An Empirical Study of SMS One-Time Password Authentication in Android Apps

Siqi Ma, Runhan Feng, Juanru Li, Yang Liu, **Surya Nepal**, Diethelm Ostry, Elisa Bertino, Robert H. Deng, Zhuo Ma, Sanjay Jha

Data61 CSIRO, Shanghai Jiao Tong University, Xidian University, Purdue University, Singapore Management University, University of New South Wales

Outline

- <u>Authentication in Android</u>

- One-time password

- SMS OTP Analyzer

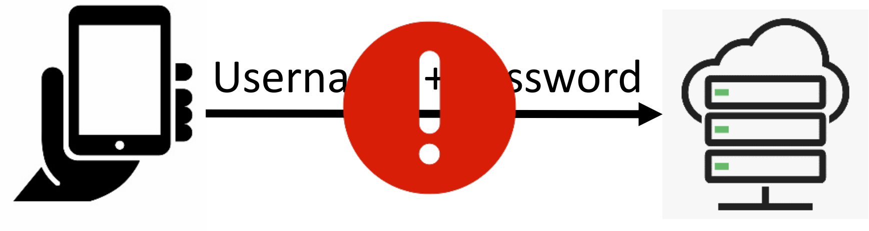
- Evaluation

- Conclusion

Authentication in Mobile Phones

Single-factor Authentication

- Password-based Authentication – GLACIATE (ESORICS’19)

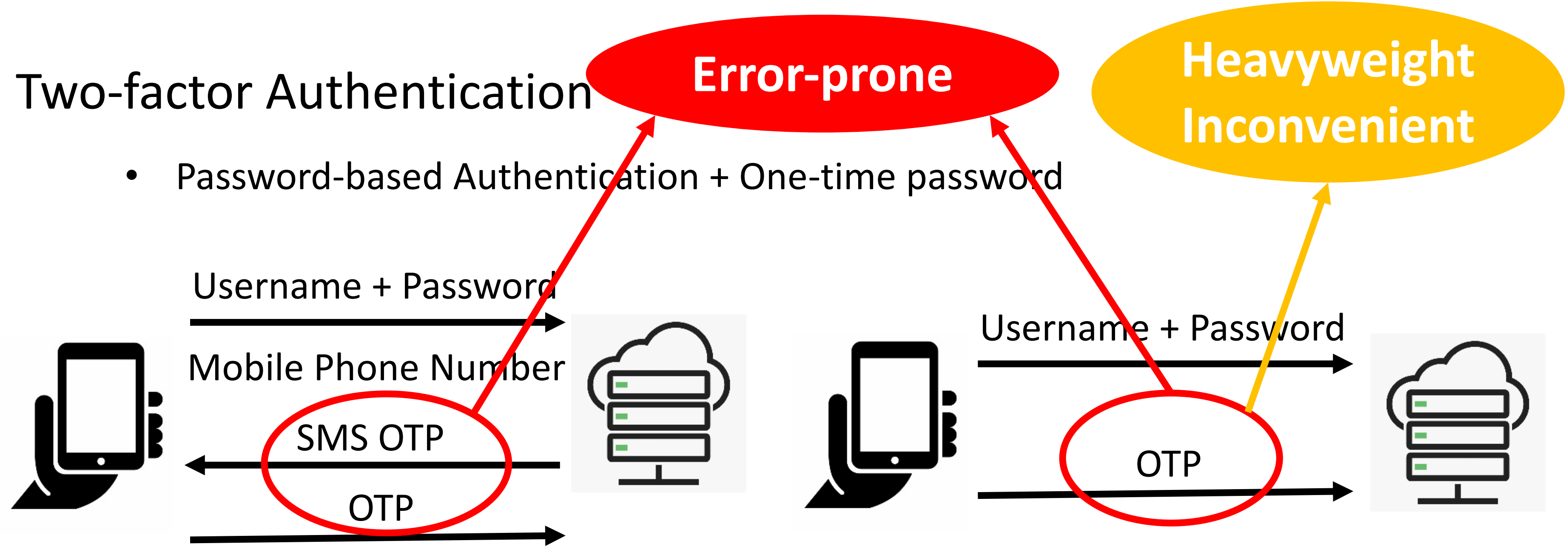


Weak passwords

Authentication in Mobile Phones

Two-factor Authentication

- Password-based Authentication + One-time password



Error-prone

Heavyweight

Inconvenient

Username + Password

Mobile Phone Number

SMS OTP

OTP

SMS OTP Authentication

Username + Password

OTP

Token OTP Authentication

Outline

- Authentication in Android
- <u>One-time password</u>
- SMS OTP Analyzer
- Evaluation
- Conclusion

OTP Authentication

HMAC-based OTP (HOTP)

- An incrementing counter value (C) and a secret key (K):

  $\text{HOTP}(K, C) = \text{Truncate}(\text{HMAC}(K, C))$

- Requirements:
  - Maximum number of possible attempts per login session.
  - An additional delay for each failed attempt.
  - Length should be at least Six digits

Timestamp-based OTP (TOTP)

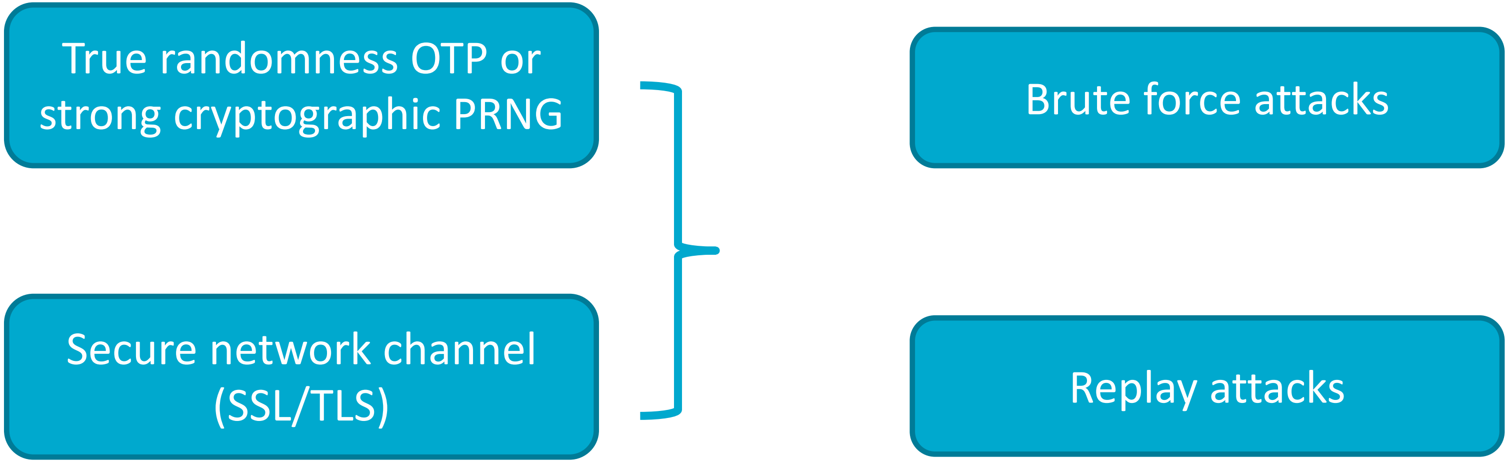
- A time step(C_T) and a secret key (K):

  $\text{TOTP} = \text{Truncated } (\text{HMAC}(K, C_T))$

- Requirements:
  - Set the time step for network delay to 30s.

Security Requirements for OTP

RFC Requirements



True randomness OTP or strong cryptographic PRNG

Secure network channel (SSL/TLS)

Brute force attacks

Replay attacks

OTP Rules

Security Rules	Description
Rule 1: OTP Randomness	Use a random value as an OTP for authentication.
Rule 2: OTP Length	Generate an OTP value with at least six digit.
Rule 3: Retry Attempts	Set a limit on the number of validation attempts.
Rule 4: OTP Consumption	Only allow each OTP value to be consumed once.
Rule 5: OTP Expiration	Reject expired OTP values generated by the TOTP algorithm.
Rule 6: OTP Renewal Interval	OTP values generated by the TOTP algorithm should be valid for at most 30s.

RFC 4226 – HOTP, RFC 2289 – OTP, RFC 6238 – TOTP

Rule Violations – Single

OTP Rules	Violations/Attacks
Rule 1: OTP Randomness	Replay attacks
Rule 2: OTP Length	Brute-force attacks
Rule 3: Retry Attempts	Brute-force attacks
Rule 4: OTP Consumption	Replay attacks
Rule 5: OTP Expiration	Unlimited time to discover the OTP
Rule 6: OTP Renewal Interval	A long time window to crack the OTP

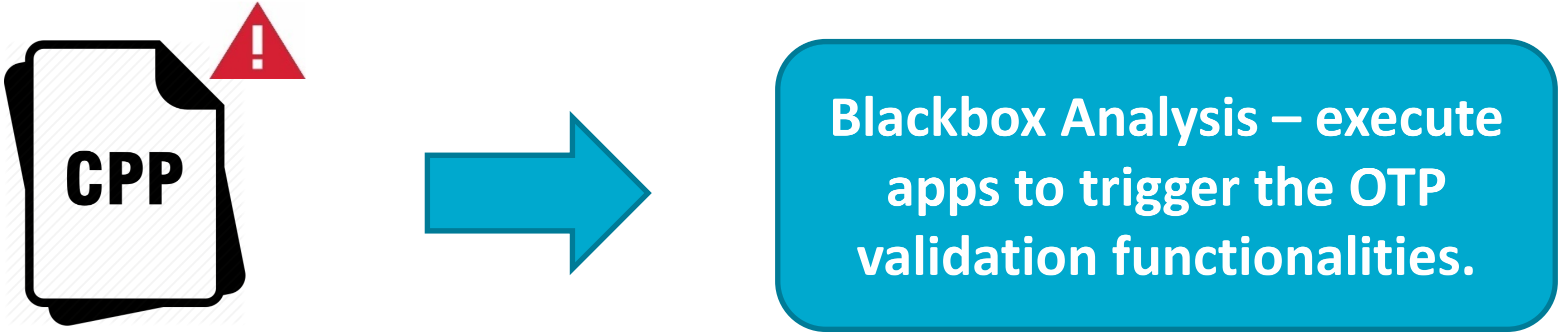
Rule Violation – Multiple

Rule Combination	Violation/Attacks
R1 + any other rules	Replay attacks
R2 + R3	Brute-force attacks
R4 + R5	Replay attacks
R2 + R3 + R6	Brute-force attacks

Outline

- Authentication in Android
- One-time password
- <u>SMS OTP Analyzer</u>
- Evaluation
- Conclusion

Design Challenge – SMS OTP Analyzer



Blackbox Analysis – execute apps to trigger the OTP validation functionalities.

Without source code

Design Challenge – SMS OTP Analyzer

Trigger OTP Validation System

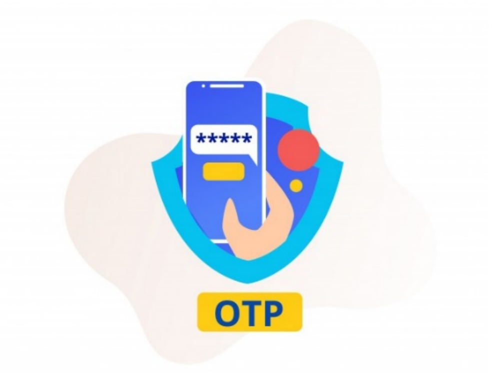
Semantic Analysis – use Login Activity declarations and function information.

Design Challenge – SMS OTP Analyzer

Perform login

Code Analysis – decompile the apk and collect widget information.

Design Challenge – SMS OTP Analyzer



Analyze SMS message

Text Analysis – Examine altered fields in each message

SMS OTP Analyzer – AUTH-EYE

Login Code Detector:

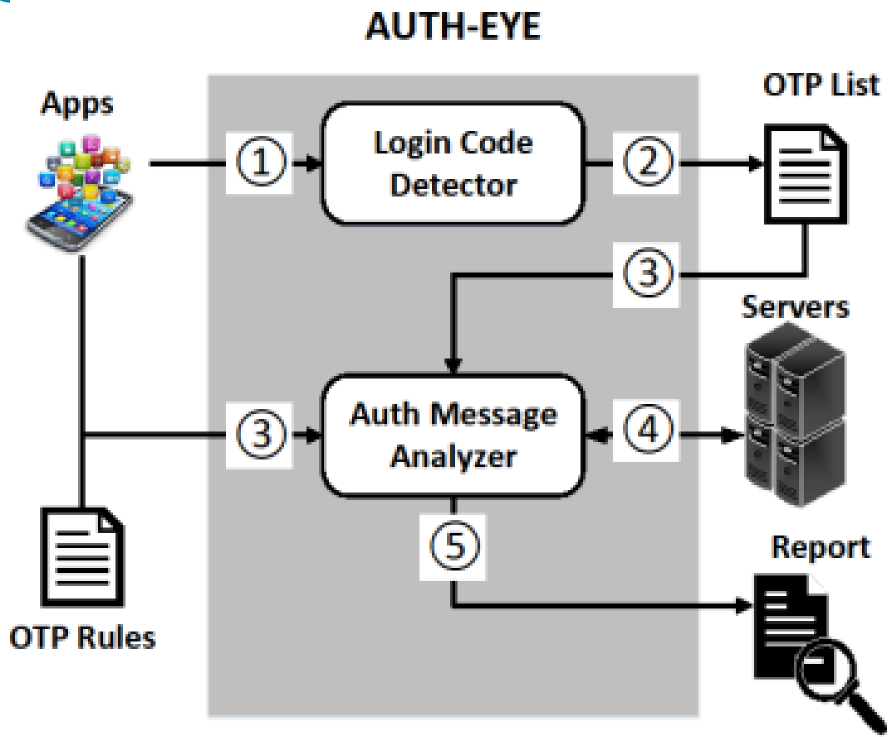
✓App Decompilation

✓Login Activity Locating

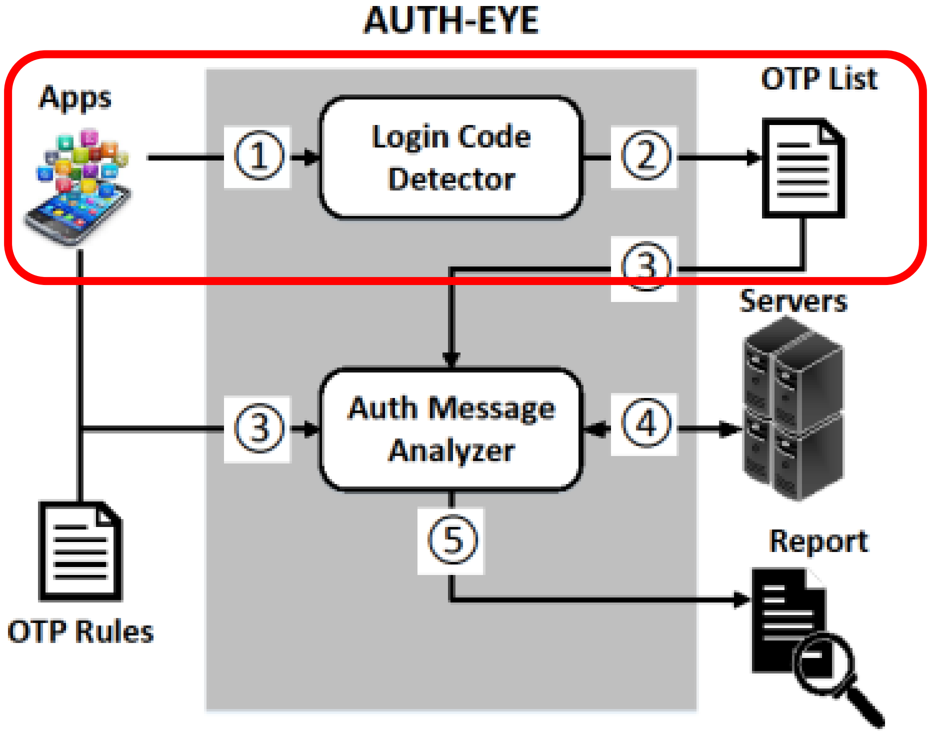
Auth Message Analyzer:

✓OTP Login Execution

✓Evaluating Rule Violations



SMS OTP Analyzer – AUTH-EYE



Login Code Detector:

✓App Decompilation

✓Login Activity Locating

Auth Message Analyzer:

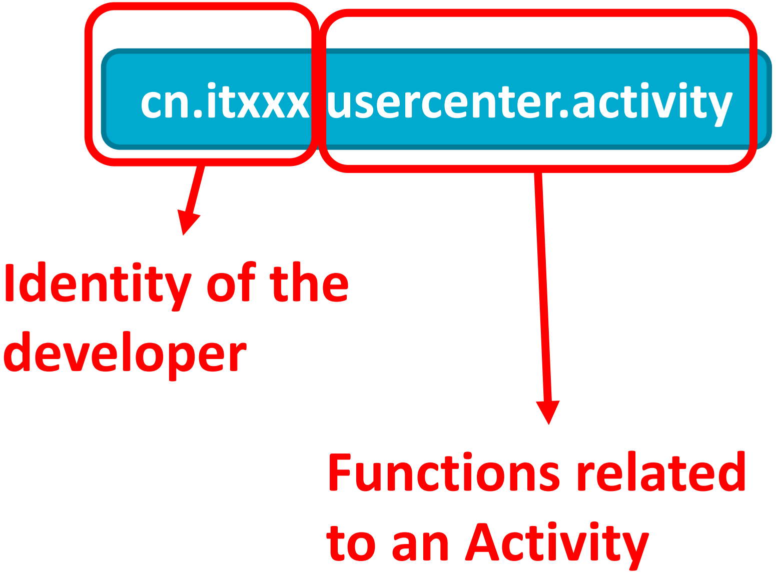
✓OTP Login Execution

✓Evaluating Rule Violations

CSIRO

AUTH-EYE: Login Code Detector

- App Decompilation: JEB Android Decompiler
- Login Activity Locating:
  - Customized package selection



cn.itxxx usercenter.activity

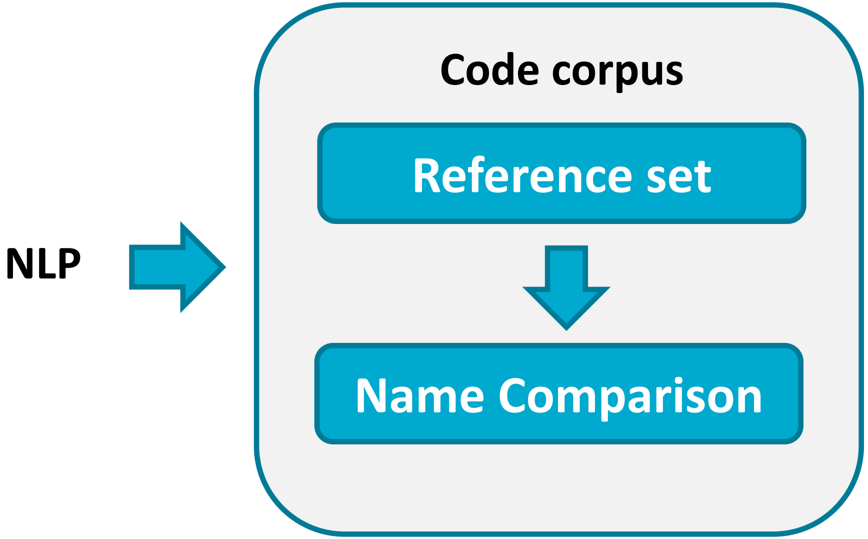
Identity of the developer

Functions related to an Activity

AUTH-EYE: Login Code Detector

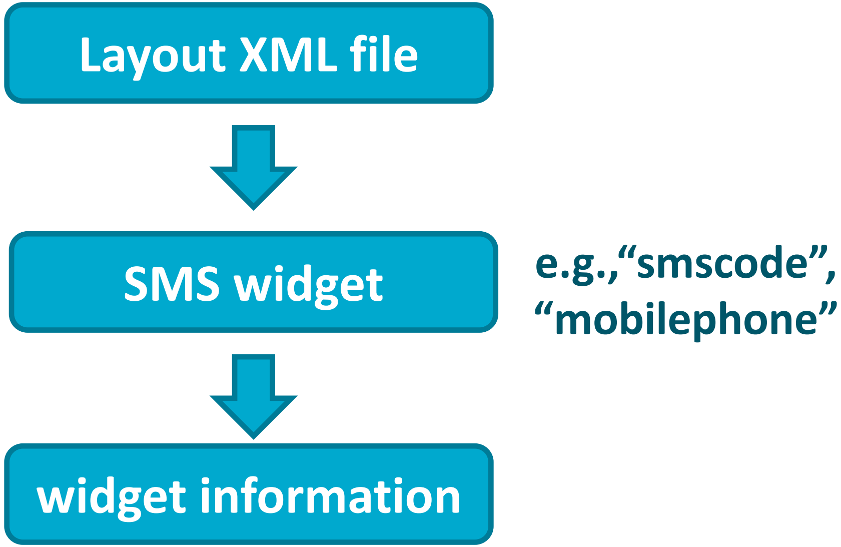
- App Decompilation: JEB Android Decompiler

- Login Activity Locating:
  - Customized package selection
  - Login Function Identification



AUTH-EYE: Login Code Detector

- App Decompilation: JEB Android Decompiler
- Login Activity Locating:
  - Customized package selection
  - Login Function Identification
  - SMS OTP Identification



Design

SMS OTP Analyzer – **AUTH-EYE**

Login Code Detector:

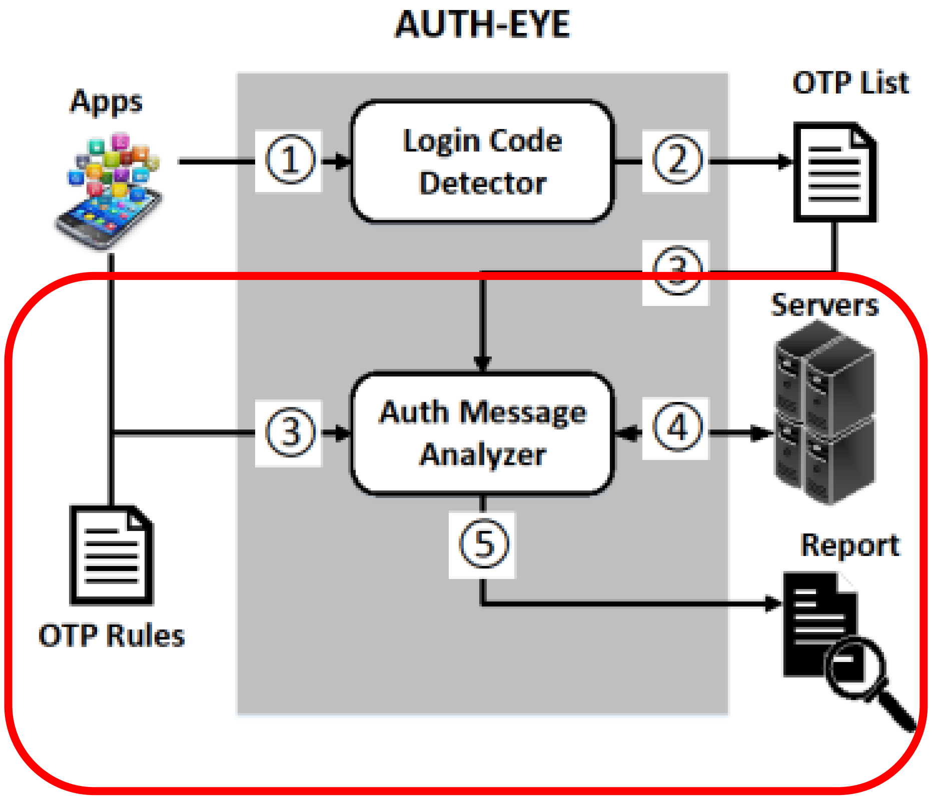
✓App Decompilation

✓Login Activity Locating

Auth Message Analyzer:

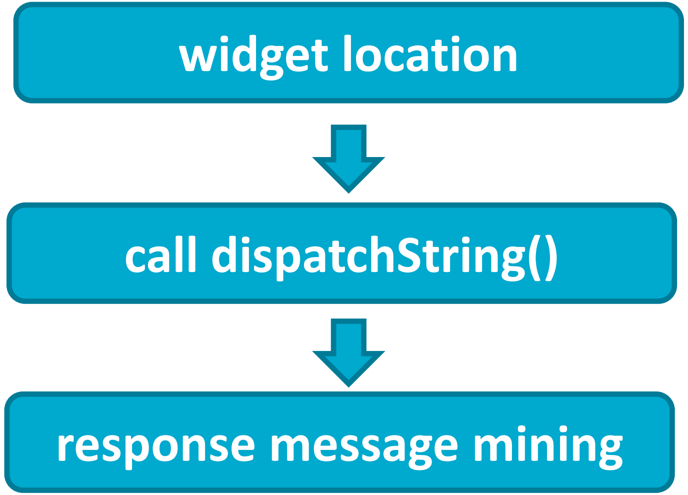
✓OTP Login Execution

✓Evaluating Rule Violations



AUTH-EYE: Auth Message Analyzer

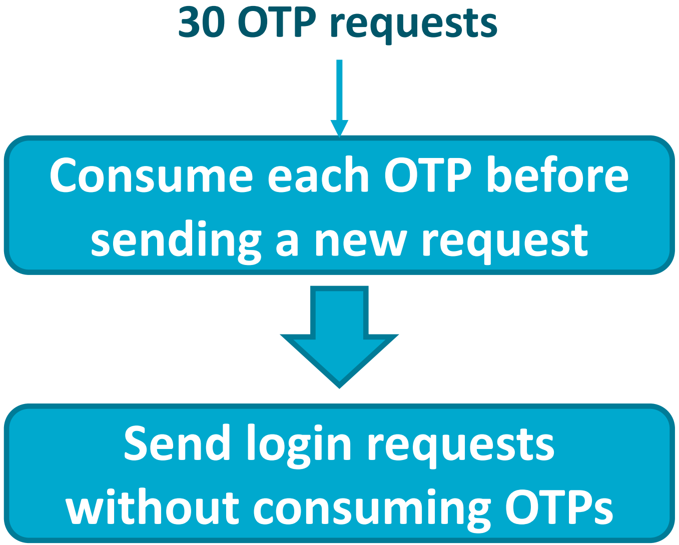
- OTP Login Execution:
  - Monkey tool – trigger SMS OTP login Activities.
  - Response Message Analysis



AUTH-EYE: Auth Message Analyzer

- OTP Login Execution

- Evaluating Rule Violations
  - R1: OTP Randomness



30 OTP requests

Consume each OTP before sending a new request

Send login requests without consuming OTPs

AUTH-EYE: Auth Message Analyzer

- OTP Login Execution

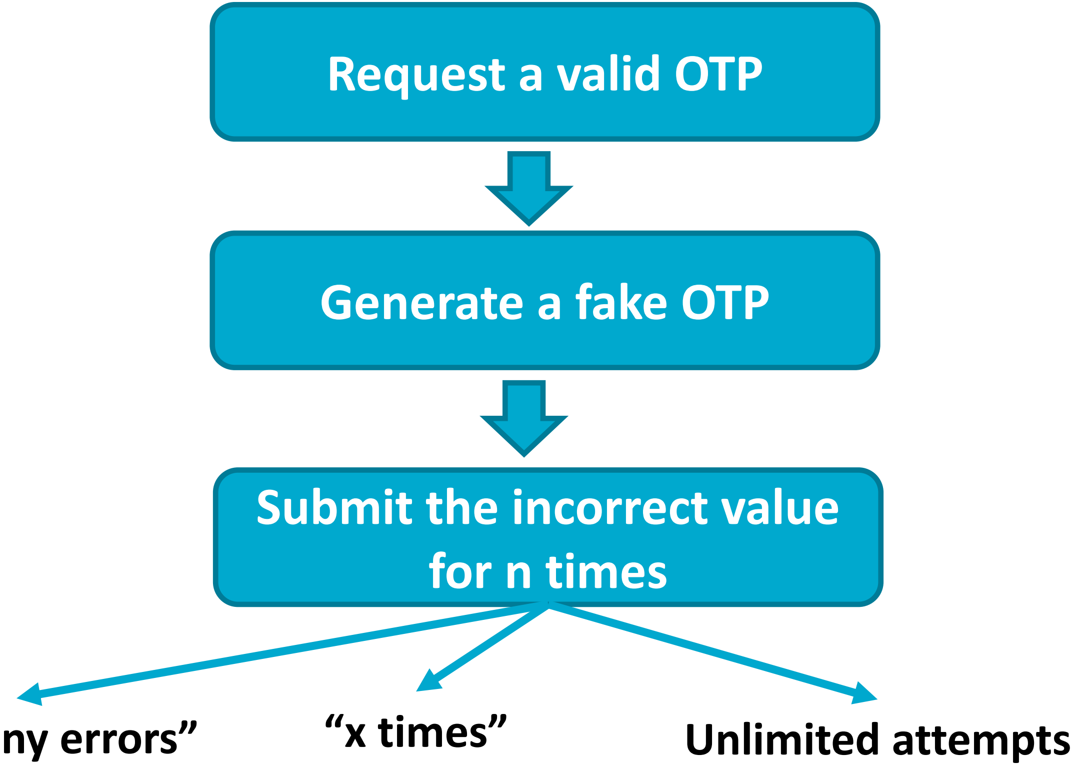
- Evaluating Rule Violations
  - R1: OTP Randomness
  - R2: OTP Length

Check the length of each OTP

AUTH-EYE: Auth Message Analyzer

- OTP Login Execution:

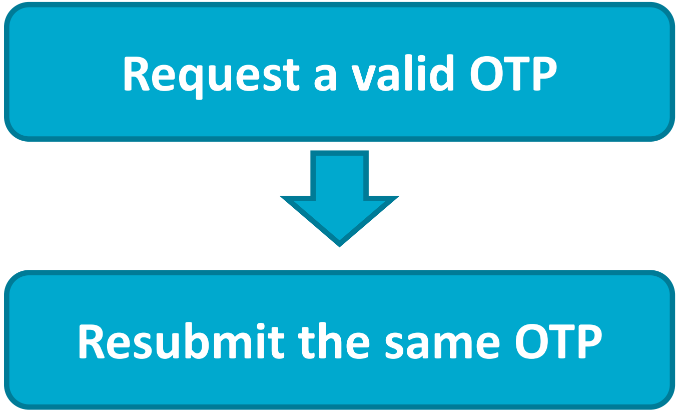
- Evaluating Rule Violations
  - R1: OTP Randomness
  - R2: OTP Length
  - R3: Retry Attempts



AUTH-EYE: Auth Message Analyzer

- OTP Login Execution:

- Evaluating Rule Violations
  - R1: OTP Randomness
  - R2: OTP Length
  - R3: Retry Attempts
  - R4: OTP Consumption

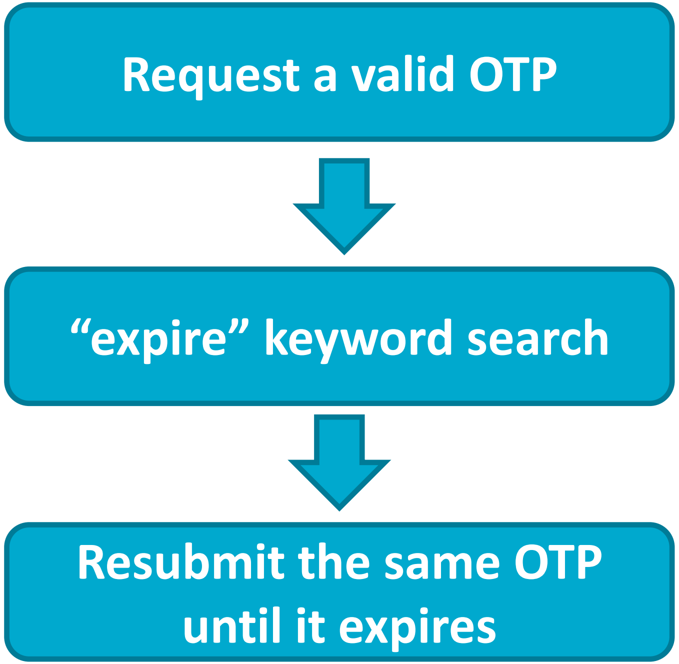

Request a valid OTP

Resubmit the same OTP

AUTH-EYE: Auth Message Analyzer

- OTP Login Execution:

- Evaluating Rule Violations
  - R1: OTP Randomness
  - R2: OTP Length
  - R3: Retry Attempts
  - R4: OTP Consumption
  - R5: OTP Expiration



Request a valid OTP

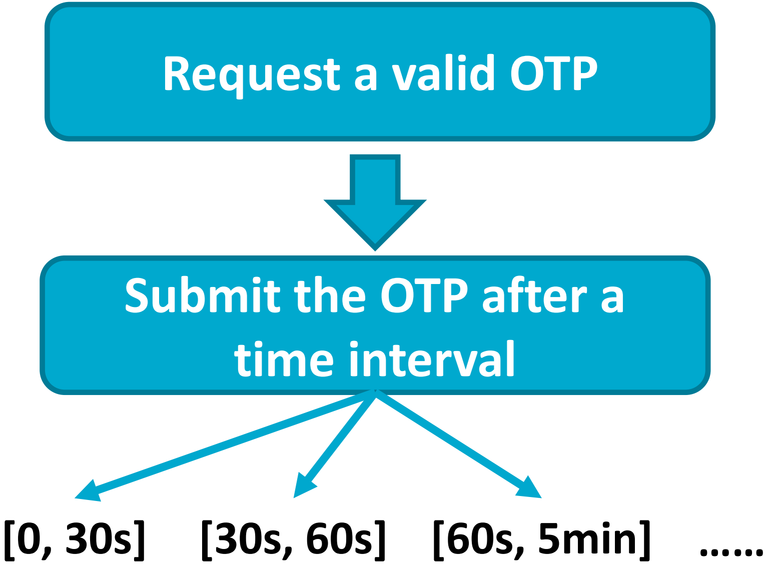
“expire” keyword search

Resubmit the same OTP until it expires

AUTH-EYE: Auth Message Analyzer

- OTP Login Execution:

- Evaluating Rule Violations
  - R1: OTP Randomness
  - R2: OTP Length
  - R3: Retry Attempts
  - R4: OTP Consumption
  - R5: OTP Expiration
  - R6 OTP Renewal Interval



Outline

- Authentication in Android
- One-time password
- SMS OTP Analyzer
- Evaluation
- Conclusion

Evaluation

- Dataset
  - From: GooglePlay Store and Tencent App Store
  - Total: 3,303 apps
  - Categories: 21 – Beauty, Books & Reference, Communication, Education, Entertainment, Finance, Health & Fitness, Lifestyle, Map & Navigation, Medical, Music & Audio, News & Magazine, Parenting, Personalization, Photography, Productivity, Shopping, Social, Tool, Travel & Local, Video Player & Editors.
  - Successfully analyzed **1,364** apps (648 failed to be decompiled, 1,298 crashed during SMS OTP analysis).

Results – OTP Login Activity Identify

- AUTH-EYE identified 1,069 (out of 1,364) apps with login activities, we manually inspected the apps and found **934** implemented login activities.

- **544** apps used OTP authentication
- 354 (out of 544) apps use two-factor authentication

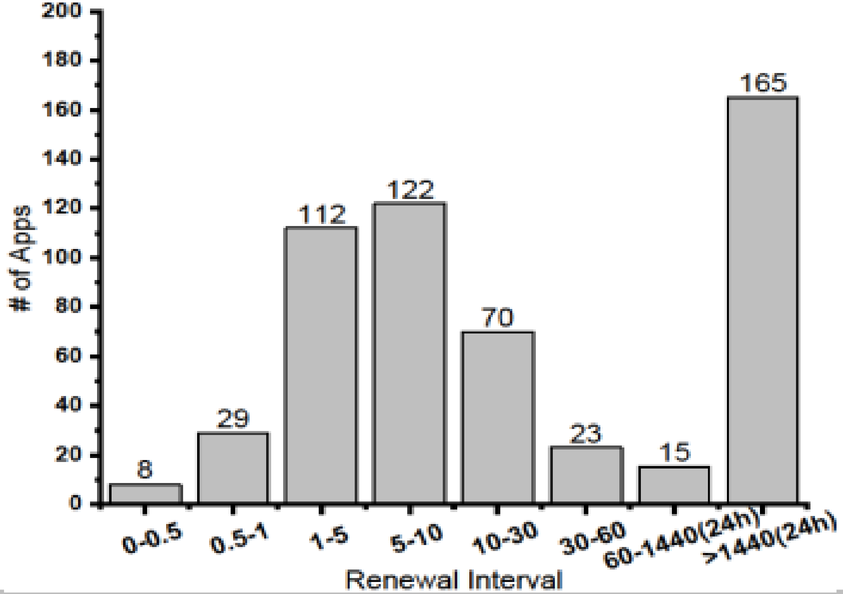
Login Activity Names	# of apps
Login	105
LoginSuccess	53
doLogin	37
smsLogin	18
onLogin	16
requestLogin	14
startLogin	14

Results – OTP Rules Violations

Rules	# of apps
R6: OTP Renewal Interval	536
R3: Retry Attempts	324
R2: OTP Length	209
R4: OTP Consumption	106
R1: OTP Randomness	71
R5: OTP Expiration	41

Results – R6 : OTP Renewal Interval

- Only 8 apps follow this requirement.
- 165 apps do not renew their OTP values.

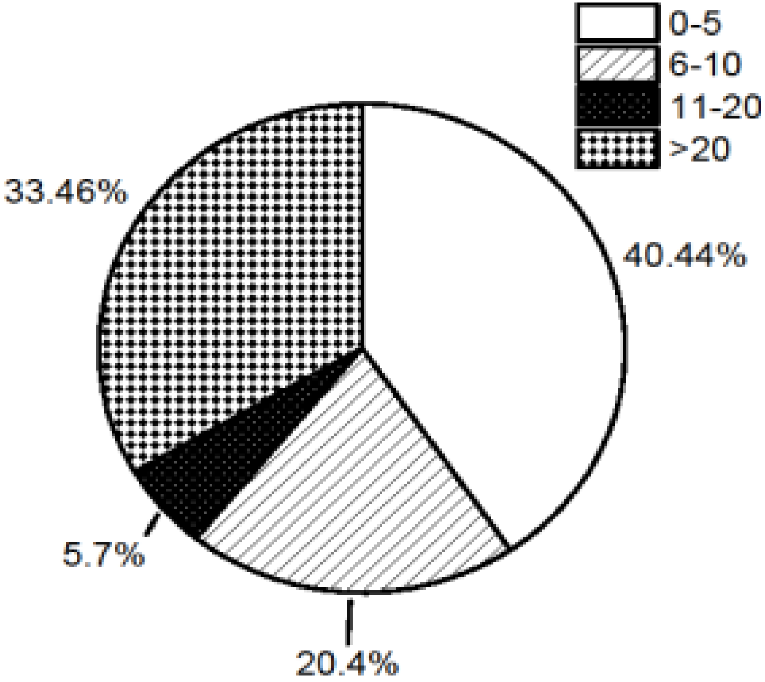


Results – R3: Retry Attempts

- Only 220 (40.44%) apps have OTP validation complying with the rule.

- AUTH-EYE was set to send a fake OTP at most 20 times. It identified that 126 apps still work after 20 times of retry.

- 97 apps have the delay protection for OTP validation.



Results – R2: OTP Length

- 209 apps use OTP values with the length < 6

- Although the OTP length could be set at 10 digits, all validation systems generate OTPs with at most 6 digits.

Results – R4: OTP Consumption

- Apps violated this rule are only from 8 categories: Shopping, Video Player & Editor, Books & Reference, Music & Audio, Travel & Local, Entertainment & Productivity.

- 37.7% and 18.9% vulnerable apps are from Books & Reference and Video Players & Editor, respectively.

Results – R1: OTP Randomness

- Two types of errors are identified: repeated values and static values.

- Repeated values: 56 apps generate repeated OTP values
  - 21 apps generate a sequence of unique values and then repeat the same sequence.
  - 35 apps repeat the same OTP values for n times (n = 2 or 3).
- Static Values: 15 apps use static OTP values.

Results – R5: OTP Expiration

- 33 apps reject the OTP value if it is expired.

- 40 apps accept expired OTP values.

- 471 apps do not have any expiration set for OTP values

Results – Multiple Rules Violation

# of apps	Multiple-rules violated
65	R2 (OTP Length) & R4 (OTP Consumption)
13	R1 (OTP Randomness) & (R2 or R3 (Retry Attempts))
9	R4 (OTP Consumption) & R5 (OTP Expiration)
2	R2 & R3

Outline

- Authentication in Android
- One-time password
- SMS OTP Analyzer
- Evaluation
- Conclusion

Conclusion

- We listed 6 OTP rules based on RFC documents.
- We designed AUTH-EYE to check for violations of OTP rules.
- An empirical study is conducted, and most Android apps are found with incorrect OTP implementations.
- The validation systems of apps in security-critical domains, such as Finance, Shopping, and Social are not secure.

Thank You

Q & A