CryptoShield – Automatic On-Device Mitigation for Crypto API Misuse in Android Applications

GRAZ UNIVERSITY OF TECHNOLOGY

SECURE INFORMATION TECHNOLOGY AUSTRIA

ACM AsiaCCS 2023

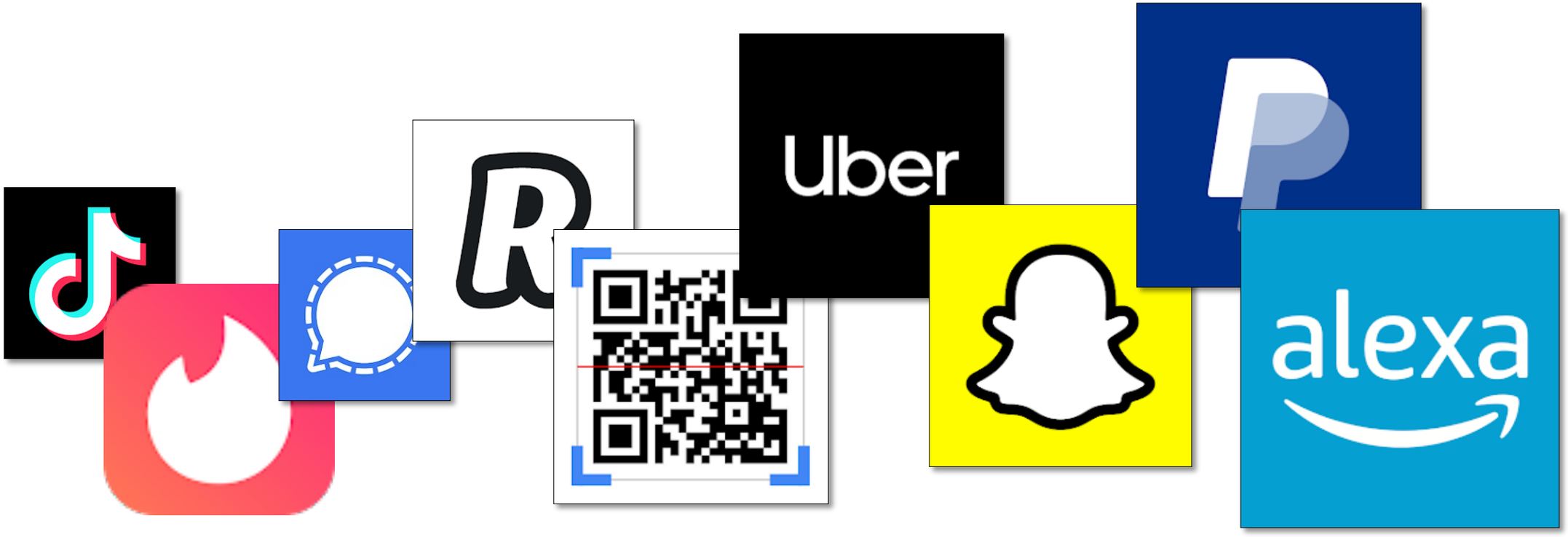
Florian Draschbacher
Graz University of Technology, Graz, Austria
Secure Information Technology Austria, Vienna, Austria
florian.draschbacher@iaik.tugraz.at

Johannes Feichtner
Dynatrace Austria GmbH, Linz, Austria
johannes.feichtner@dynatrace.com

July 14th, 2023

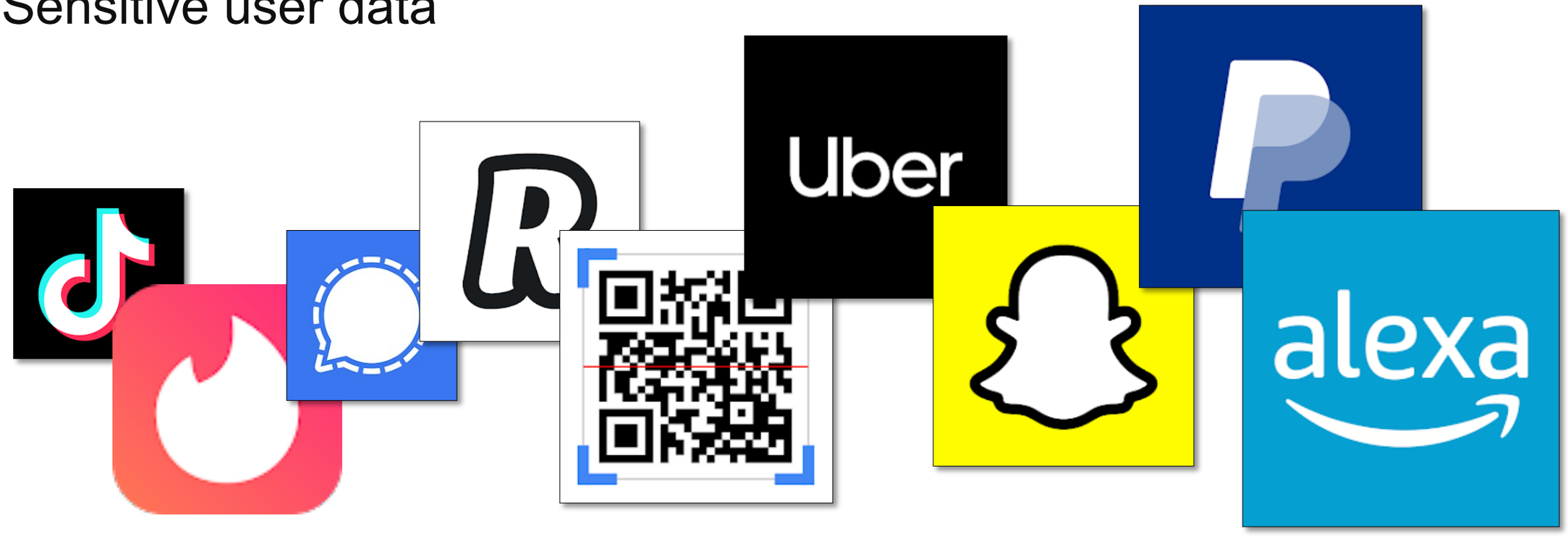
Mobile App Security

- New mobile computing use cases



Mobile App Security

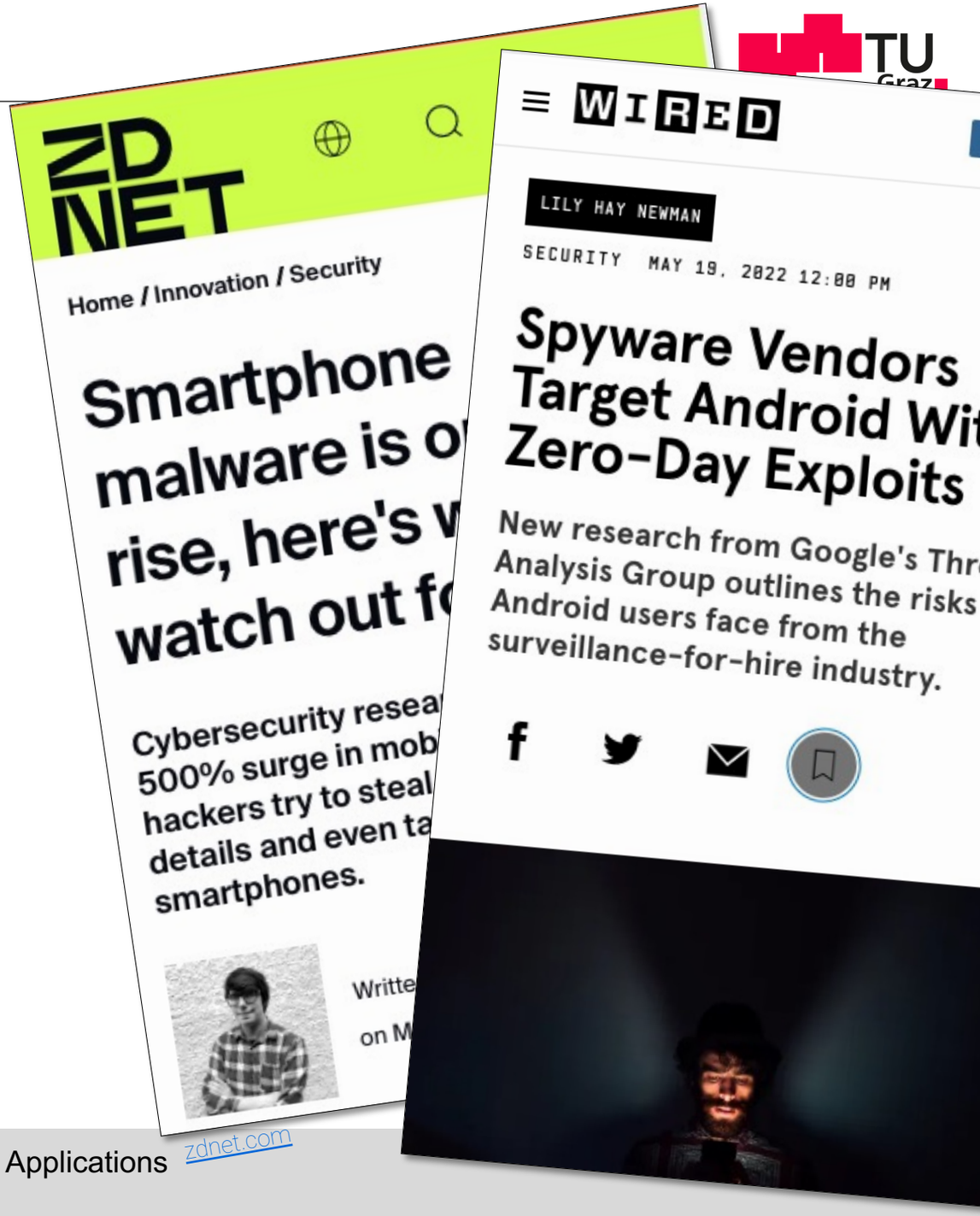
- New mobile computing use cases
  - Sensitive user data



Mobile App Security

- New mobile computing use cases
  - Sensitive user data

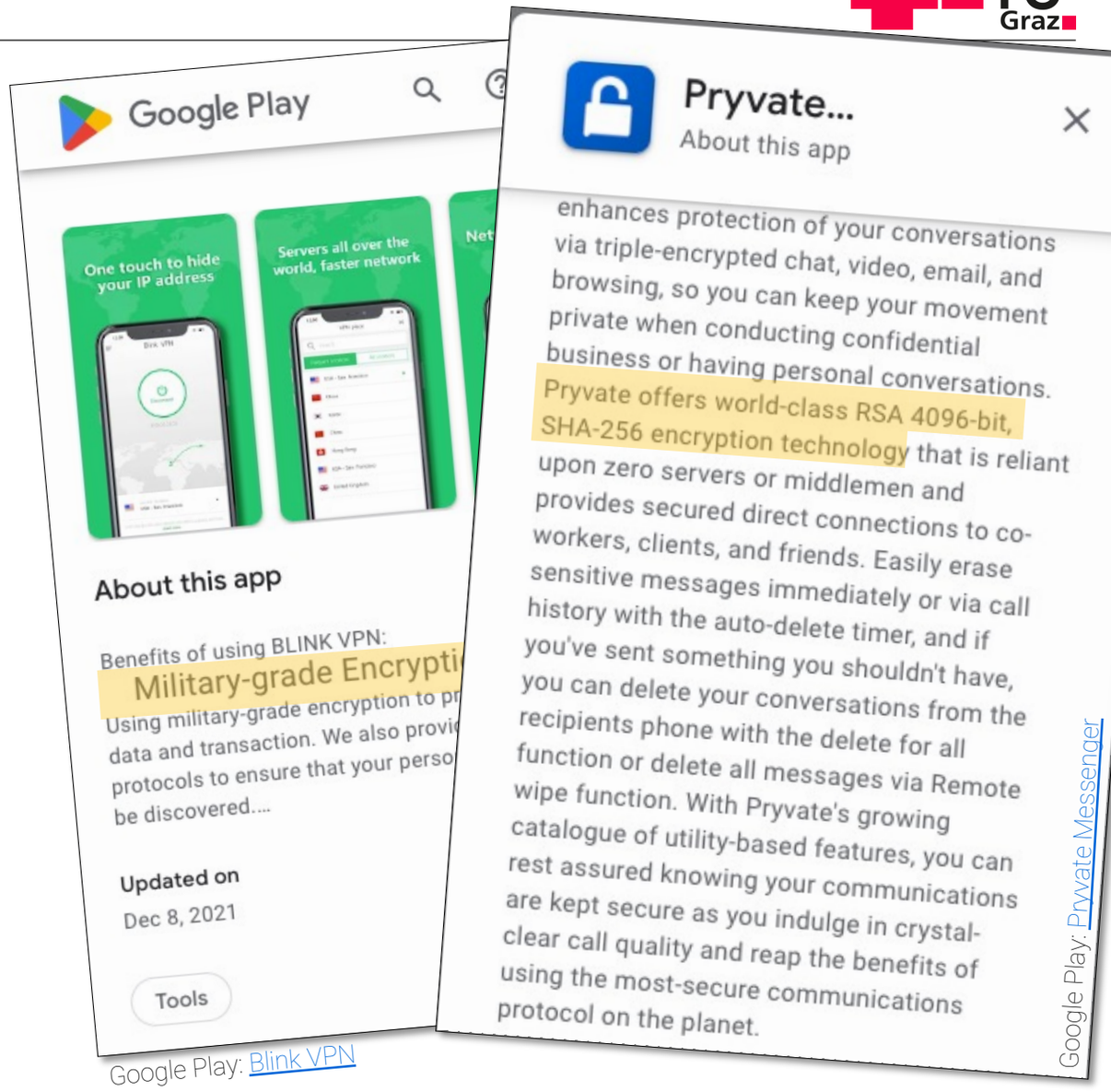
- Attractive for attackers



zdnet.com

Mobile App Security

- New mobile computing use cases
  - Sensitive user data
- Attractive for attackers
- Proper data protection?
  - Users rely on developers



Google Play: Blink VPN

Google Play: Pryvate Messenger

Motivation

Relying on App Developers…

- Mistakes in validating TLS certificates
  - 37% of apps in 2021 [**OHA+21**]
- Crypto API misuse in general
  - 91% of apps in 2019 [**RXA+19**]
- Many developers fail to fix these issues
  - Same misuse reintroduced again and again [**GKL+19**]

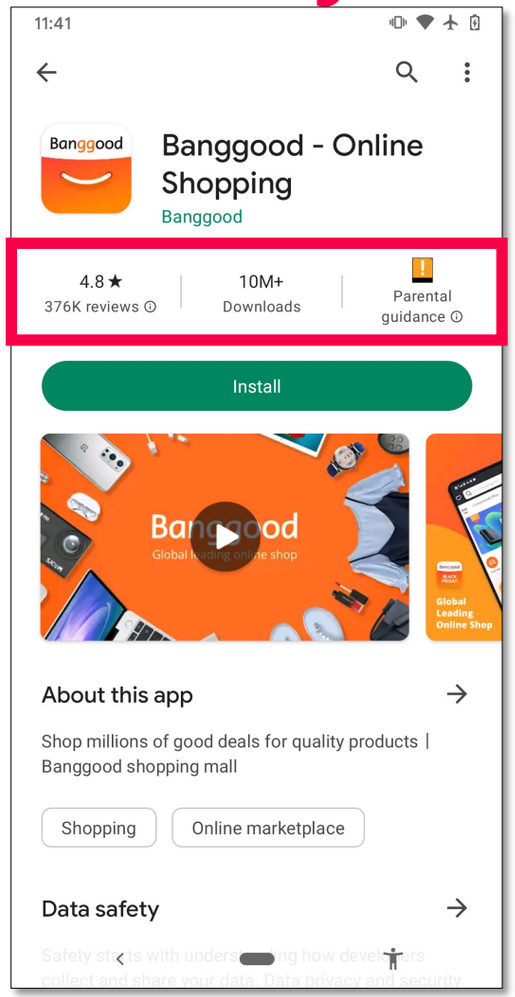
Existing Mitigations

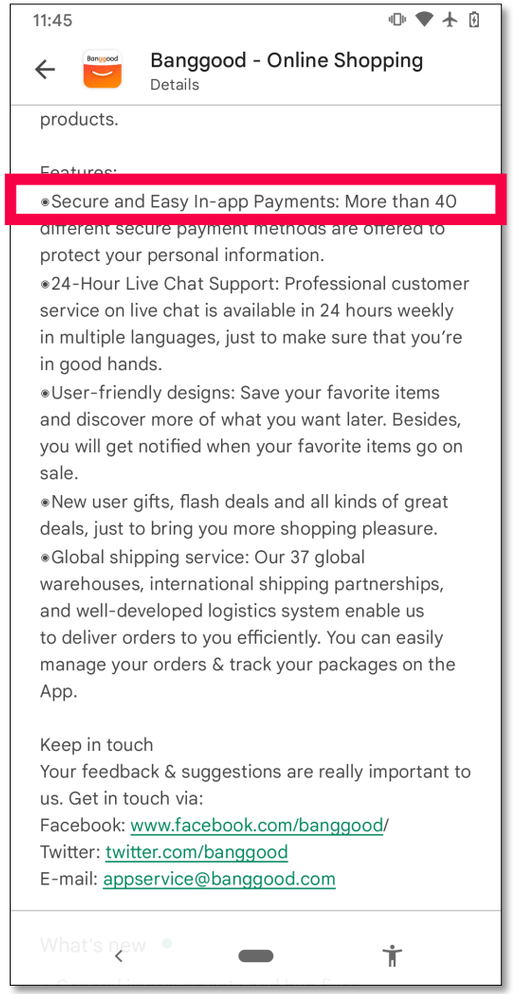
- Google improved tools for **developers**

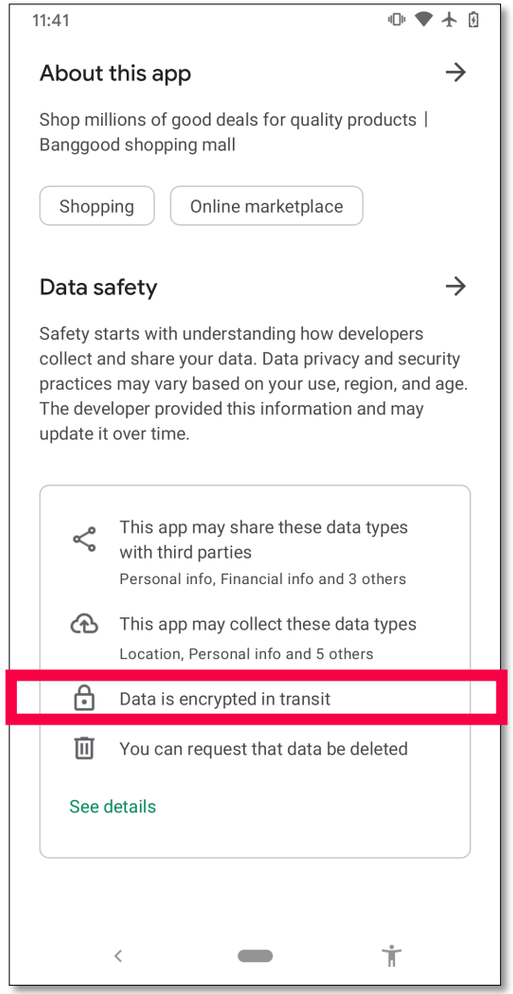
- For **end users**, the academic research community proposed
  - Using static analysis to apply fix patterns [**MLT+16**]
  - Using root access to dynamically mitigate TLS misuse [**BHM+16**]

Issue remains **highly prevalent** and **no practical mitigation** in sight

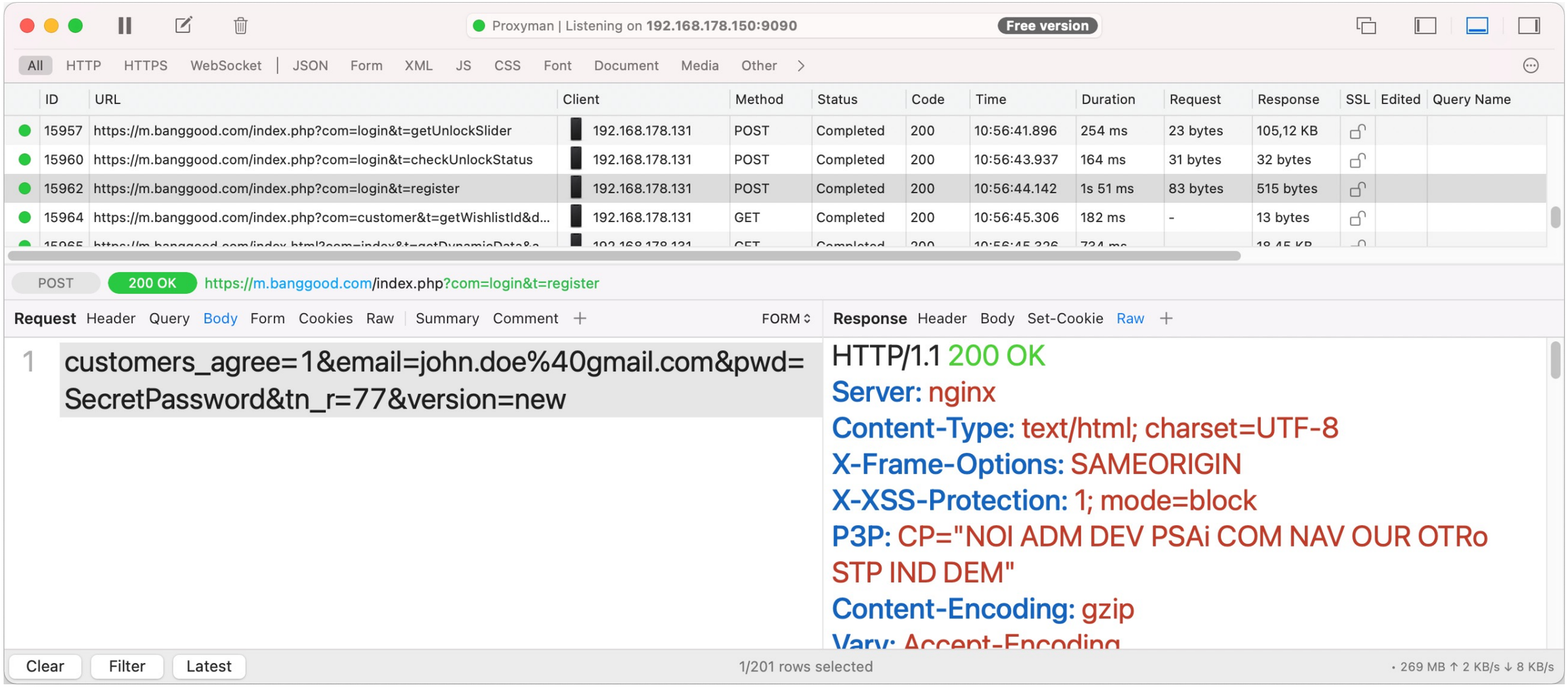
Case Study


11:41
Banggood - Online Shopping
Banggood
4.8★
376K reviews
10M+
Downloads
Parental guidance
Install
About this app
Shop millions of good deals for quality products | Banggood shopping mall
Shopping
Online marketplace
Data safety


11:45
Banggood - Online Shopping
Details
products.
Features:
•Secure and Easy In-app Payments: More than 40 different secure payment methods are offered to protect your personal information.
•24-Hour Live Chat Support: Professional customer service on live chat is available in 24 hours weekly in multiple languages, just to make sure that you're in good hands.
•User-friendly designs: Save your favorite items and discover more of what you want later. Besides, you will get notified when your favorite items go on sale.
•New user gifts, flash deals and all kinds of great deals, just to bring you more shopping pleasure.
•Global shipping service: Our 37 global warehouses, international shipping partnerships, and well-developed logistics system enable us to deliver orders to you efficiently. You can easily manage your orders & track your packages on the App.
Keep in touch
Your feedback & suggestions are really important to us. Get in touch via:
Facebook: www.facebook.com/banggood/
Twitter: twitter.com/banggood
E-mail: appservice@banggood.com
What's new


11:41
About this app
Shop millions of good deals for quality products | Banggood shopping mall
Shopping
Online marketplace
Data safety
Safety starts with understanding how developers collect and share your data. Data privacy and security practices may vary based on your use, region, and age. The developer provided this information and may update it over time.
This app may share these data types with third parties
Personal info, Financial info and 3 others
This app may collect these data types
Location, Personal info and 5 others
Data is encrypted in transit
You can request that data be deleted
See details

Case Study

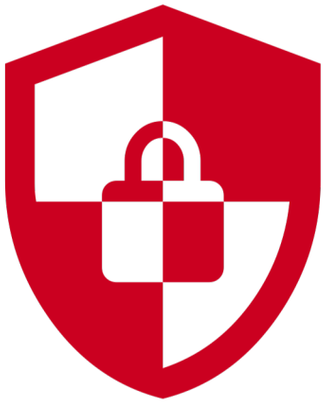

Proxyman | Listening on 192.168.178.150:9090
Free version
All HTTP HTTPS WebSocket JSON Form XML JS CSS Font Document Media Other
ID URL Client Method Status Code Time Duration Request Response SSL Edited Query Name
15957 https://m.banggood.com/index.php?com=login&t=getUnlockSlider 192.168.178.131 POST Completed 200 10:56:41.896 254 ms 23 bytes 105,12 KB
15960 https://m.banggood.com/index.php?com=login&t=checkUnlockStatus 192.168.178.131 POST Completed 200 10:56:43.937 164 ms 31 bytes 32 bytes
15962 https://m.banggood.com/index.php?com=login&t=register 192.168.178.131 POST Completed 200 10:56:44.142 1s 51 ms 83 bytes 515 bytes
15964 https://m.banggood.com/index.php?com=customer&t=getWishlistId&d... 192.168.178.131 GET Completed 200 10:56:45.306 182 ms - 13 bytes
POST 200 OK https://m.banggood.com/index.php?com=login&t=register
Request Header Query Body Form Cookies Raw Summary Comment FORM
1 customers_agree=1&email=john.doe%40gmail.com&pwd=SecretPassword&tn_r=77&version=new
Response Header Body Set-Cookie Raw
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Content-Encoding: gzip
Vary: Accept-Encoding
Clear Filter Latest
1/201 rows selected
269 MB ↑ 2 KB/s ↓ 8 KB/s

Problem Statement & Approach

CryptoShield

Our Goal: Put users in control

- **Practicality**
  Integrate into real-world environments
- **User-Centricity**
  Remove dependency on app developers
- **Compatibility**
  Support broad range of apps



Crypto Rules

Cover most **critical** crypto misuse cases **that can be mitigated**

12 Cases from [**PGC+21**] and [**RXA+19**]

- Easy to exploit
- High gain for attacker

Remove **2 Cases**

- Hardcoded keys
- Insecure hash algorithms

➢ **10 critical misuse cases** defined as **violations of rules**

Crypto Rules

R01: Don't use ***unprotected*** **HTTP** connections

R02: Don't verify **TLS** connections in ***insecure*** ways

R03: Don't use ***predictable*** **passwords** for **key stores**

R04: Don't use ***predictable*** **passwords** for **key derivations**

R05: Don't use ***ECB*** mode for **symmetric ciphers**

R06: Don't use ***predictable*** **IVs** for **symmetric ciphers**

R07: Don't ***reuse*** **IVs** for **symmetric ciphers**

R08: Don't use ***predictable*** **salt** values for **key derivations**

R09: Don't ***reuse*** **salt** values for **key derivations**

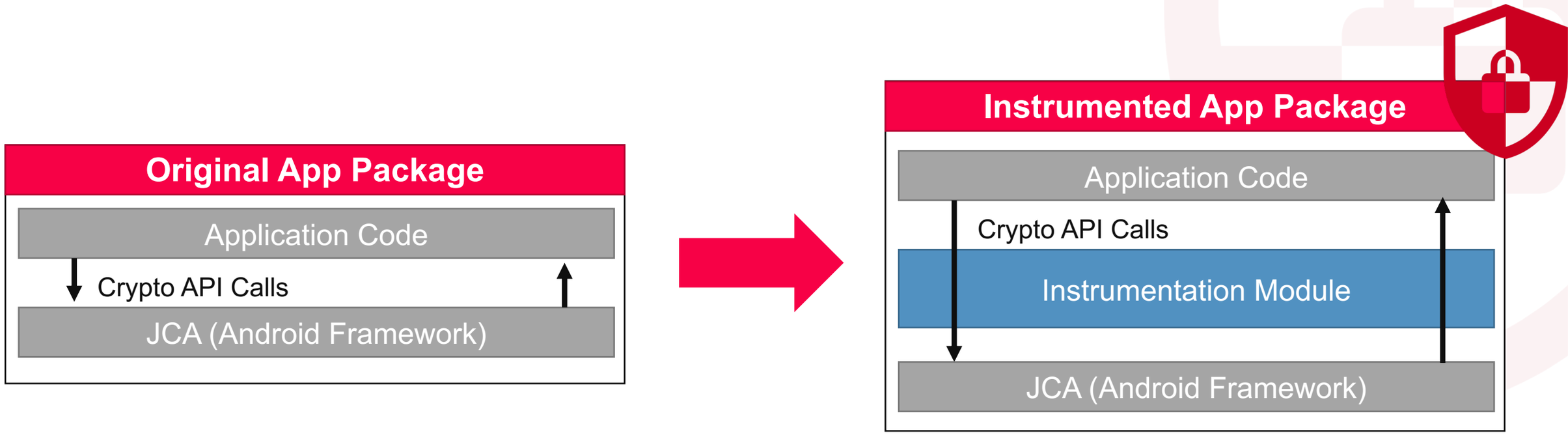
R10: Don't use ***predictable*** **CSRNG** seeds

Approach

1. Define **mitigation** for 10 most critical crypto misuse cases

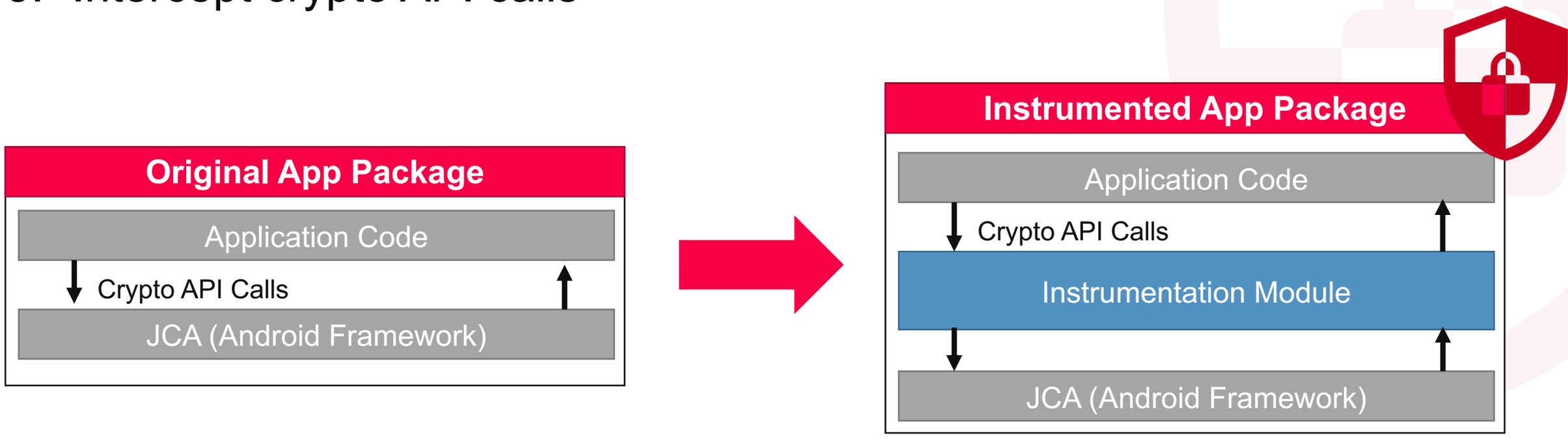
Approach

1. Define **mitigation** for 10 most critical crypto misuse cases
2. Inject **instrumentation** module



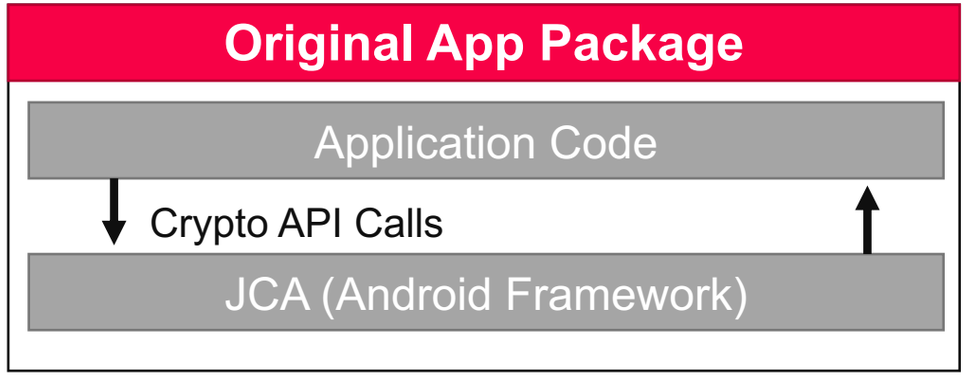
Approach

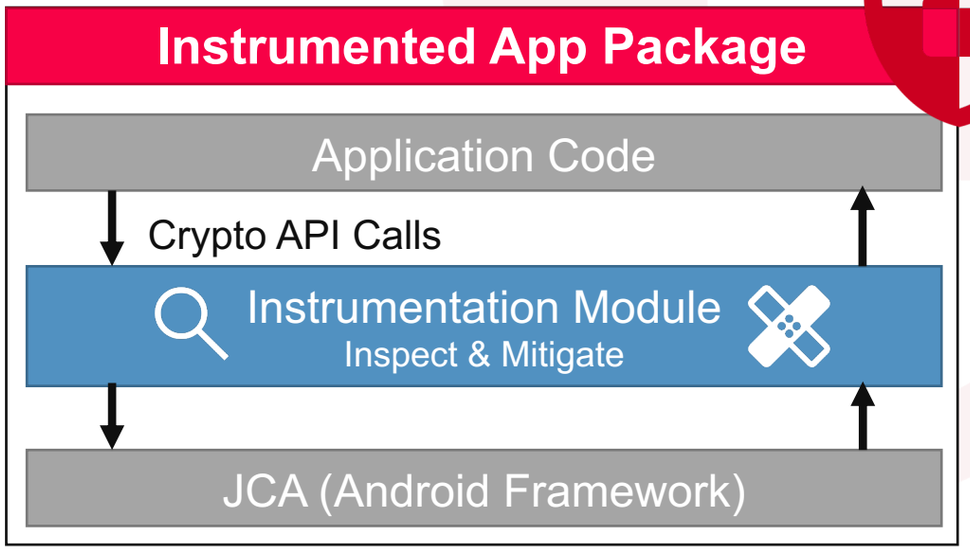
1. Define **mitigation** for 10 most critical crypto misuse cases
2. Inject **instrumentation** module
3. Intercept crypto API calls



Approach

1. Define **mitigation** for 10 most critical crypto misuse cases
2. Inject **instrumentation** module
3. Intercept crypto API calls
4. Inspect arguments, employ mitigations





Mitigation Procedures

Example Misuse Case

Implicit ECB Mode for AES

```
byte[] encrypt(byte[] pt, SecretKeySpec k){
 Cipher c = Cipher.getInstance("AES");
 c.init(ENCRYPT_MODE, k);
 return c.doFinal(pt);
}
```

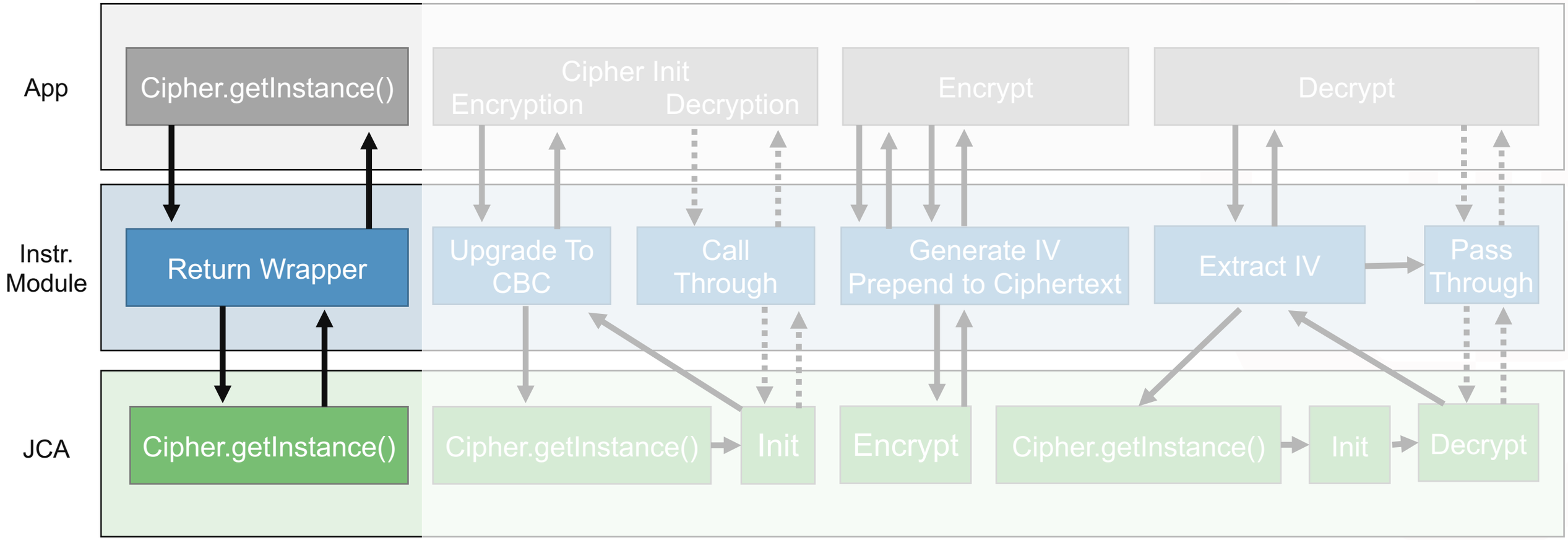
Encryption

Decryption

```
byte[] decrypt(byte[] ct, SecretKeySpec k){
  Cipher c = Cipher.getInstance("AES");
  c.init(DECRYPT_MODE, k);
  return c.doFinal(ct);
}
```

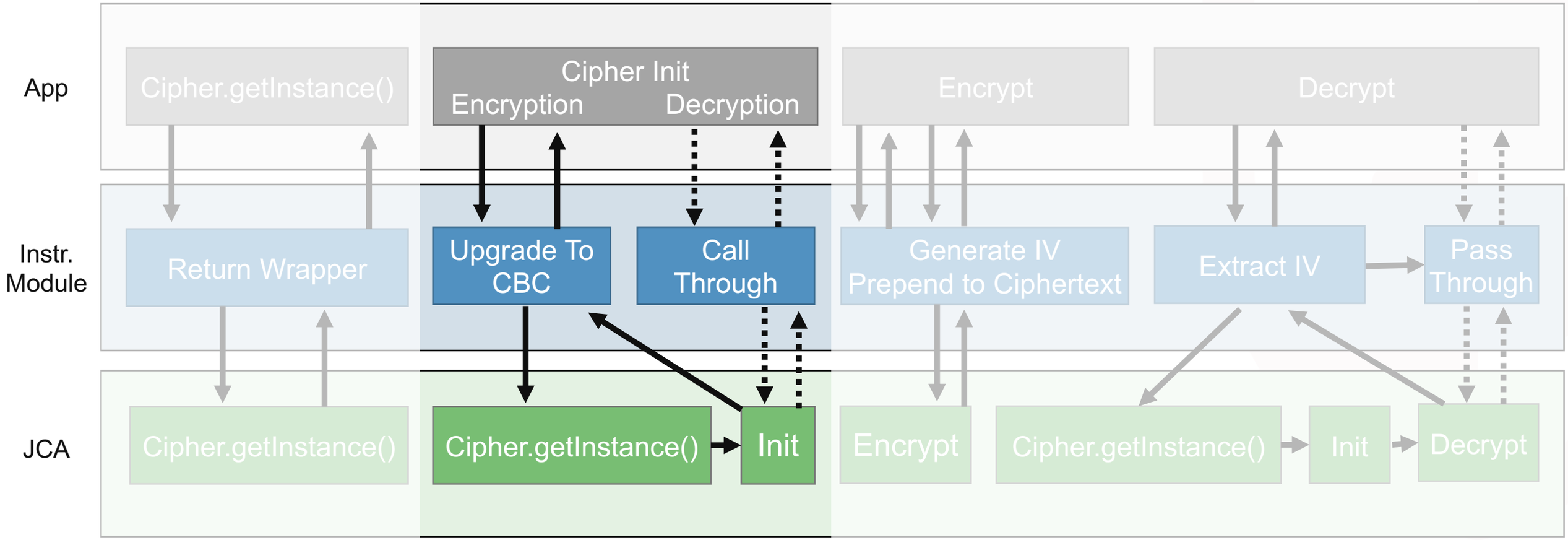
Example Mitigation

Misuse Case: Implicit ECB Mode for AES



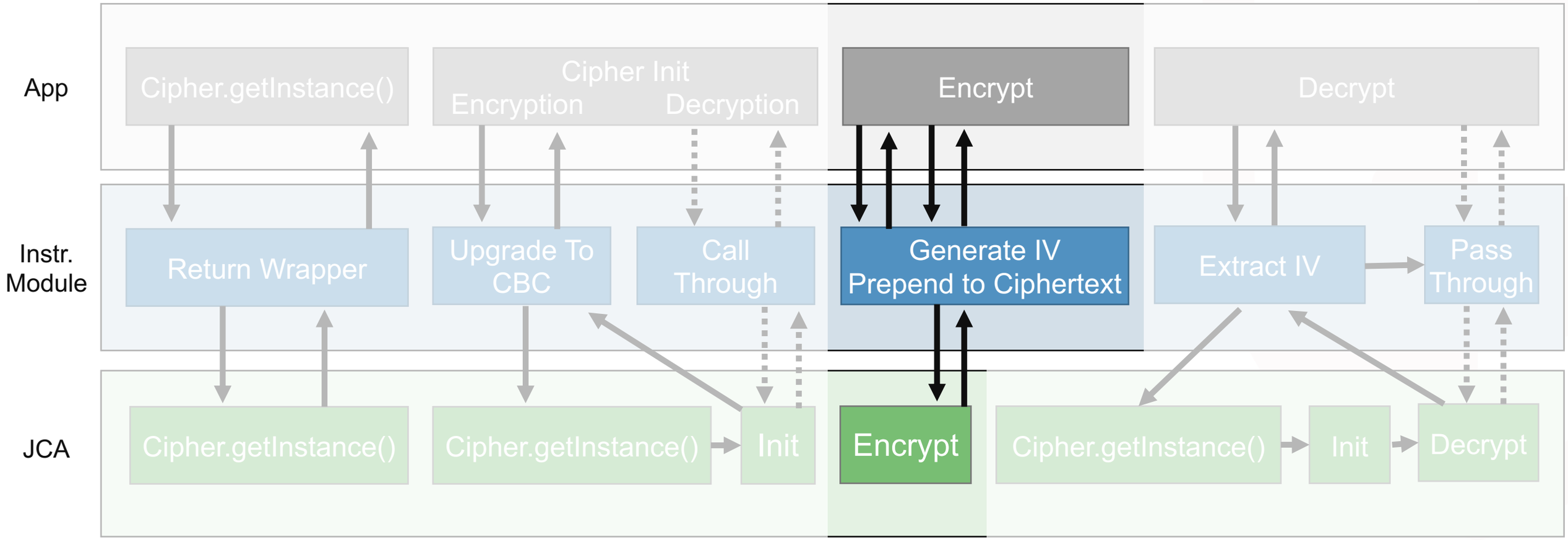
Example Mitigation

Misuse Case: Implicit ECB Mode for AES



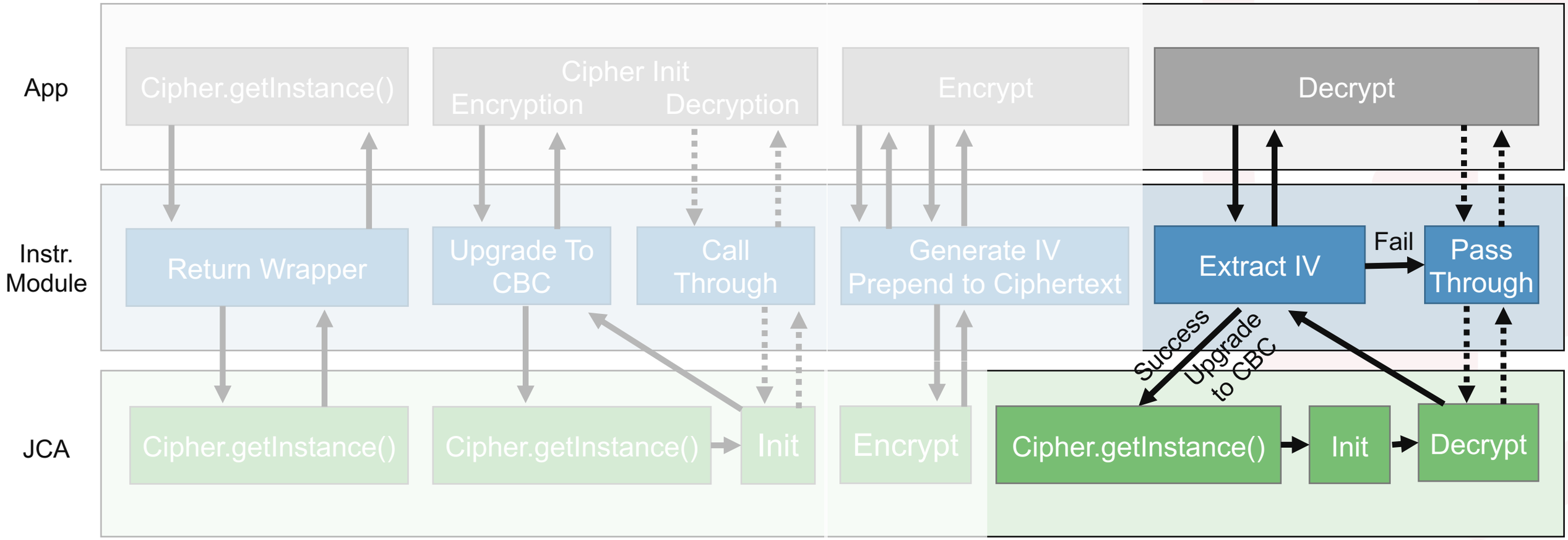
Example Mitigation

Misuse Case: Implicit ECB Mode for AES



Example Mitigation

Misuse Case: Implicit ECB Mode for AES



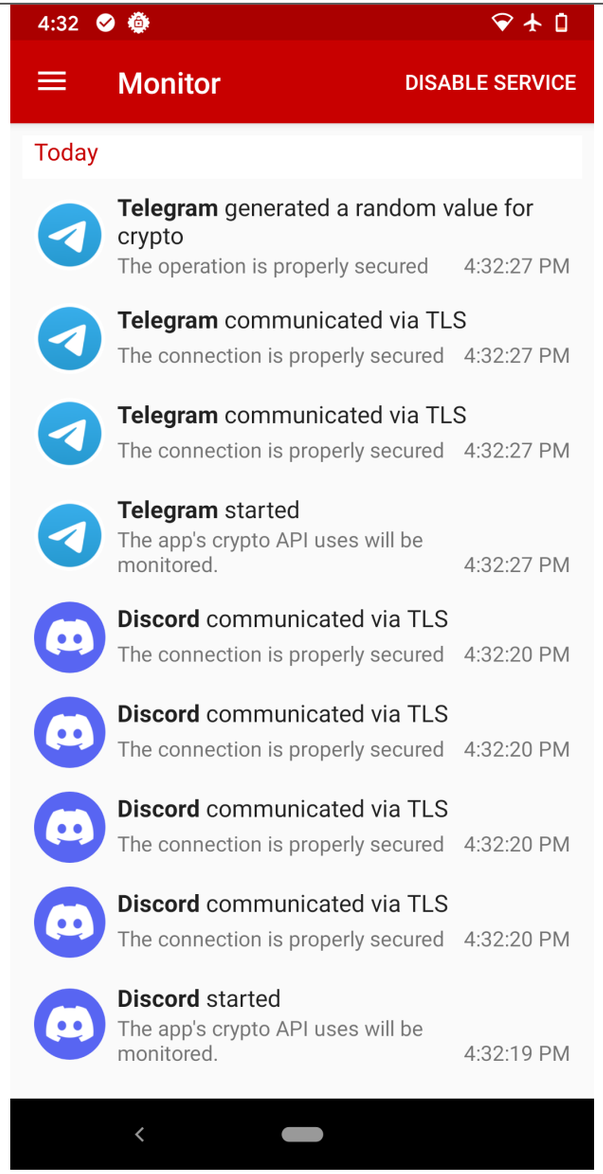
Implementation

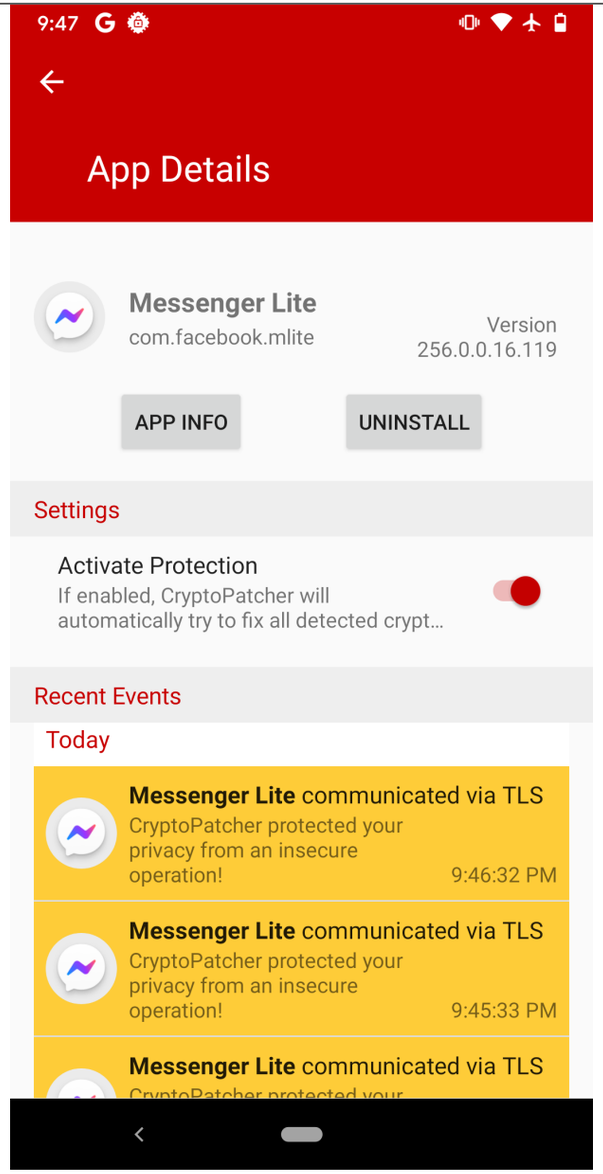
Implementation

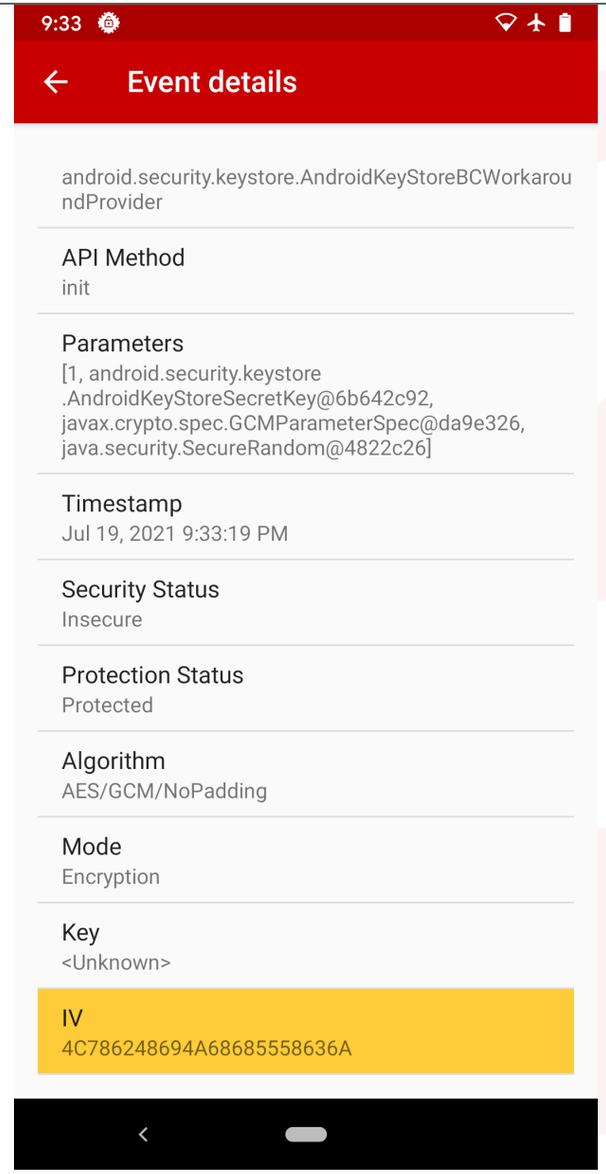
- Itself an Android application
- Instruments **all apps** installed on device
- Uses **Device Admin API** [1]
  - Unrooted operation, MDM
- Original app is only **disabled**, kept on device
  - Updates through Google Play

[1]: Android Developers: Device administration overview. https://developer.android.com/guide/topics/admin/device-admin

Screenshots





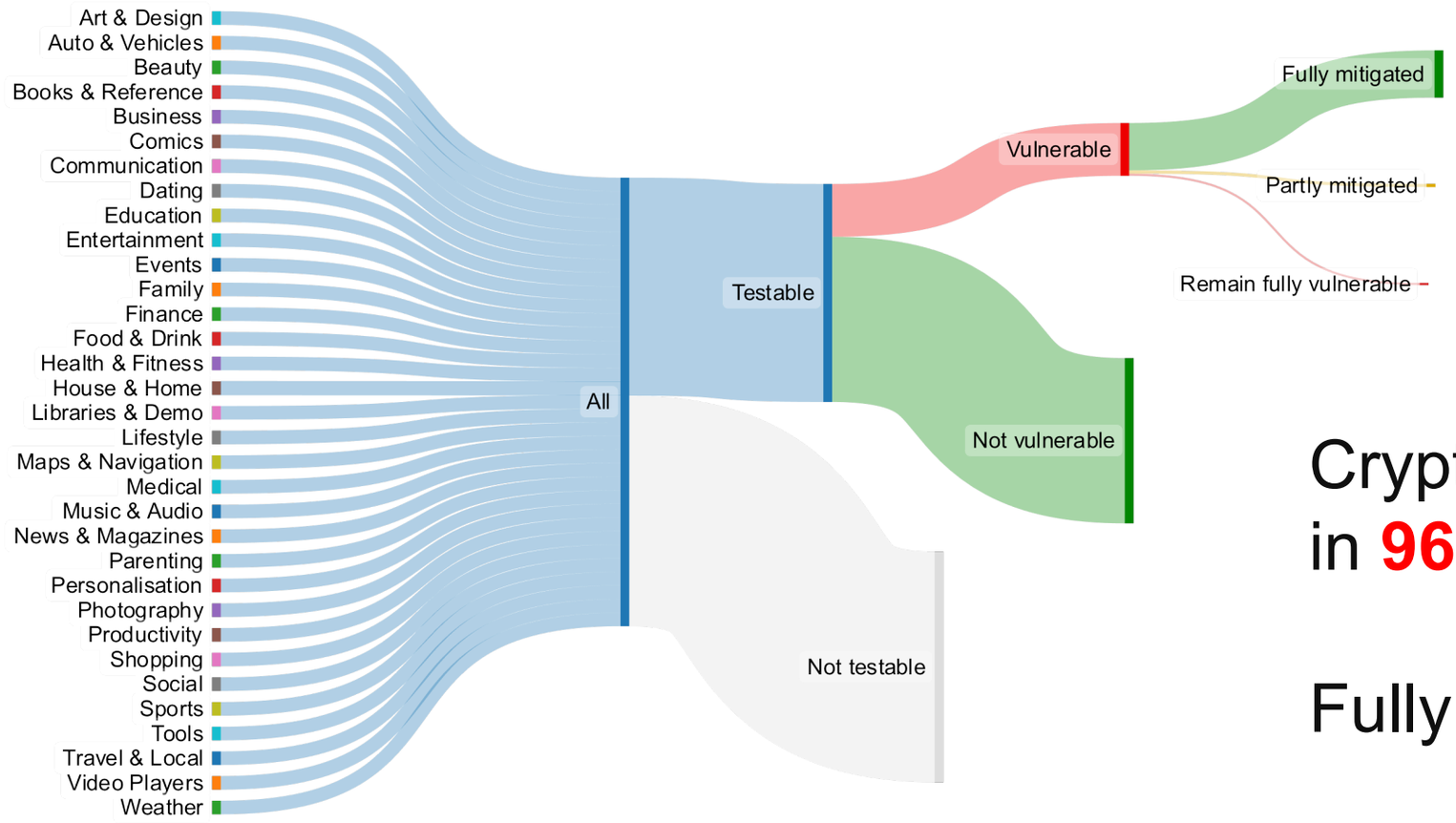


Evaluation

Evaluation

Automated analysis on 1604 most popular apps from Google Play

1604



Crypto API misuse mitigated in **96%** of vulnerable apps

Fully mitigated in **90%**

Evaluation

- Automated analysis
  - Misuse **mitigated in 96%** of vulnerable apps
- Manual analysis
  - Functionality retained for **92%** of 99 popular apps
- Performance measurements
  - **Minimal** size and runtime overheads
- Synthetic detection benchmark
  - **No FN, better FP** than CryptoGuard
- Case studies of 2 critically vulnerable apps

Conclusion

CryptoShield

- First practical mitigation for crypto API misuse in compiled apps
  - Help Android users protect themselves
- Mitigation procedures
  - for 10 common crypto API misuses
- High efficiency and efficacy

Questions?

Scan for full paper

Bibliography

[**GKL+19**]: Gao et al.: “Negative Results on Mining Crypto-API Usage Rules in Android Apps”, *MSR 2019*

[**OHA+21**]: Oltrogge et al.: ”Why Eve and Mallory Still Love Android: Revisiting TLS (In)Security in Android Applications”. *Usenix Security 2021*

[**PGC+21**]: Piccolboni et al.: “CRYLOGGER: Detecting Crypto Misuses Dynamically”. *S&P 2021*

[**BHM+16**]: Buhov et al.: “Pin it! Improving Android network security at runtime”. *IFIP Networking 2016*

[**MLT+16**]: Ma et al.: CDRep: “Automatic Repair of Cryptographic Misuses in Android Applications”. *AsiaCCS 2016*

[**RXA+19**]: Rahaman et al.: “CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects”. *CCS 2019*

Bonus Case Study

- Amaze File Manager
  - Open Source, more than 10 million users total

- Used hardcoded IV for all AES-GCM file encryptions
  - $P_2 = C_1 \oplus C_2 \oplus P_1$ (for C_1, C_2 using same key)
  - Any app that guessed any P could decrypt any C

- CryptoShield's mitigation generates fresh IVs
  - Successfully fixes the flaw