Maginot Line: Assessing a New Cross-app Threat to PII-as-Factor Authentication in Chinese Mobile Apps

Fannv He, Yan Jia, Jiayu Zhao, Yue Fang,
Jice Wang, Mengyue Feng, Peng Liu, and Yuqing Zhang

NIPC, University of Chinese Academy of Sciences
DISSec, Nankai University
The Pennsylvania State University
Xidian University
Hainan University

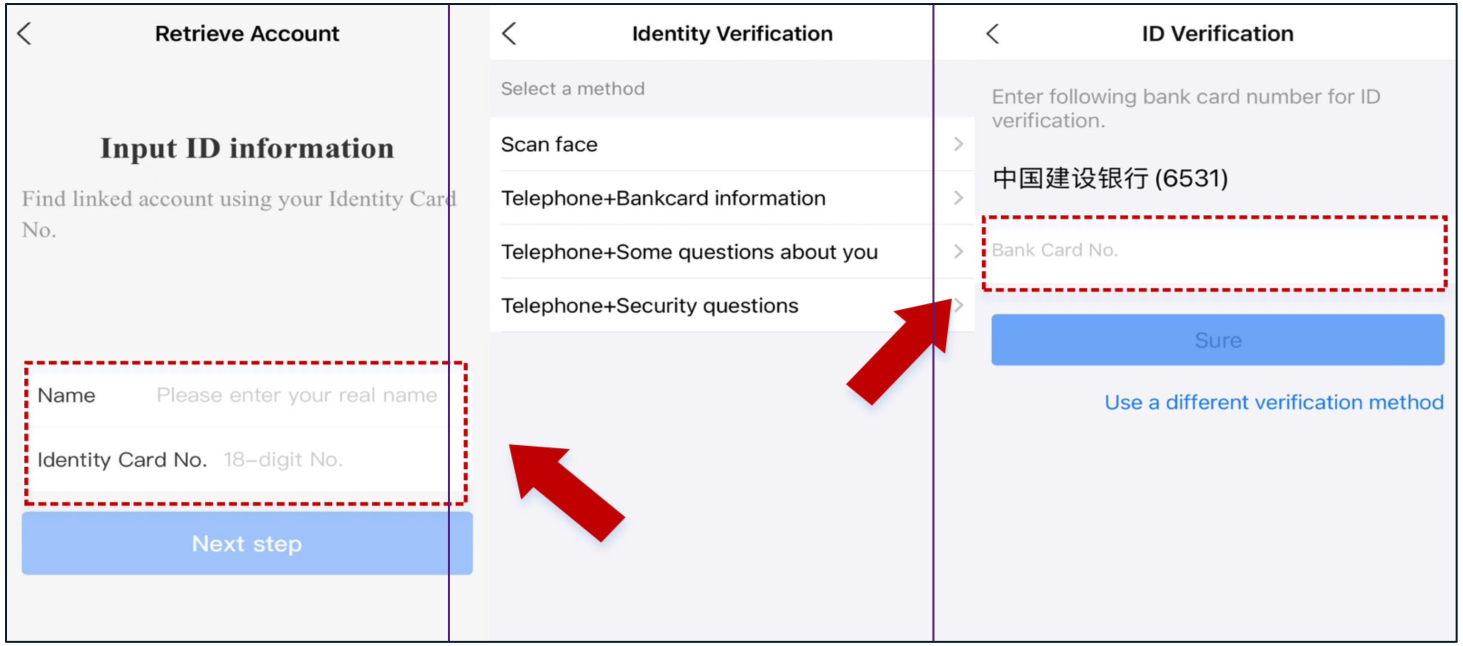
NDSS SYMPOSIUM/2024

Presented by Internet Society

What is PII-as-Factor Authentication?

What is PII-as-Factor Authentication?

Personally identifiable information (PII) serves as additional secrets to authenticate users.



Retrieve Account

Input ID information

Find linked account using your Identity Card No.

Name Please enter your real name

Identity Card No. 18–digit No.

Next step

Identity Verification

Select a method

Scan face

Telephone+Bankcard information

Telephone+Some questions about you

Telephone+Security questions

ID Verification

Enter following bank card number for ID verification.

中国建设银行 (6531)

Bank Card No.

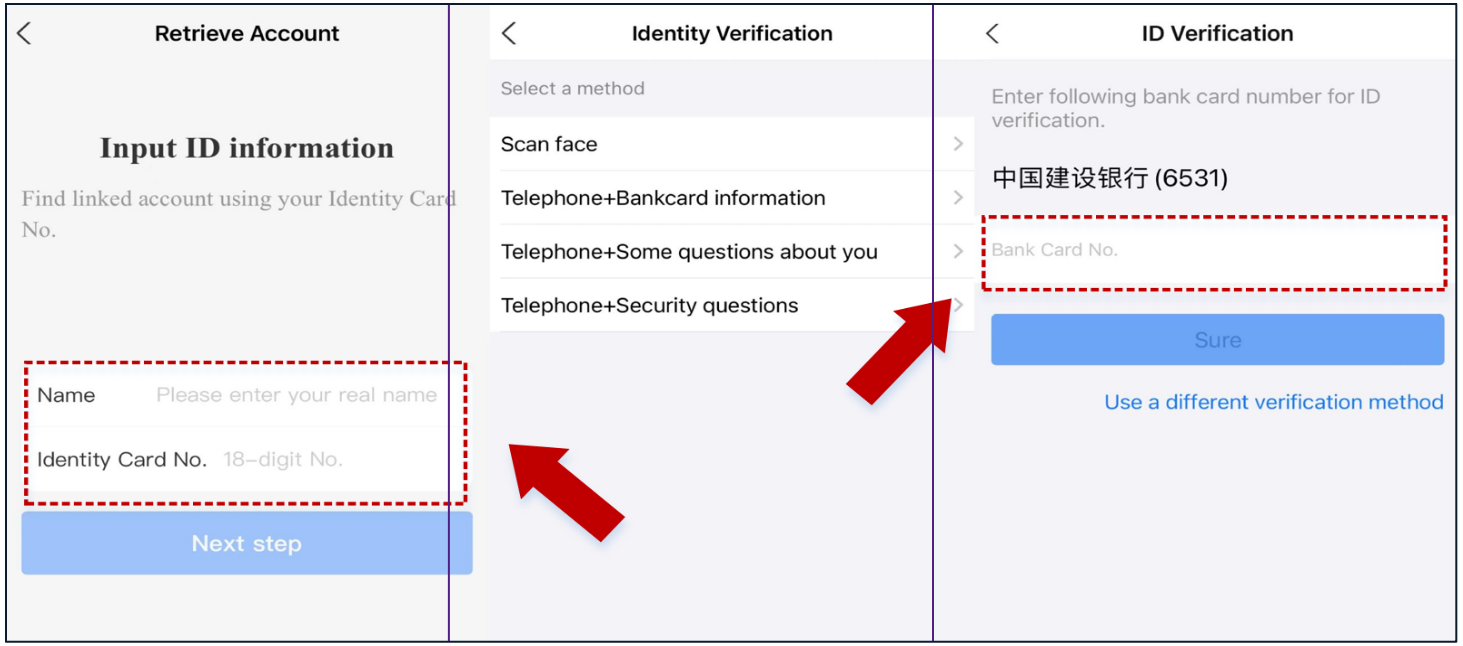
Sure

Use a different verification method

PaFA mechanisms designed by Alipay

What is PII-as-Factor Authentication?

Personally identifiable information (PII) serves as additional secrets to authenticate users.



Retrieve Account

Input ID information

Find linked account using your Identity Card No.

Name Please enter your real name

Identity Card No. 18–digit No.

Next step

Identity Verification

Select a method

Scan face

Telephone+Bankcard information

Telephone+Some questions about you

Telephone+Security questions

ID Verification

Enter following bank card number for ID verification.

中国建设银行 (6531)

Bank Card No.

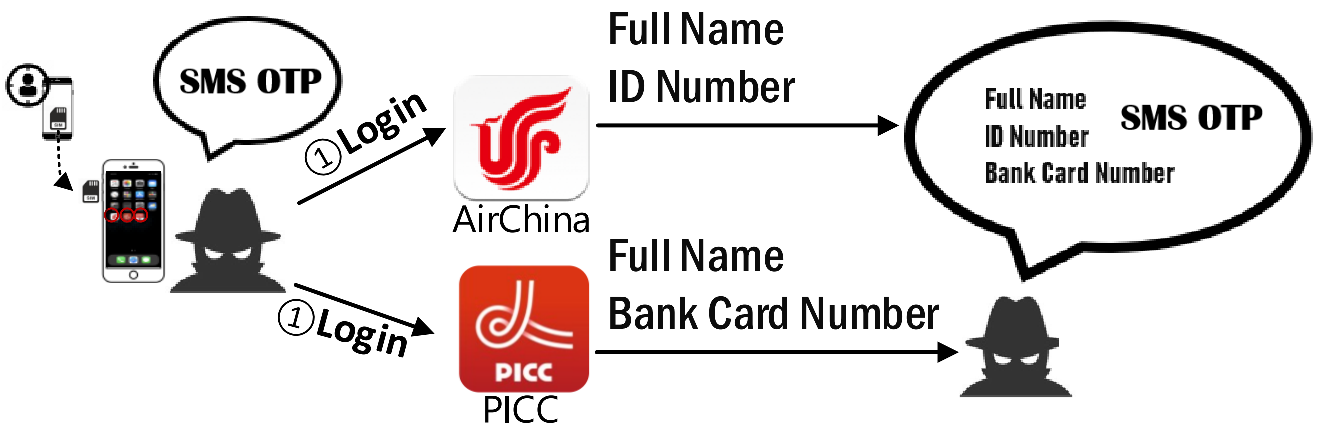
Sure

Use a different verification method

PaFA mechanisms designed by Alipay

Is PaFA effective?

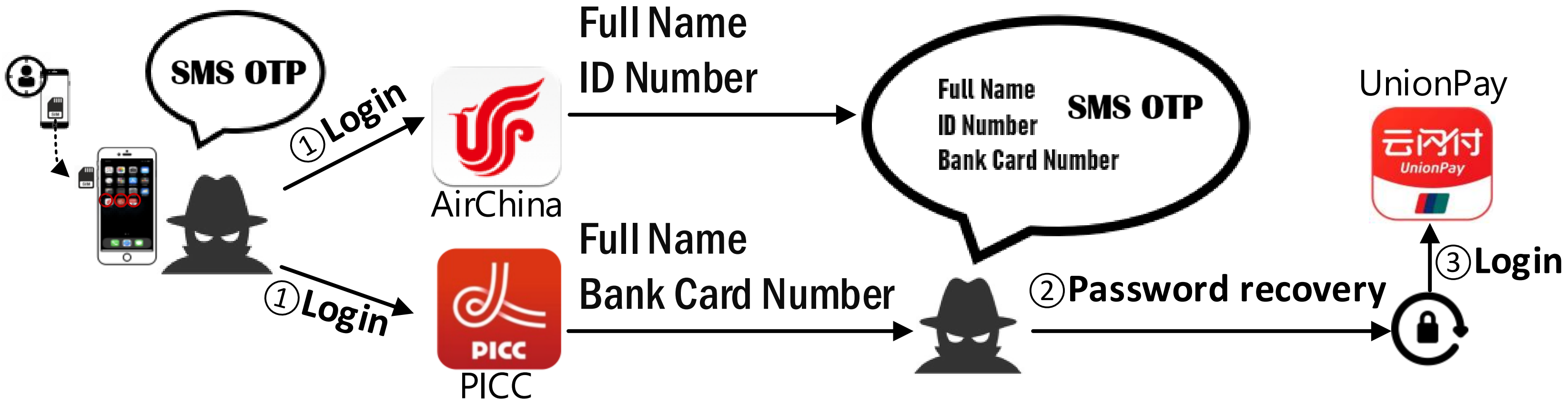
A Motivating Case



An attack path for UnionPay.

- Log in to AirChina and PICC and **gather useful PII**.

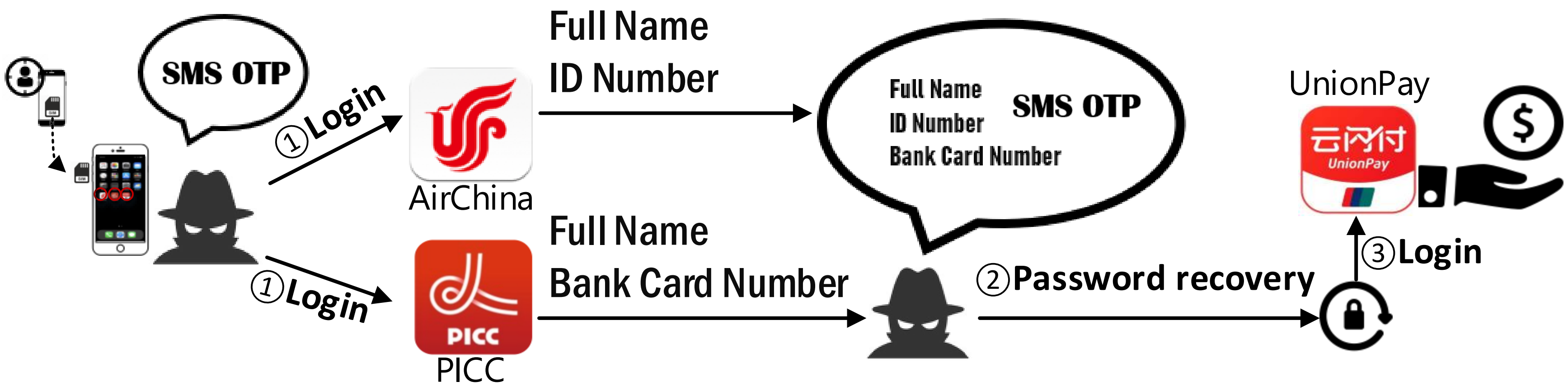
A Motivating Case



An attack path for UnionPay.

- Log in to AirChina and PICC and **gather useful PII**.
- **Reset login and payment passwords** of the UnionPay.

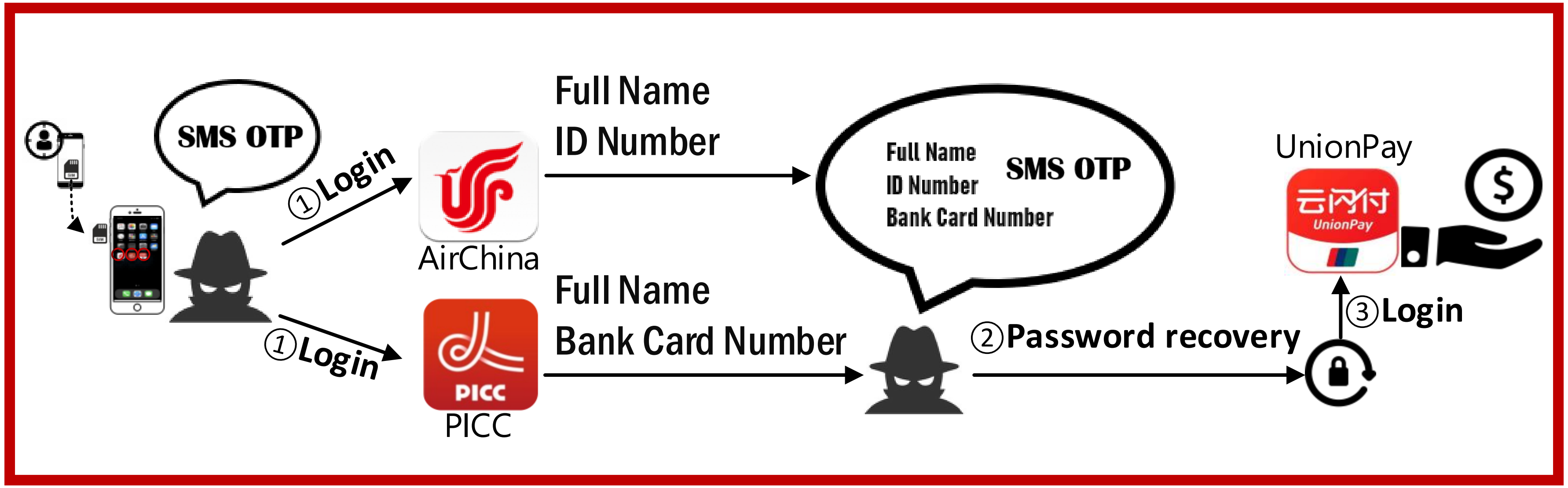
A Motivating Case



An attack path for UnionPay.

- Log in to AirChina and PICC and **gather useful PII**.
- **Reset login and payment passwords** of the UnionPay.
- **Transfer money** from UnionPay account.

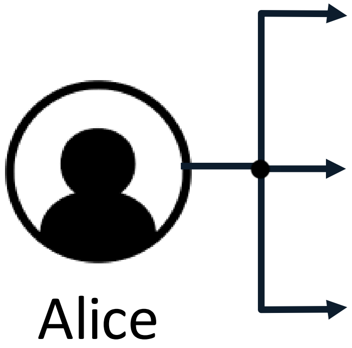
A Motivating Case



(**B**ypass **A**uthentication by **C**ross **A**pp **E**xploitation)

Bacae attack

Threat Model



A normal user

installed numerous popular apps

provided real personal information to these apps

Threat Model

Alice

- A normal user
- installed numerous popular apps
- provided real personal information to these apps

VS

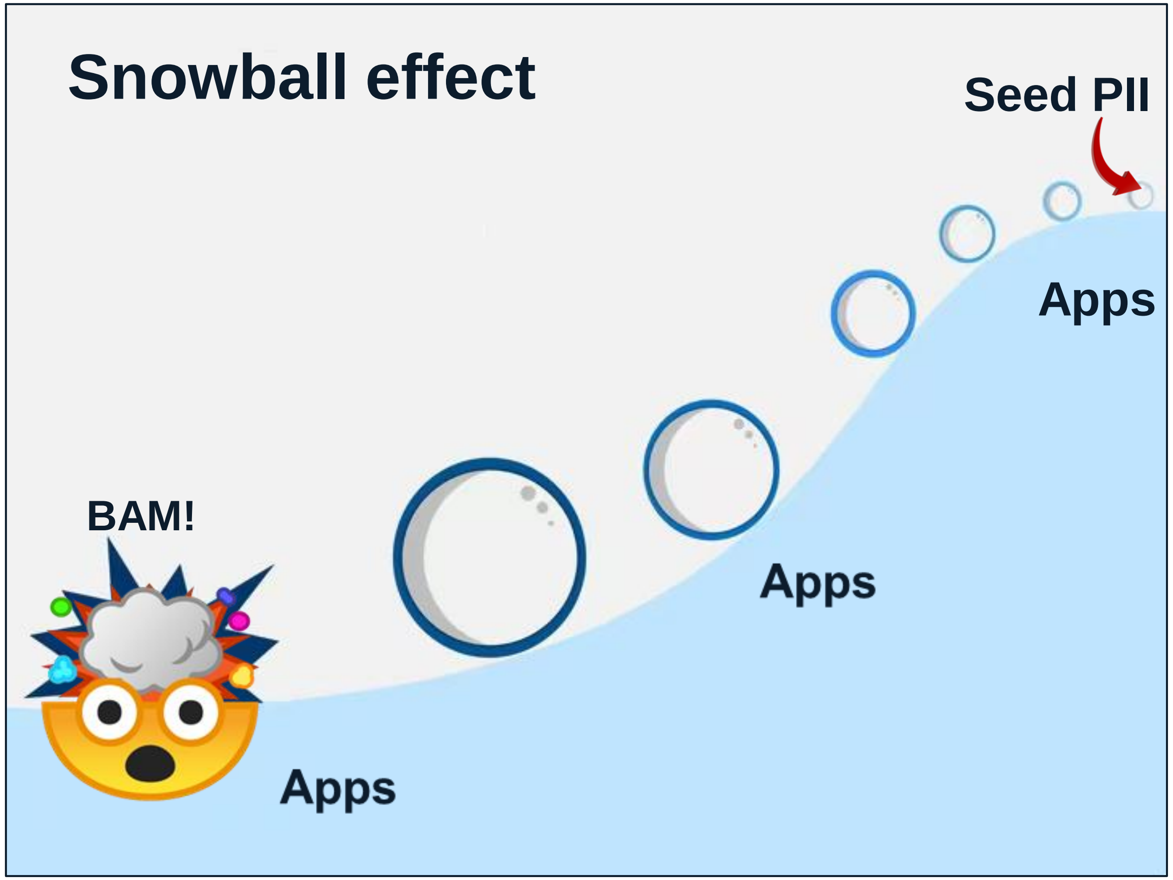
Mallory

- An attacker
- Can only obtain Alice’s SMS OTP
- Aims to compromise the authentication mechanisms of a target app

Method

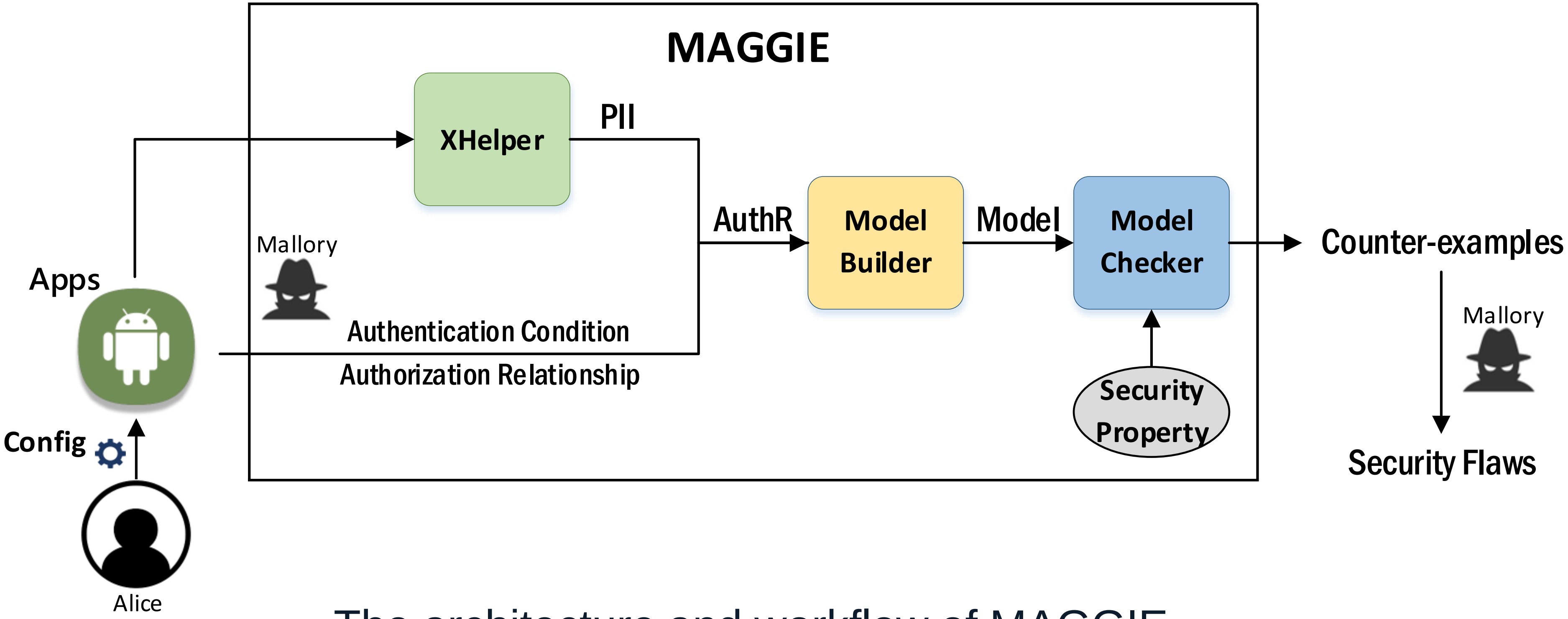
Our idea

- Act as the adversary 🕵
- Operate other apps
- Break the target authentication
- From “weak authentication” apps (obtain some **seed PII**)
- Achieve the “**snowball effect**”



Method

Architecture

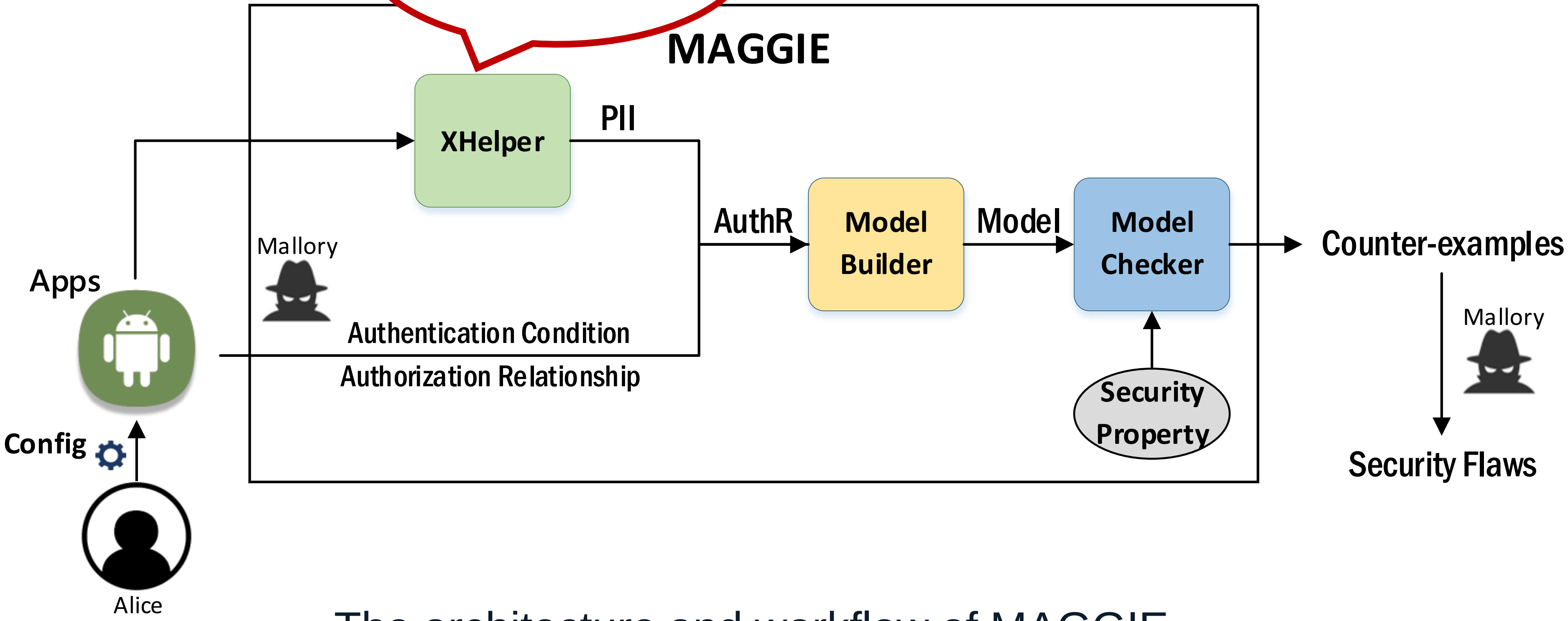


The architecture and workflow of MAGGIE.

Method

XHelper

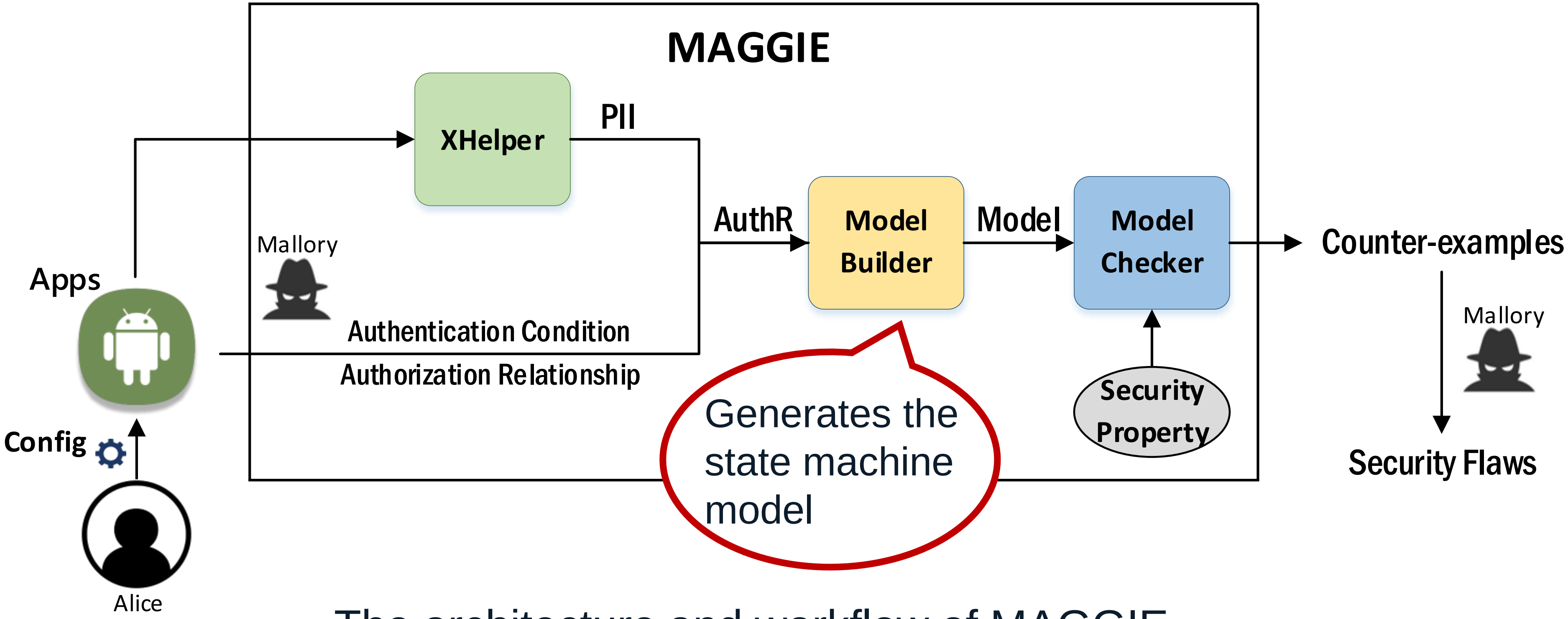
Gathers available **PII** in apps



The architecture and workflow of MAGGIE.

Method

Model Builder



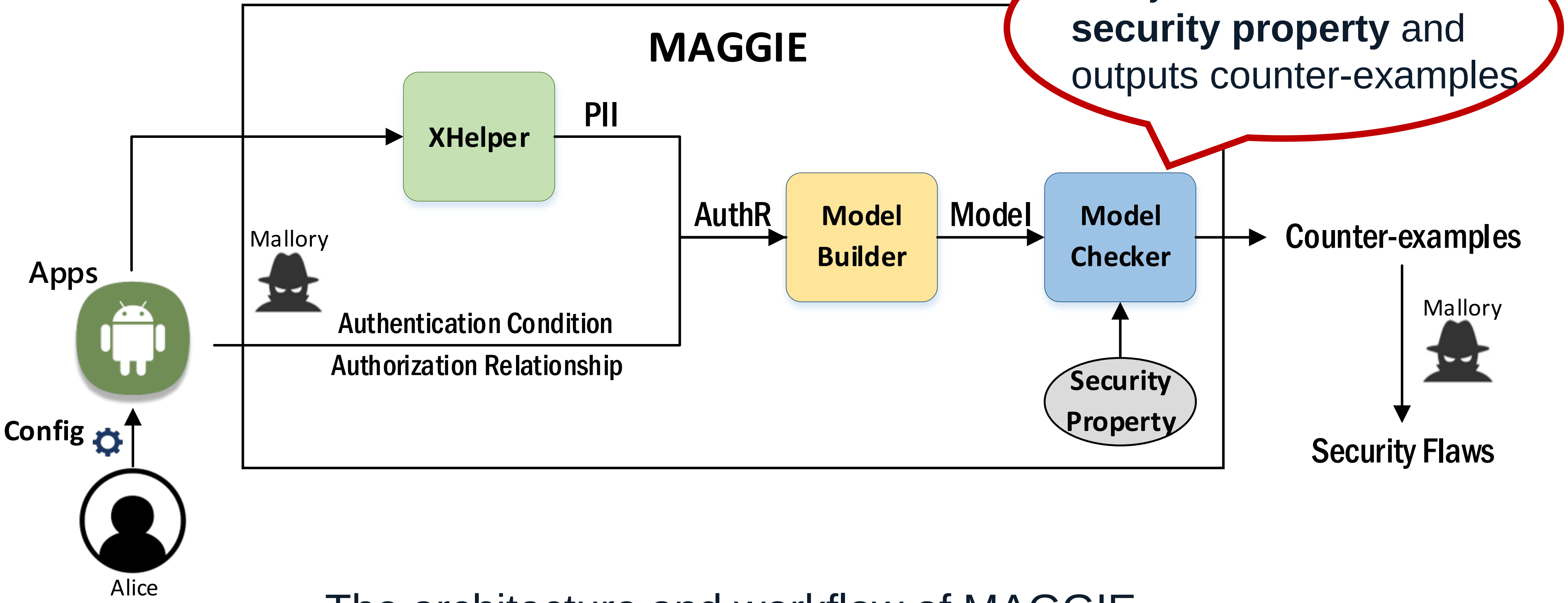
Generates the state machine model

The architecture and workflow of MAGGIE.

Method

Model Checker

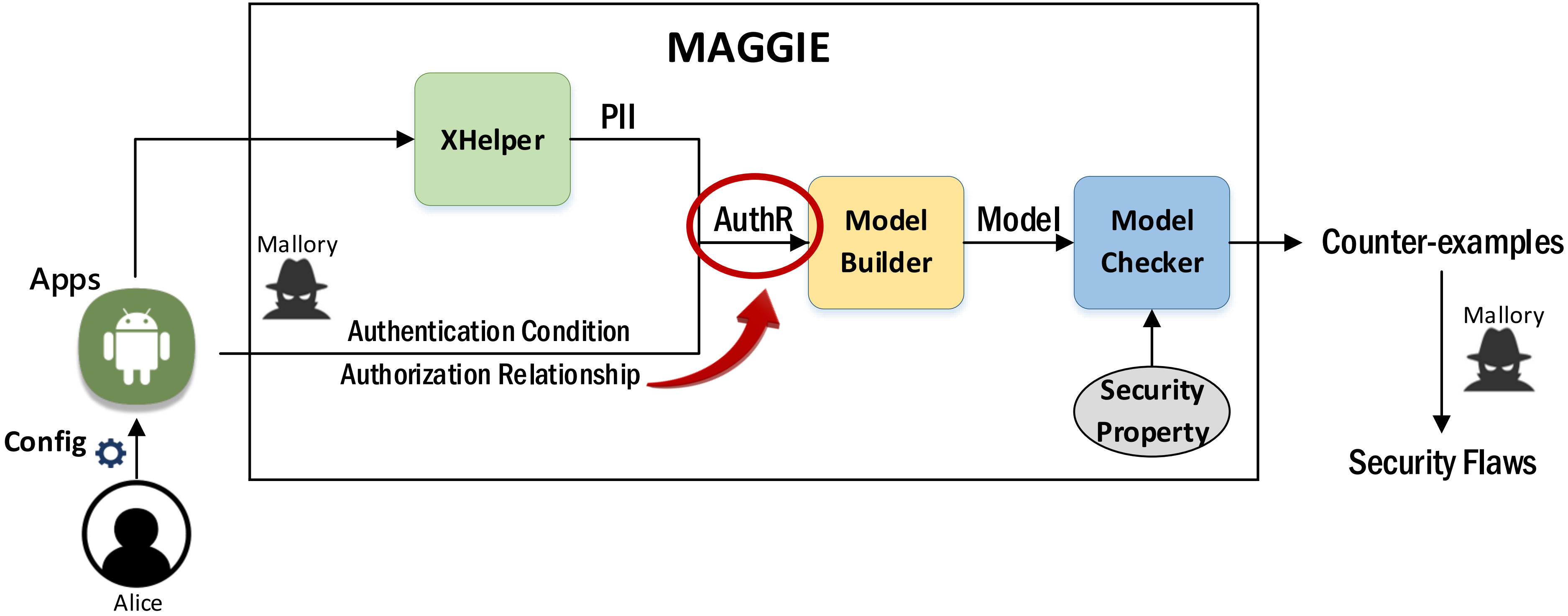
Analyzes the model with **security property** and outputs counter-examples



The architecture and workflow of MAGGIE.

Method

Authentication&Reward (AuthR)



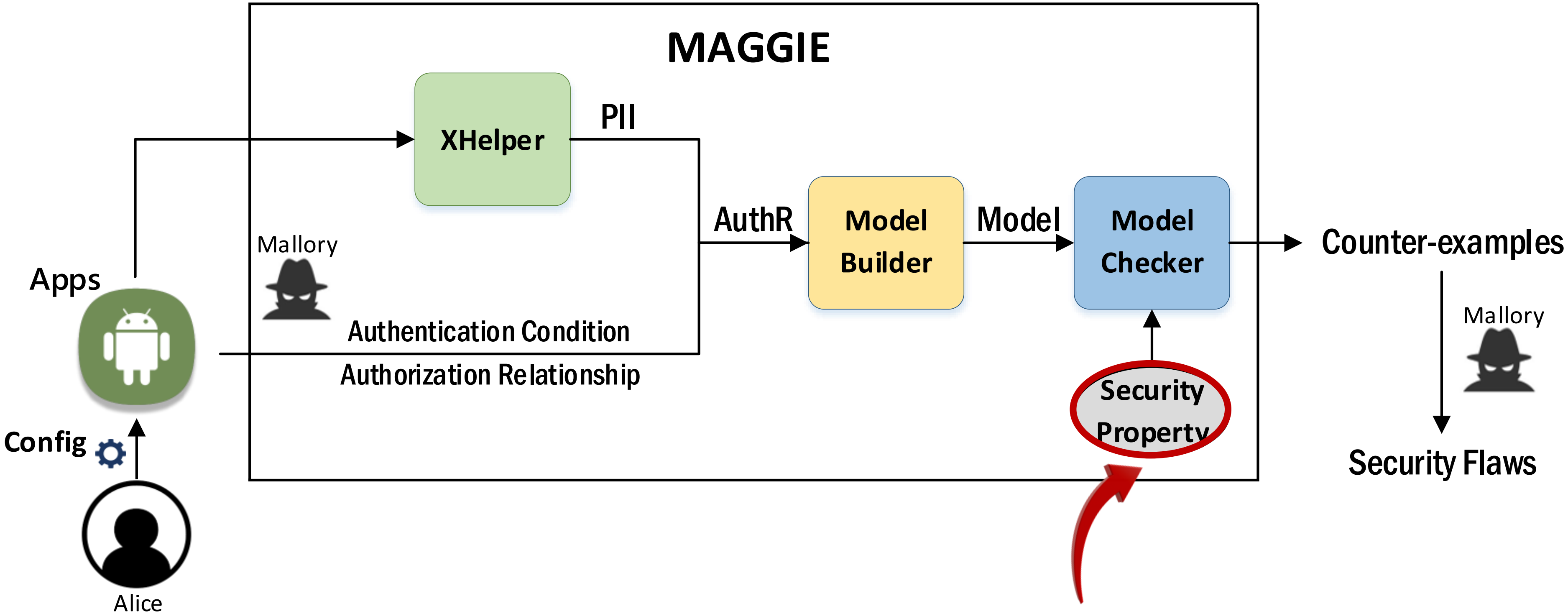
Method

AuthR::=(App.Op, Cond, Authorz, Reward)

- App.Op: **operations** within an app
- Cond: **SUCCESS** condition**,** a set of **authentication factors**
- **Authorz**: third-party delegated operations
- Reward: a set of **PII**

Method

Security property



Method

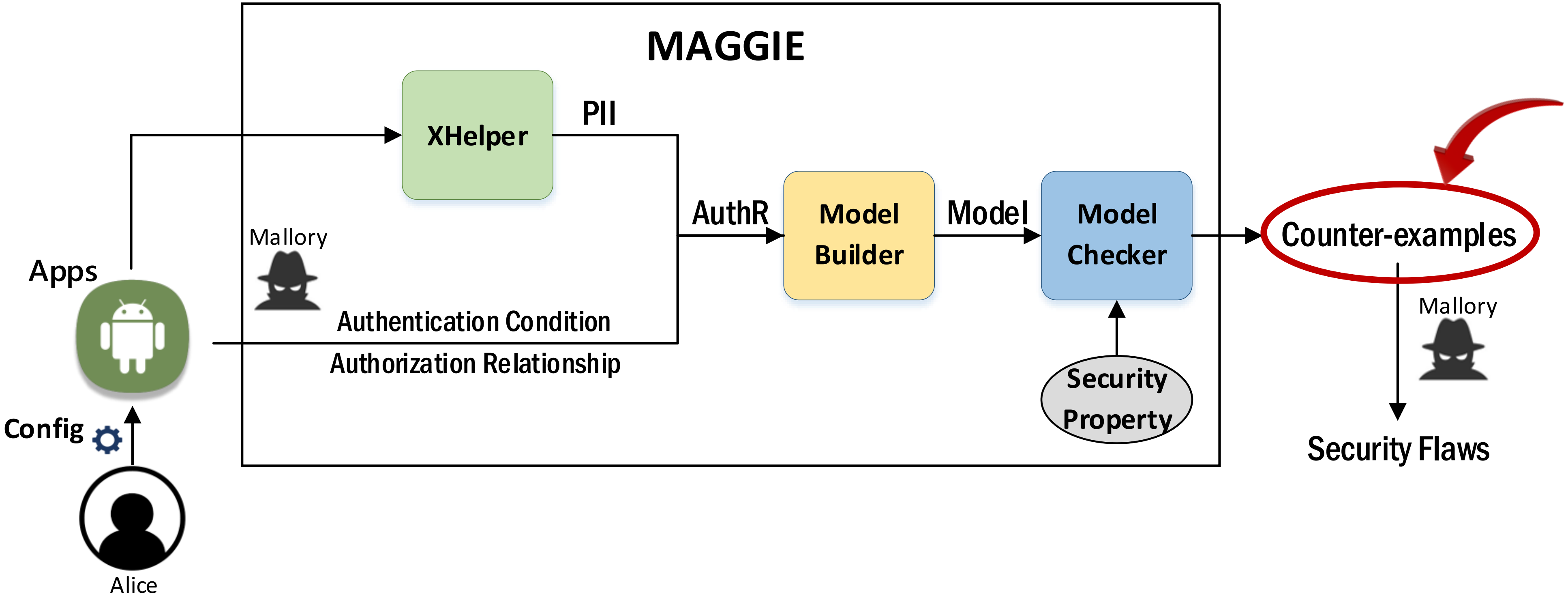
- AuthR::=(App.Op, Cond, Authorz, Reward)

- **Security property:** There should **NOT** be an access path.

App.Op

Method

Counter- example



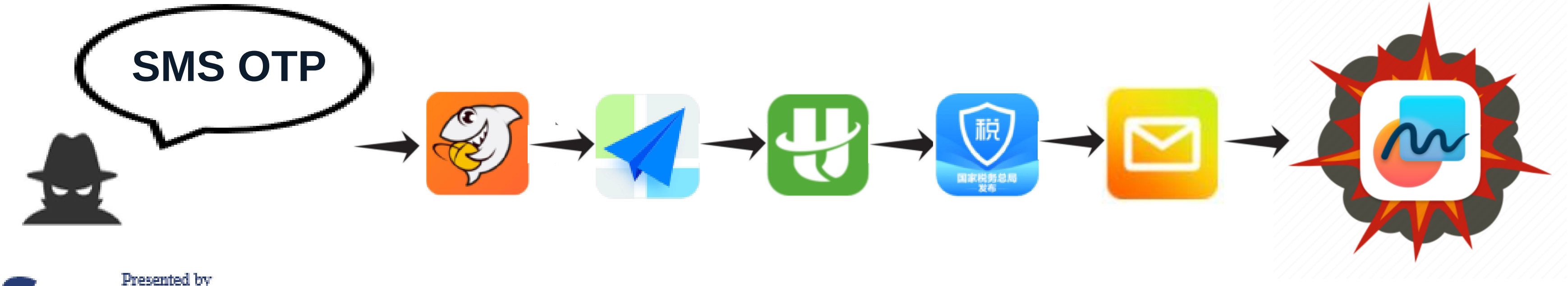
Method

- AuthR::=(App.Op, Cond, Authorz, Reward)

- Security property: There should NOT be an access path.

App.Op

- **Counter- example (security property violation) » Attack path**



SMS OTP

Dataset

- App Store: Huawei, Vivo, and Tencent App Centre
- **39 categories** (National Standard “GB/T 41391-2022”)
- Selected **top 6 apps** with the **highest total download numbers**
- **234 high-profile apps**
- June 2022

Measurement

Root Cause ➊ of Bacae Attack

- Ubiquitous PII in apps

Measurement

Root Cause ➊ of Bacae Attack

- Ubiquitous PII in apps

  Full exposure

Measurement

Root Cause ➊ of Bacae Attack

- Ubiquitous PII in apps

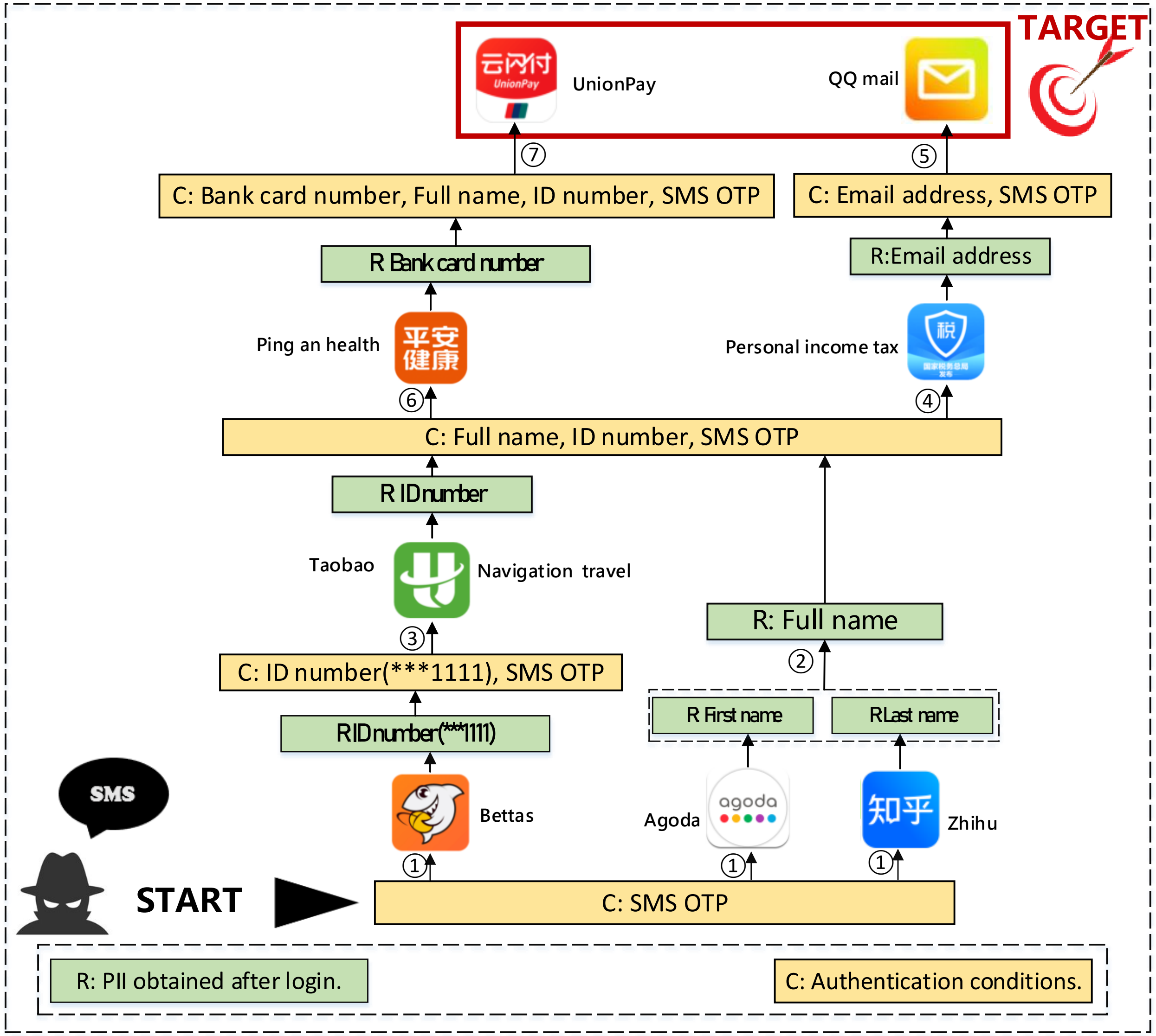
  Full exposure

  Risky partial exposure

Measurement

Root Cause ❶ of Bacae Attack

- Ubiquitous PII in apps
  - Full exposure
  - Risky partial exposure
- **Case study**



Measurement

Root Cause ❷ of Bacae Attack

- Cross-app business partnership

Measurement

Root Cause ❷ of Bacae Attack

- Cross-app business partnership

  Account sharing

  Business authorization

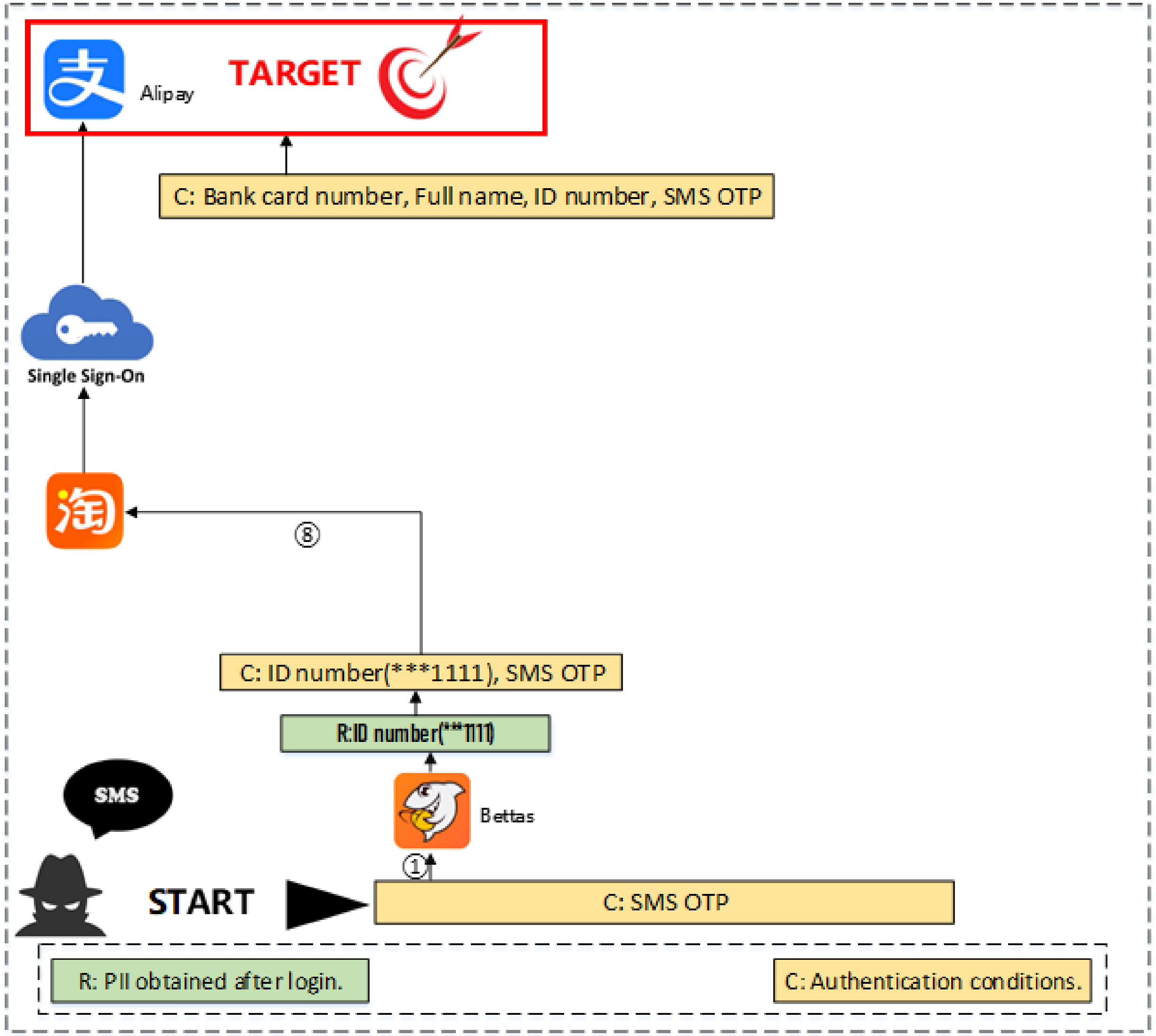
Measurement

Root Cause ❷ of Bacae Attack

- Cross-app business partnership

  Account sharing

  Business authorization
- **Case study**


Alipay
TARGET
C: Bank card number, Full name, ID number, SMS OTP
Single Sign-On
⑧
C: ID number(***1111), SMS OTP
R:ID number(***1111)
SMS
Bettas
①
START
C: SMS OTP
R: PII obtained after login.
C: Authentication conditions.

Measurement

Root Causes of Bacae Attack

- Ubiquitous PII in apps

  Full exposure

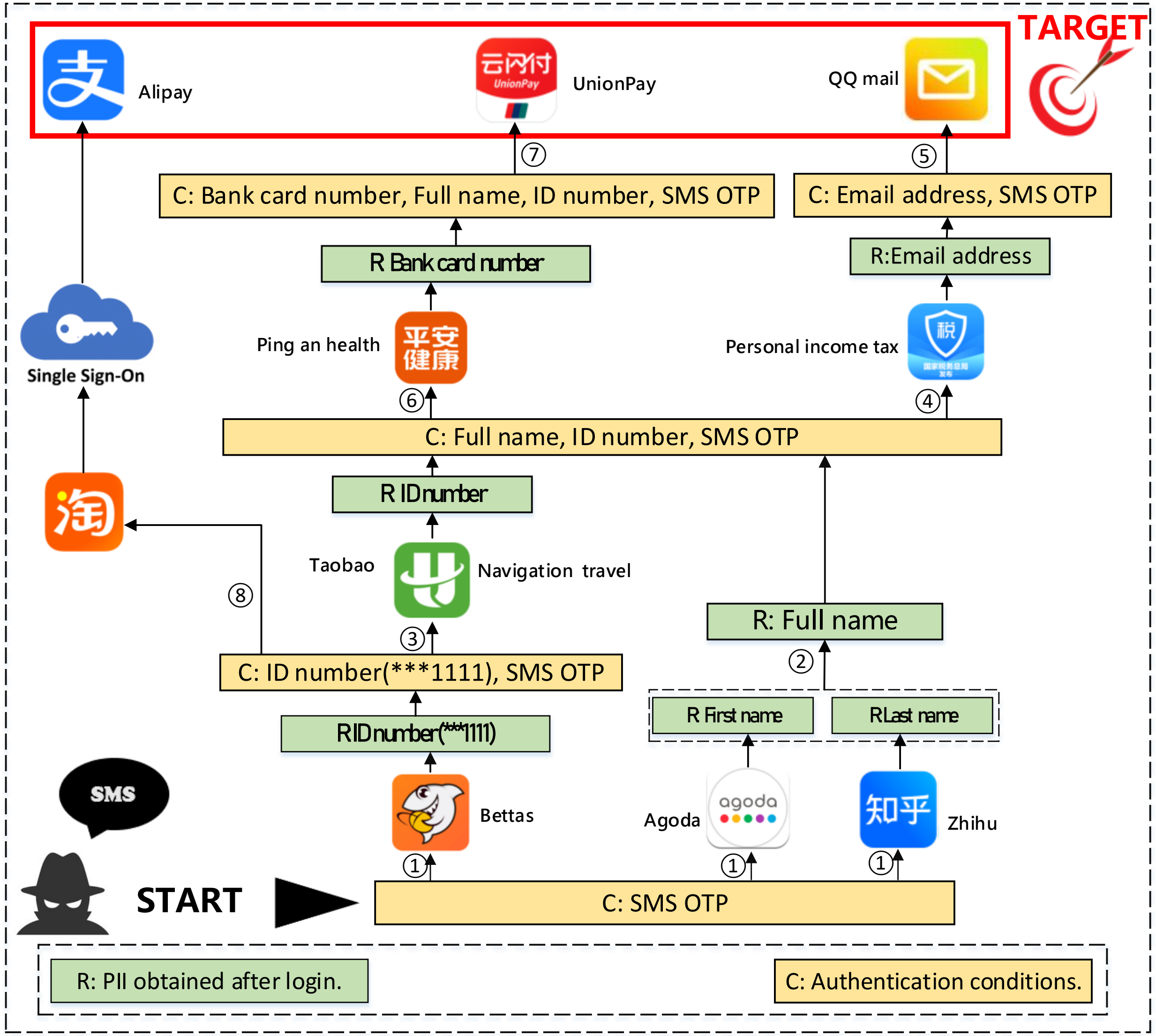
  Risky partial exposure

- Cross-app business partnership

  Account sharing

  Business authorization

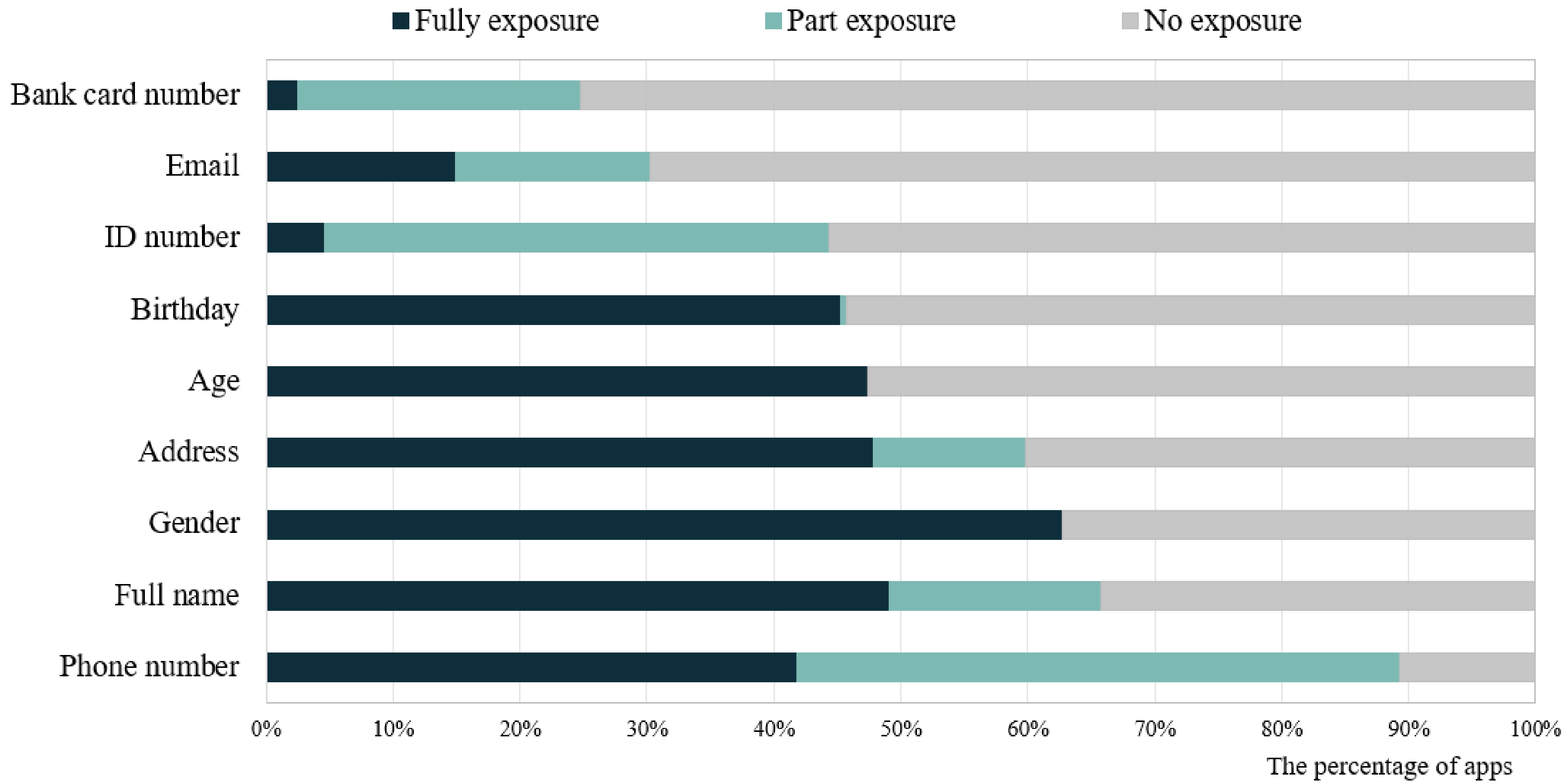
PaFA do NOT provide the expected security!



Statistic Results

PII availability

- **95.7%** of apps show PII on one or more UI pages.



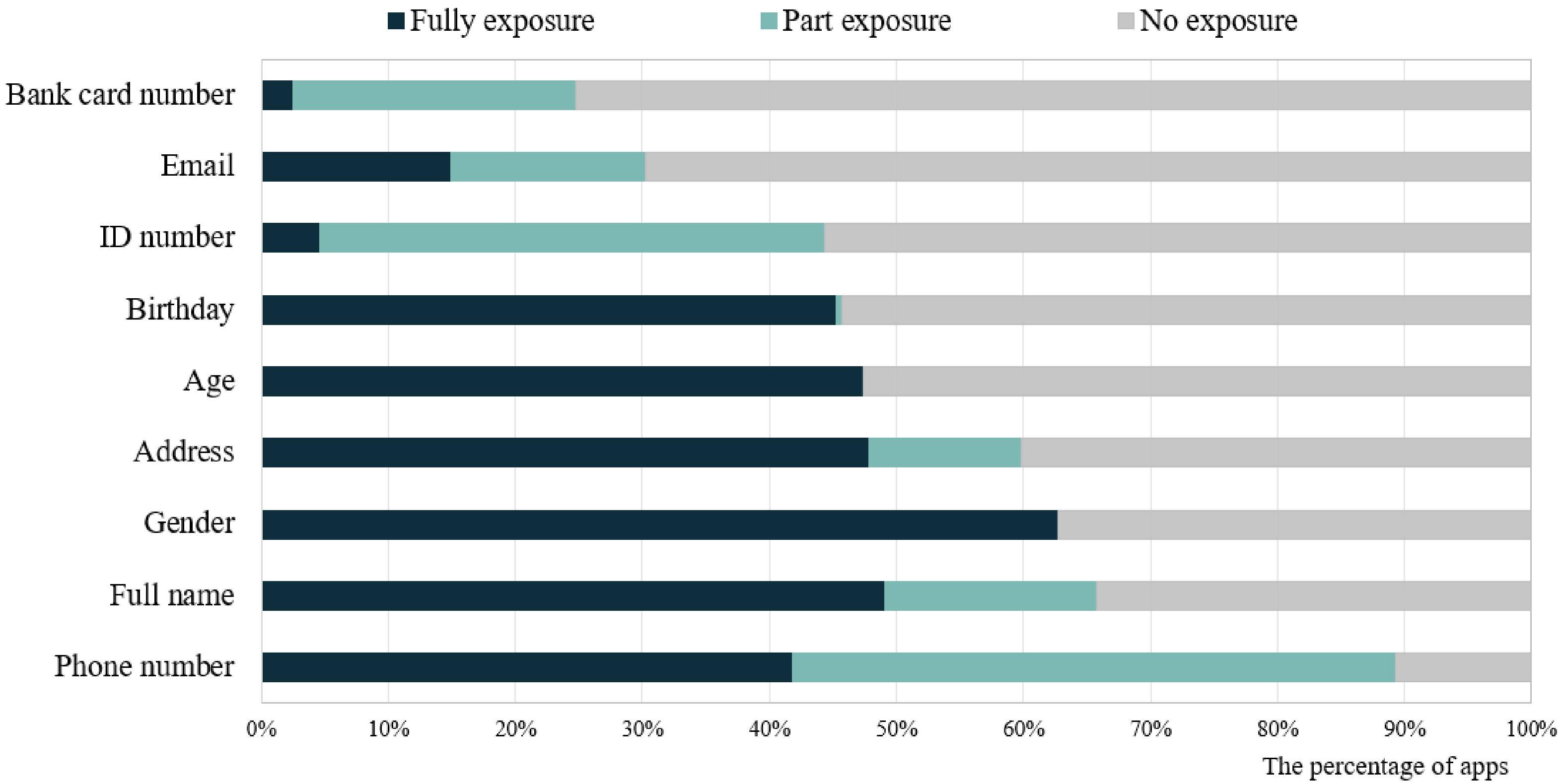
The percentage of apps that exposed personal data in 234 apps.

Statistic Results

PII availability

- **95.7%** of apps show PII on one or more UI pages.

- **86.3%** of apps have a complete display of PII.

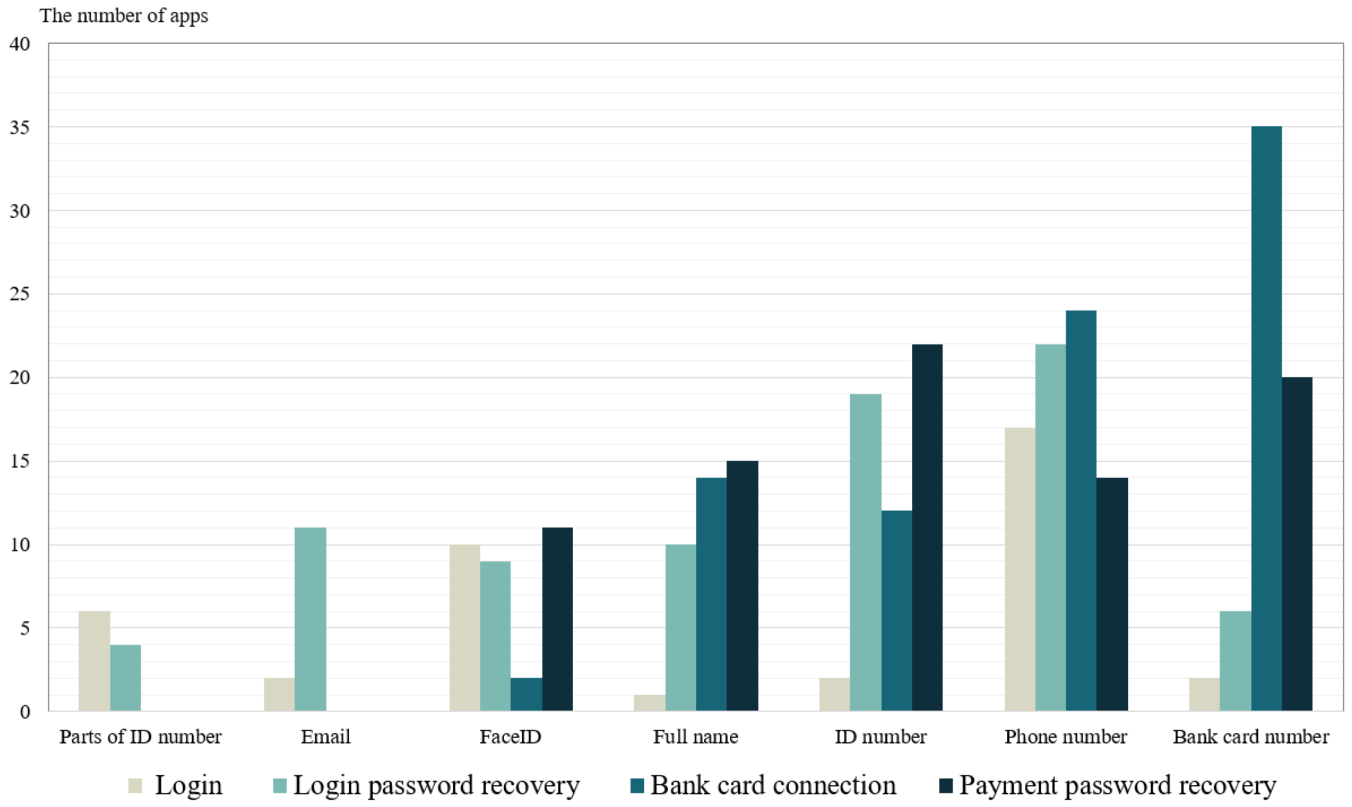


The percentage of apps that exposed personal data in 234 apps.

Statistic Results

PaFA deployment

- **65** out of 234 apps deployed PaFA.



PII usage in PaFA of 65 apps

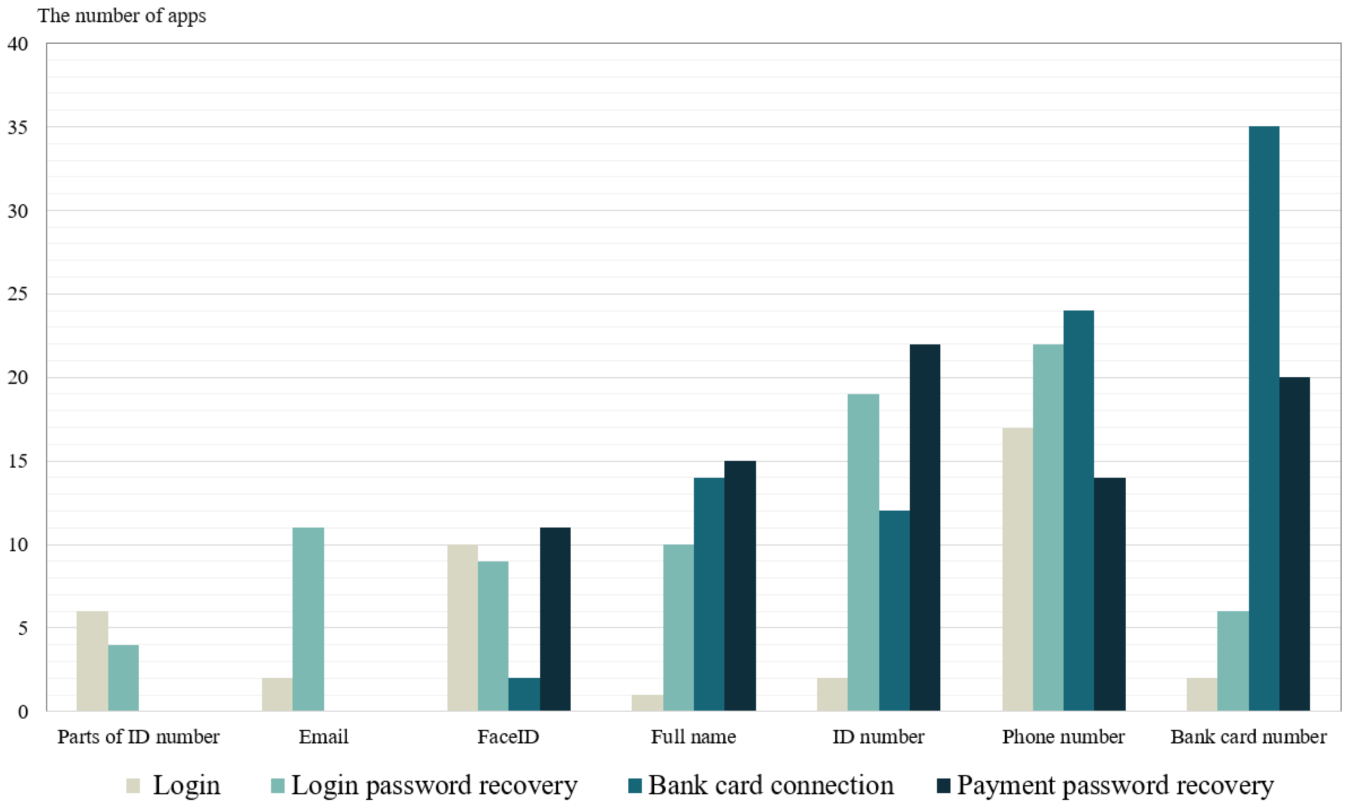
Statistic Results

PaFA deployment

- 65 out of 234 apps deployed PaFA.

Impact

- **75.4%** of PaFA deployed apps are susceptible to Bacae attacks.



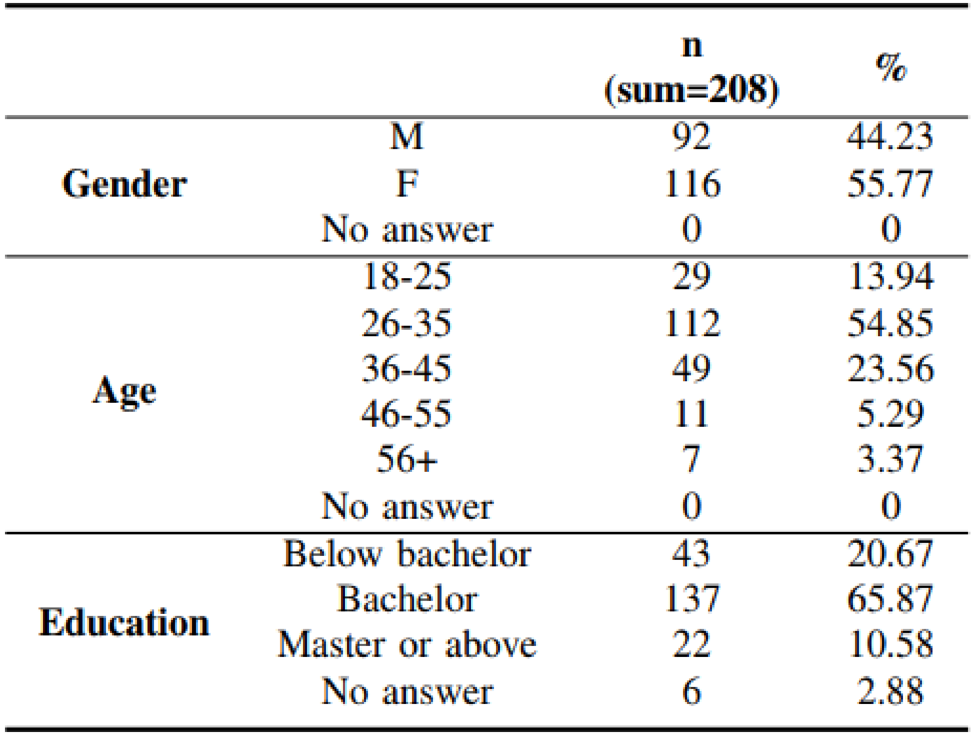
PII usage in PaFA of 65 apps

Statistic Results

User study

- 281 participants
- Select the apps (among 234 apps) had registered and used.
- 208 effective responses
- **94.2%** of participants had at least one attack path to break the authentication of an installed app.

DEMOGRAPHICS OF THE QUESTIONNAIRE PARTICIPANTS



		n (sum=208)	**%**
Gender	M	92	44.23
	F	116	55.77
	No answer	0	0
Age	18-25	29	13.94
	26-35	112	54.85
	36-45	49	23.56
	46-55	11	5.29
	56+	7	3.37
	No answer	0	0
Education	Below bachelor	43	20.67
	Bachelor	137	65.87
	Master or above	22	10.58
	No answer	6	2.88

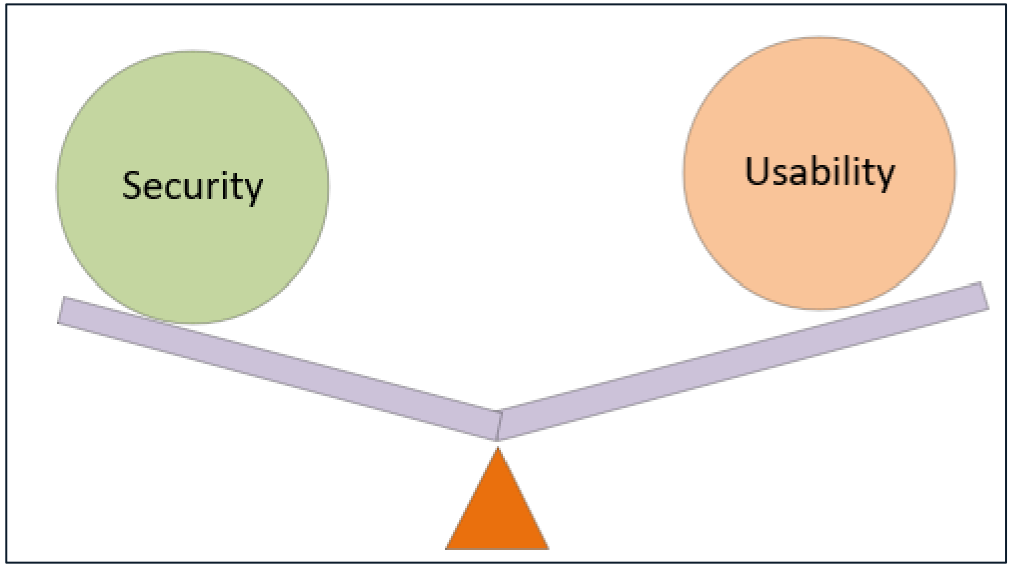
Discussion

Is PaFA effective? ✗

SMS OTP becomes the sole protection!

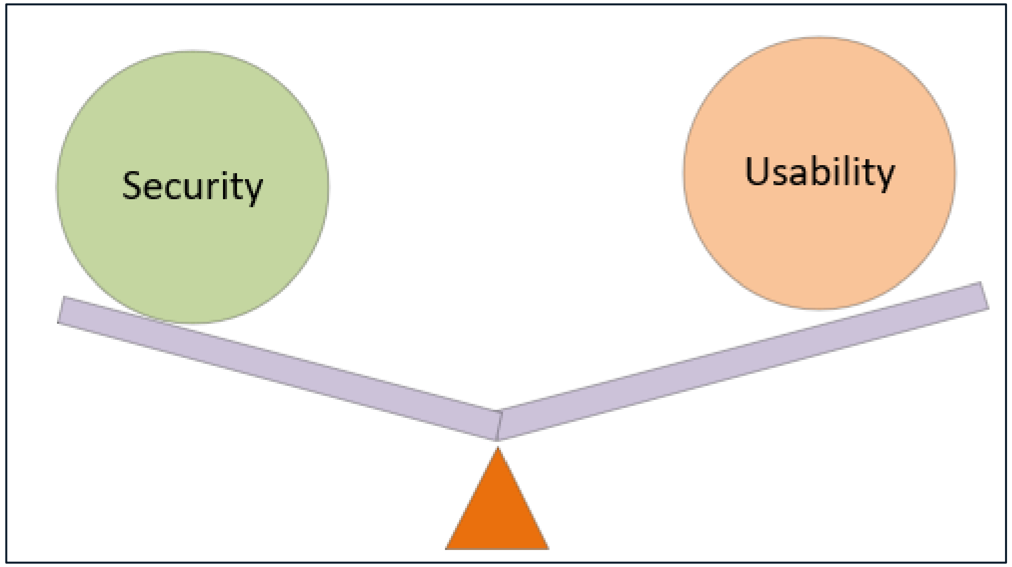
Risks Mitigation

- A standardized data display mechanism
- Additional biometric authentication mechanisms
- Do not rely on PII for authentication purposes



Risks Mitigation

- A standardized data display mechanism
- Additional biometric authentication mechanisms
- Do not rely on PII for authentication purposes



Striking a balance between security and usability remains a challenge!

THANK YOU!

Fannv He
hefn@nipc.org.cn