al [2], Bicakci et. al [3], and İşler and Küpçü [4]
  - Proposed a secure and usable approach
  - A user remembers only **one single password** and username for all her accounts
- Secure against **phishing, man-in-the-middle, and honeypot attacks**
- When login server and storage provider (e.g. mobile device) collude (or both are corrupted by an attacker), can perform **offline dictionary attack**,



# MOBILE-BASED SINGLE PASSWORD AUTHENTICATION (MOBILE-BASED SPA)



(Trusted) Mobile-Device



(Alice, password, Tel)



bank.com

Generate a key  $K$  (e.g. MAC key)

$c_{text} \leftarrow \text{Encrypt}(\text{Hash}(\text{password}), K)$

$c_{text}$  (via QR code)

Alice,  $K$



Forget everything except her single password

Registration



# MOBILE-BASED SINGLE PASSWORD AUTHENTICATION (MOBILE-BASED SPA - ACAR ET. AL [1])



(Trusted) Mobile Device  
(c<sub>text</sub>)



(Alice, password)

Alice



bank.com (tel, K)

Challenge *chal* (e.g. via SMS)

*password*

$K \leftarrow \text{Decrypt}(\text{Hash}(\text{password}), \text{c}_{\text{text}})$

$\text{resp} \leftarrow \text{GenerateResp}(K, \text{chal})$









*resp*

*resp*

Accept/Reject  $\text{resp} \stackrel{?}{\equiv} \text{GenerateResp}(K, \text{chal})$

**Authentication**

# 2FA VS. MOBILE-BASED SPA

	2FA	Mobile-based SPA
Security against offline dictionary attacks		
Security against Phishing & Man-in-the-middle attacks		
Provable security		
Single password usage		

# USER STUDY DESIGN

- **Testing Environment:**

- User studies are conducted in the Koç University's Media and Virtual Arts Lab.
- Pre-installed (e.g. no installation )
- Participants tried both Mobile-based SPA and 2FA (random order)

- Created 3 banking-like website (e.g. Bank A)
- NEXMO SMS service for Mobile-based SPA
- Google Authenticator for 2FA

- **Participants:**

- There were 25 participants
  - 14 female, 11 male
  - They had diverse educational backgrounds

# USER STUDY DESIGN

- **Measures:**
  - **Demographic questionnaire:** sex, age interval, education level, and experience with online/mobile banking.
  - **Post-questionnaire:** 4-point Likert scale (strongly disagree, disagree, agree, strongly agree).
    - Numerical evaluation
    - **Paired t-test:** assesses whether the means of two groups are *statistically* different from each other.
  - **Comments:**
    - discussion with the participants about each system they tested, their feelings and concerns

# USER STUDY DESIGN

- Measured the following properties for each study;

*Effort expectancy*  
*Anxiety*  
*Behavioral intention to use the system*  
*Attitude towards using technology*  
*Performance expectancy*

} Standard questionnaire

*Perceived security*

# RESULTS

- The majority of participants (*more than 50% per question*) agreed (or strongly agreed) that mobile-based SPA ;
  - Is easy to use,
  - Is useful,
  - Is trustworthy,
  - Is not intimidating to use,
  - Has a positive attitude towards and intention to using this system



# RESULTS

- **Anxiety:** Mobile-based SPA was less threatening than two-factor authentication ( $t(24) = 2.77$  and  $p = 0.01$ ),
  - **96%** : not scared to lose a lot of information by hitting the wrong key in mobile-based SPA.

*“There was nothing to worry, since I did not give any important information to the websites.”*

- **Attitude towards using technology :** Mobile-based SPA performed statistically significantly better compared to 2FA ( $t(24) = 2.71$  and  $p = 0.01$ )

*“I found two things she wanted at the same time, which are usability (easing her job by remembering one password) and more security (via employing a personal device and challenge).”*

# RESULTS

- **Perceived security:** The users trusted mobile-based SPA more than they trust 2FA ( $t(24) = 3.25$  and  $p = 0.003$ )
- **80%** : typing the password on the mobile device made the user feel more secure,

*“Seeing all works (computations) carried out on the mobile device made me feel more secure, and I felt as though I had the control of my password security”*

# RESULTS

- There was **no significant difference** between mobile-based SPA and 2FA regarding :
  - **Effort expectancy** ( $t(24) = 1.10$  and  $p = 0.28$ ),
  - **Behavioral intention to use the system** ( $t(24) = 0.00$  and  $p = 1.00$ ),
  - **Performance expectancy** ( $t(24) = 1.04$  and  $p = 0.30$ ).

# RESULTS

## Success and failure rate

The percentage distribution of password attempts to login

	Success percent at trial number			
	1	2	3	Failure (%)
2FA	82	5	4	9
Mobile-based SPA	100	0	0	0

- 2FA had **no failure** due to authentication code but had **failure** due to password.
- Mobile-based SPA had **20% failure** due to **authentication code** but had **no failure** due to password.

# REMARKS

- **Password Creation and Recall:** 85% of the users struggle while coming up with a strong password as well as recalling them.
  - **Hierarchy** : *different password for different type of accounts*

## Recall:

- **Paper** : *note passwords on a paper*
- **Creating hint** : *hint for recalling a password*
- **Password Reset:**
  - **Traditional authentication & 2FA:**
    - logging in to a backup e-mail = another password,
    - memorizing extra information (such as security questions)

**Mobile-based SPA:** Re-compute the registration 😞 How a secure single password reset can be efficiently carried out?

# REMARKS

- **Widespread:**

**52%** : use the mobile-based SPA and trust it if it is commonly used and advertised by a "trusted" authority such as Facebook.

*"I feel secure while I am using WhatsApp, since WhatsApp is employed for secure messaging. They use something like encryption."*

- **Complexity of the Solution:** More complex, more secure?

- **90%** : mobile-based SPA provided a better security for online banking
- Secure in the online banking scenario because it was "complex" enough.
- **Unproductive** for email type daily purposes due to its complexity,



# CONCLUSION

- We implemented mobile-based single password authentication method of Acar et. al [1] and conducted its usability analysis for **the first time**.
- Our study constitutes an important step in understanding the usability of SPA systems regarding their future deployment.
- We compared it against 2FA in a fake online banking scenario
- There is potentially a trade-off between usability and perceived security which is worth exploring.
- To obtain more generalizable results:
  - taking place in a natural settings instead of a lab environment,
  - examining other dimensions of user experience of SPA systems beyond usability.

# ACKNOWLEDGEMENT

- We acknowledge the support of;
  - TÜBİTAK (The Scientific and Technological Research Council of Turkey) under Project numbers 115E766,
  - The Royal Society of UK Newton Advanced Fellowship NA140464
  - ERC Advanced Grant ERC-2015-AdG-IMPACT
  - The FWO under an Odysseus project GOH9718N
- We thank;
  - Arjen Kılıç and İlker Kadir Öztürk for their efforts on implementation

**THANK YOU VERY MUCH**



# REFERENCES

- [1] T. Acar, M. Belenkiy, and A. Küpçü. Single password authentication. *Computer Networks*, 2013.
- [2] S. Jarecki, H. Krawczyk, M. Shirvanian, and N. Saxena. Device-enhanced password protocols with optimal online-offline protection. *ACM on Asia Conference on Computer and Communications Security*, pages, 2016.
- [3] K. Bicakci, N. B. Atalay, M. Yuceel, and P. C. van Oorschot. Exploration and field study of a browser-based password manager using icon-based passwords. In *Workshop on Real-Life Cryptographic Protocols and Standardization*, 2011.
- [4] D. İşler and A. Küpçü, *Threshold Single Password Authentication, ESORICS DPM 2017*
- [5] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, 2007.

# Post Questionnaire-1

## Effort Expectancy (EE)

(EE1) My interaction with the system would be clear and understandable

(EE2) It would be easy for me to become skillful at using the system

(EE3) I would find the system easy to use

(EE4) Learning to operate the system is easy for me

## Anxiety (A)

(A1) I feel apprehensive (worried) about using the system

(A2) It scares me to think that I could lose a lot of information using the system by hitting the wrong key

(A3) I hesitate to use the system for fear of making mistakes I cannot correct

(A4) The system is somewhat intimidating to me

# Post Questionnaire-2

## Behavioral intention to use the system (BIU)

(BIU1) I intend to use the system in the next 6 months.

(BIU2) I predict I would use the system in the next 6 months

(BIU3) I plan to use the system in the next 6 months

## Attitude towards using technology (ATUT)

(ATUT1) Using the system is a good idea.

(ATUT2) The system makes work more interesting

(ATUT3) Working With the system is fun

(ATUT4) I like working with the system



# Post Questionnaire-3

## Performance Expectancy (PE)

(PE1) I would find the system useful in my job

(PE2) Using the system enables me to accomplish tasks more quickly

(PE3) Using the system increases my productivity

(PE4) If I use the system, I will increase my chances of getting a raise

## Perceived Security (PS)

(PS1) I trust my password with this system.

(PS2) I feel secure using this system for daily use.

(PS3) I feel secure using this system for online banking.

(PS4) I feel secure reusing the same password for multiple sites employing this system.

# Demographics

**Table 1.** Responses of the participants regarding technical information

How often do you use your mobile device?		Do you have prior knowledge of password security?	
So often (Daily)	24	I heard from news, social media etc.	16
Few times in a day	1	I had a course	6
Weekly	0	Not me but someone I know had experience	3
How often do you use mobile banking?		How often do you use online banking?	
Daily	4	Daily	4
Weekly	11	Weekly	9
Monthly	5	Monthly	7
Rarely	0	Rarely	3
Never	5	Never	2
Have you ever used a browser extension?		Have you ever used a password manager?	
Yes	16	Yes	4
No	4	No	17
Never Heard	5	Never Heard	4
How often do you change your password?			
Weekly	1	Monthly	4
Every 3 months	4	Every 6 months	2
Once a year	0	If I have to	14



**Table 5.** Post-Questionnaire Percentage Distribution

<b>Mobile-based SPA</b>																							
	EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
<b>Strongly Disagree</b>	4	4	0	4	20	36	24	24	0	0	4	0	4	0	0	8	16	12	12	0	0	0	4
<b>Disagree</b>	16	8	12	12	64	60	64	56	40	48	52	20	12	28	24	28	32	40	72	12	12	24	12
<b>Agree</b>	52	56	56	48	12	4	12	16	48	36	32	48	52	44	44	28	32	36	16	64	64	40	52
<b>Strongly Agree</b>	28	32	32	36	4	0	0	4	12	16	12	32	32	28	32	36	20	12	0	24	24	36	32
<b>Two Factor Authentication</b>																							
	EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
<b>Strongly Disagree</b>	0	0	0	0	4	16	12	8	4	4	4	4	24	20	12	16	32	16	20	16	8	8	28
<b>Disagree</b>	4	8	16	0	72	56	68	60	32	36	52	36	20	16	28	28	32	36	68	40	32	40	28
<b>Agree</b>	60	68	60	52	20	16	16	28	52	48	32	52	48	56	44	40	28	36	8	32	48	36	32
<b>Strongly Agree</b>	36	24	24	48	4	12	4	4	12	12	12	8	8	8	16	16	8	12	4	12	12	16	12



Google authenticator

Mobile-based SPA



