riscure

HCE

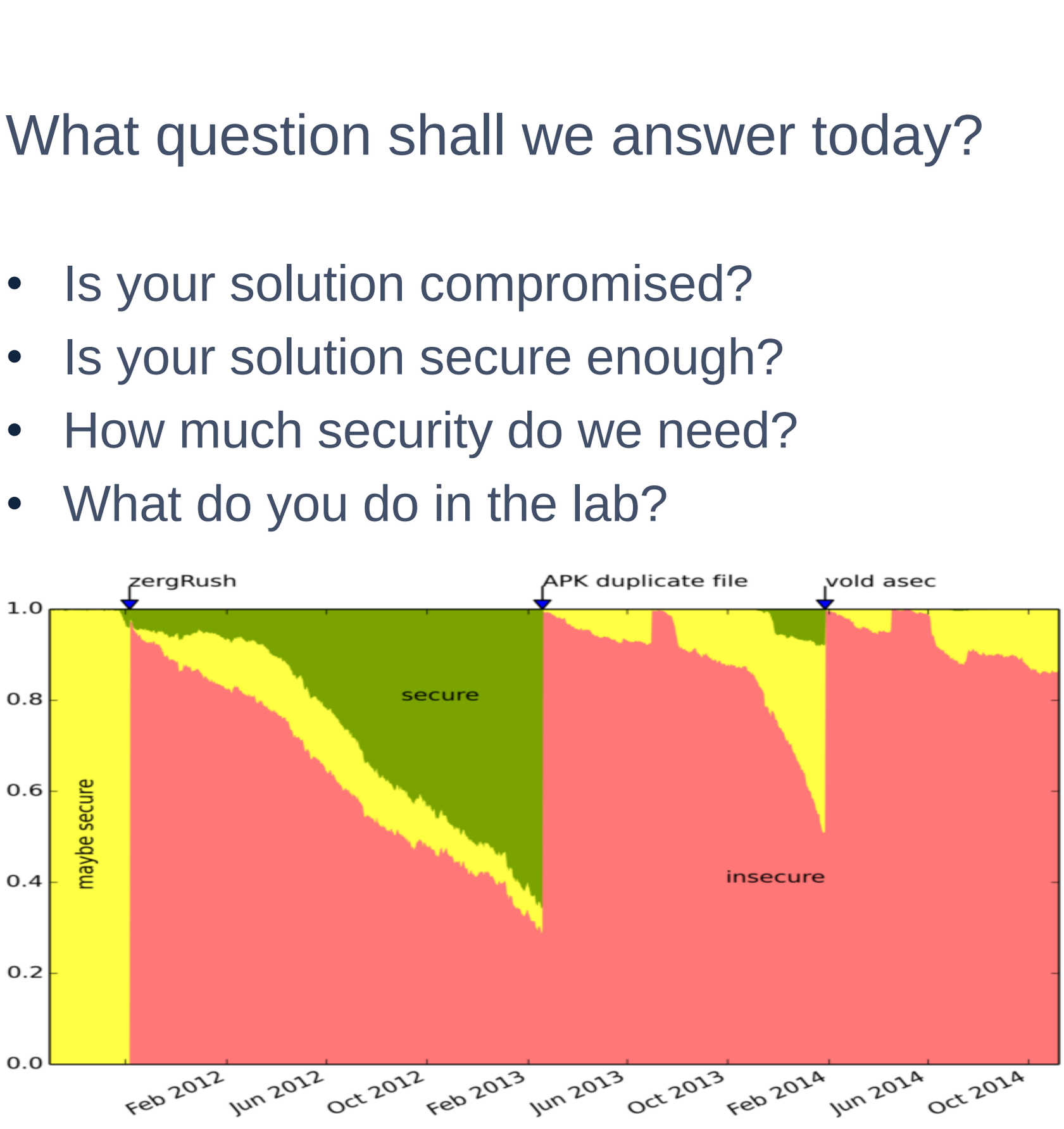
Is your solution compromised?

Alan MARZEC

May, 2015

What question shall we answer today?

- Is your solution compromised?
- Is your solution secure enough?
- How much security do we need?
- What do you do in the lab?



http://androidvulnerabilities.org/images/norm_versionsecurity.png

Content

1- What is HCE, from a security lab perspective?

2- Security Evaluation: The Process

3- Security Evaluation: the ‘Hacking’ or the tests

4- Mitigation Techniques

5 - Conclusion

1- What is HCE, from a security lab perspective?

How HCE impacted our security lab?

- Transition to a solution relying on SW only

- Product with a faster lifecycle = capped evaluation
  - **IC Evaluation:** 6-10 months
  - **Platform Evaluation:** 4-8 months
  - **ICC Evaluation:** 20-40 days
  - **MPA:** 25-40 days

- New type of developer coming from the ‘app’ world with a different mindset than traditional smartcard companies

- New tools used for the evaluation

How HCE impacted our security lab?

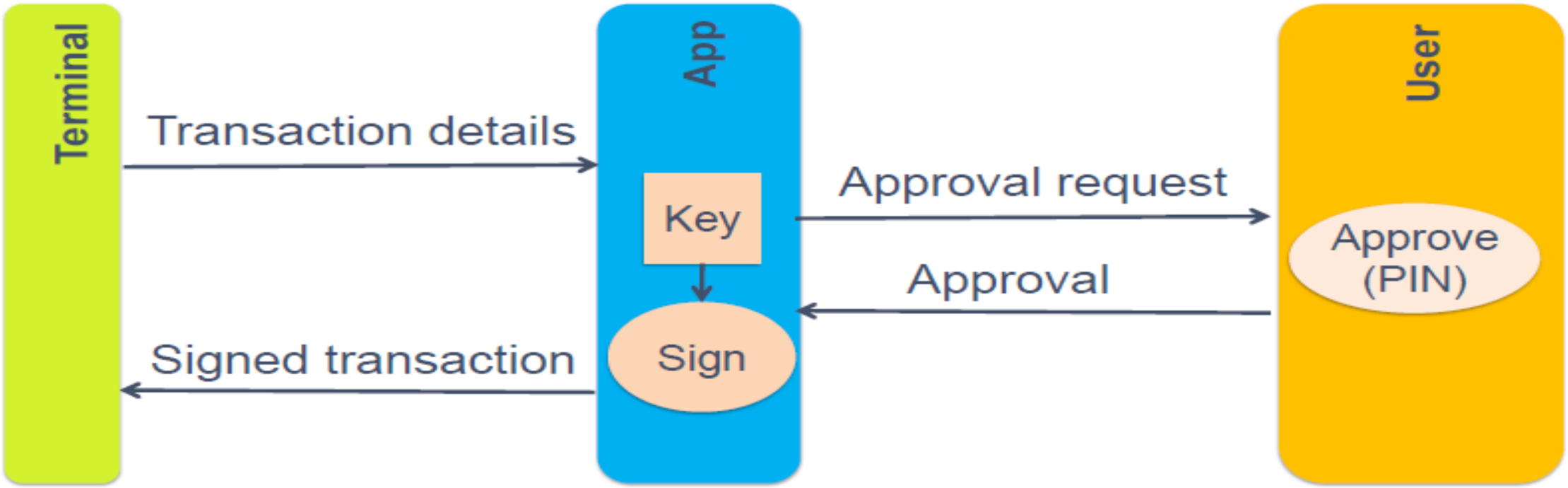
- Not yet defined level of security to attain or vulnerability rating. Common statement “We know the app is not secure”

- Important need for support, and training (admin, process, technical)

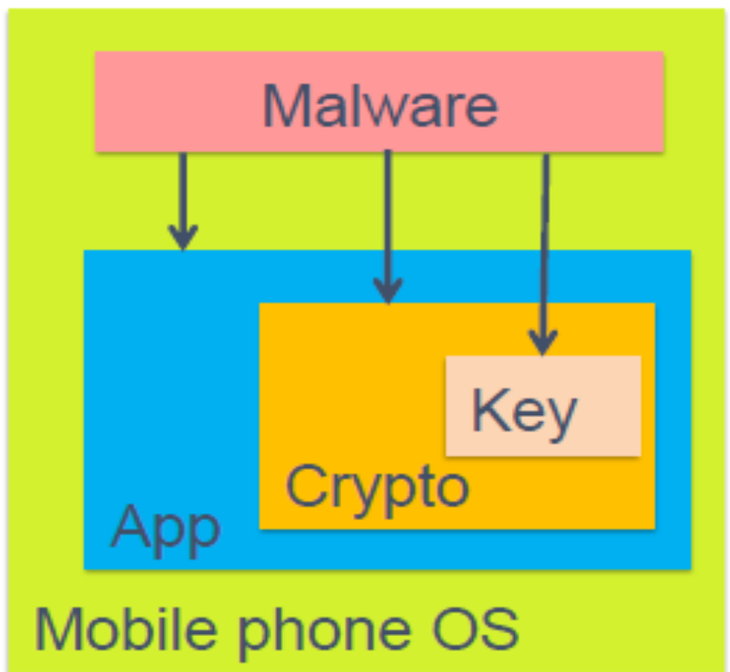
- Specific skill set for the analysts: ‘Mobile Reverse Engineering’

- Fast growing market, need to scale up resources to propose a shorter lead time

Transaction Protection, Assets and Malware



- Assets:
  - keys (transaction participation)
  - PIN (user content)
- Malware threats:
  - Sign manipulated transaction
  - Sign arbitrary transactions
  - Extract keys
  - Attacks Scale

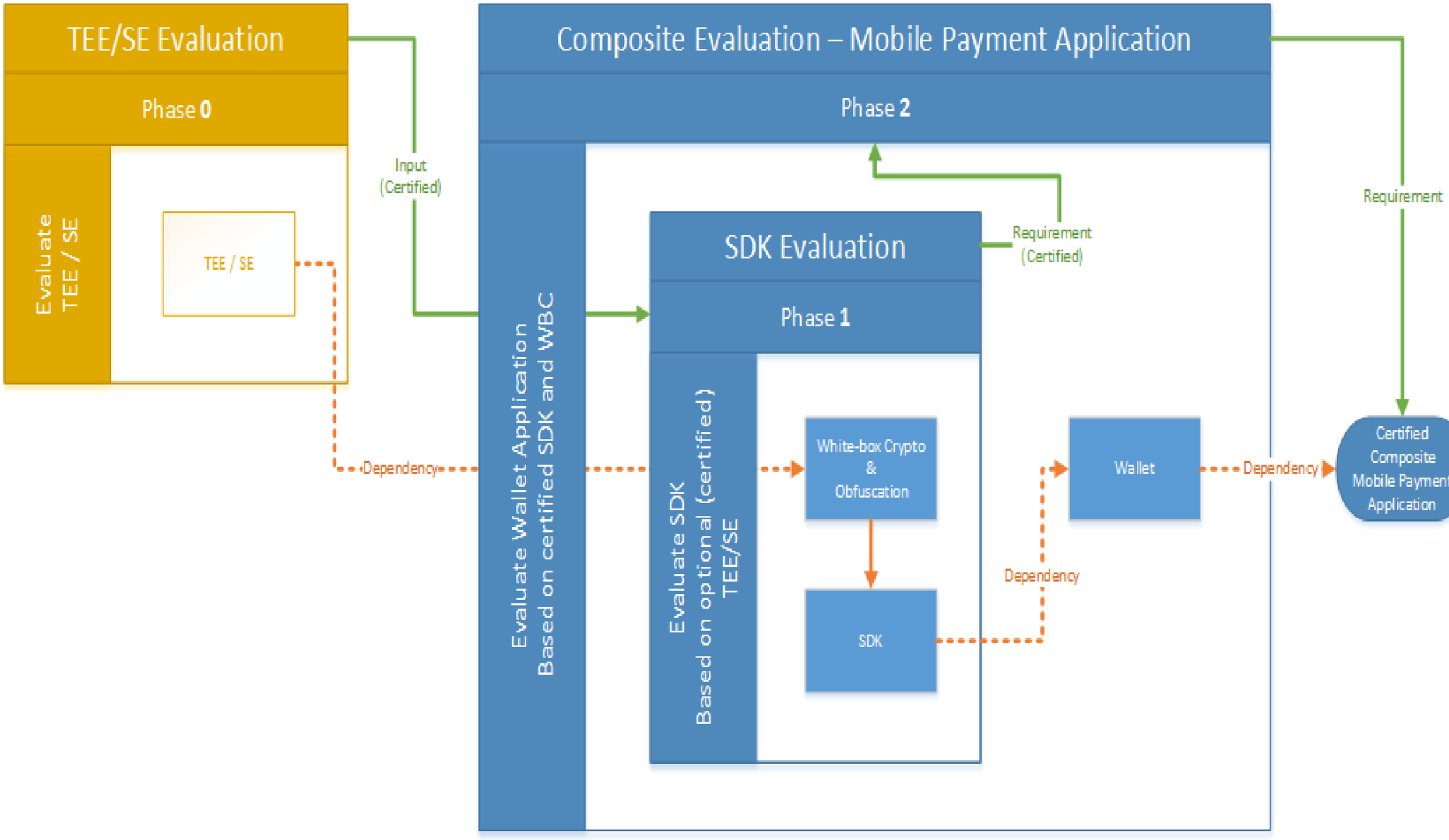


2- Security Evaluation – The process

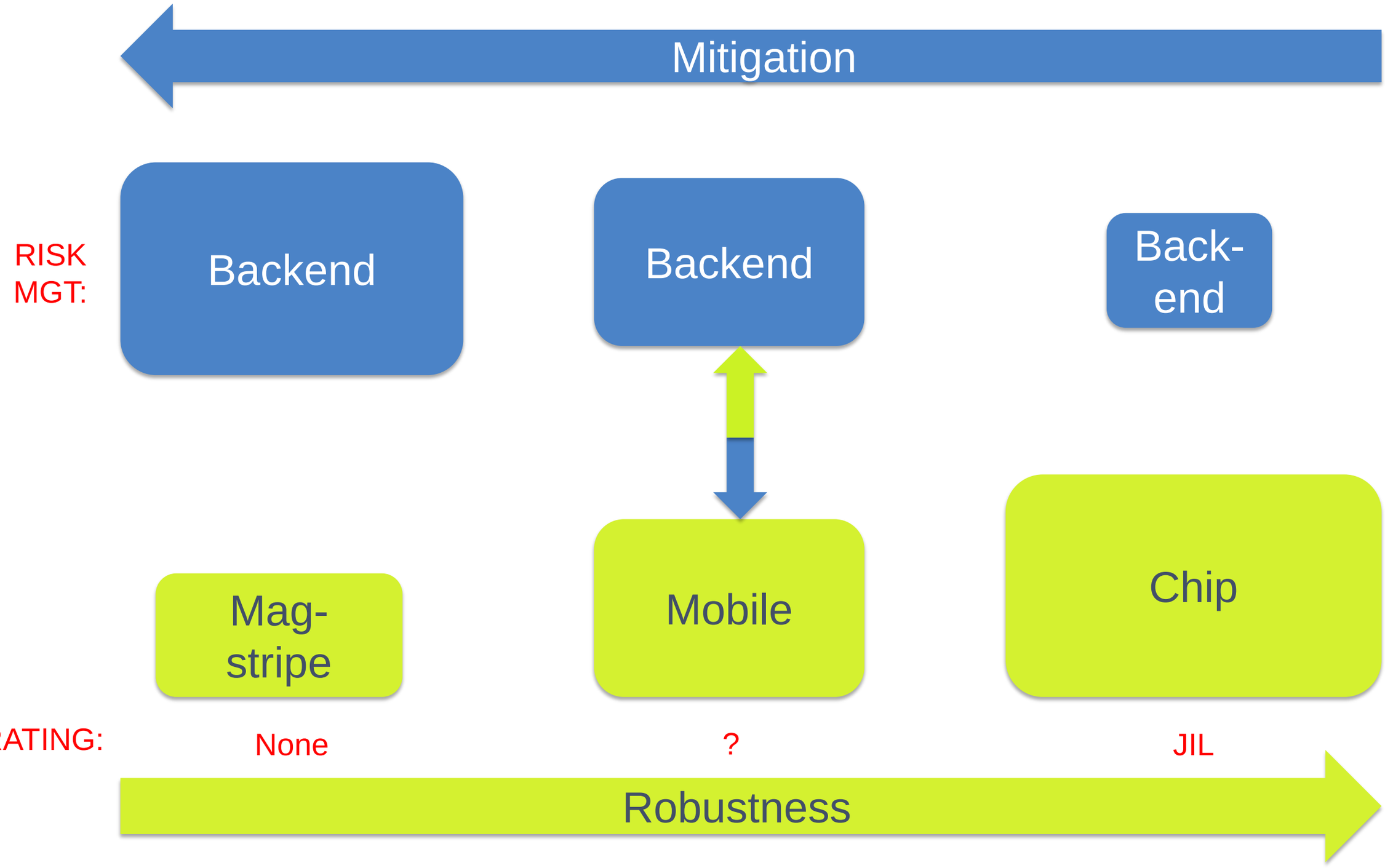
Security Evaluation Process

- Evaluation pre-requisites:
  - Security Guidance
  - Solution Description
  - Transaction Simulation Environment
  - Source Code
- Evaluation Deliverables:
  - Evaluation Report

Security Evaluation Process - Composition



Dilemma: Rating does not include Issuer controls in backend system



Security Evaluation Process - Rating

- Challenges:
  - Consider device root access
  - Differentiate assets value
  - Differentiate identification and exploitation?

- Rating Considerations:
  - Input for risk management
  - Incorporate ease of attacks
  - Incorporate scalability
  - Rating applicable on device only?

- References: JIL, CC v3.1, CVSSv2

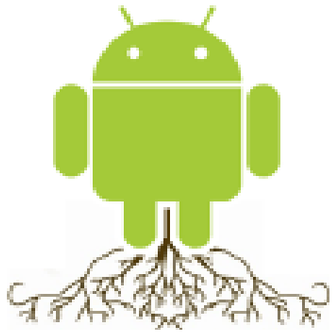
3- Security Evaluation – The ‘hacking’ or test

Security Evaluation Tests - Examples

(not to be considered as a reference test plan)

- **T-001** Reverse engineering the APK to identify protection mechanisms that have been implemented, extracting secrets and possibly lifting or cloning the implementation.
- **T-002** Circumvent the root and debug detection as a precondition for other attacks (circumvent security tests).
- **T-004** Intercept the upstream remote management communication, without modifying the APK.
- **T-005** Replace the CA certificate for the certificate pinning.
- **T-006** Extract the Storage Key and stored data
  Reason: Device information and user preference data is sufficient to reconstruct the key
- **T-009** Modify the Wallet (MPA) code without changing the SDK component (circumvent integrity check).
- **T-010** Attempt to migrate the Google Cloud Messaging (GCM) ID to a different device.

Security Evaluation Tests - Tools

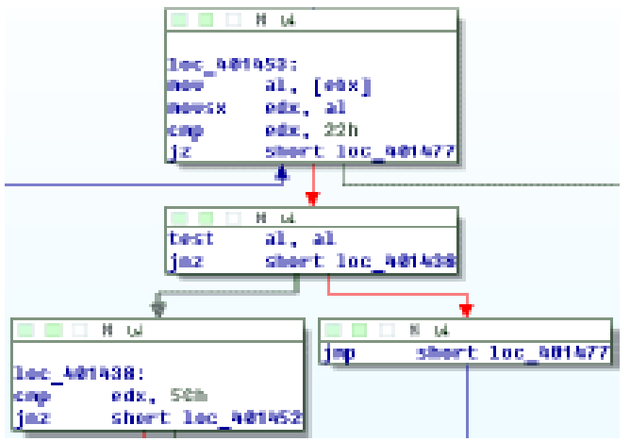


Rooting tool
e.g. Towelroot

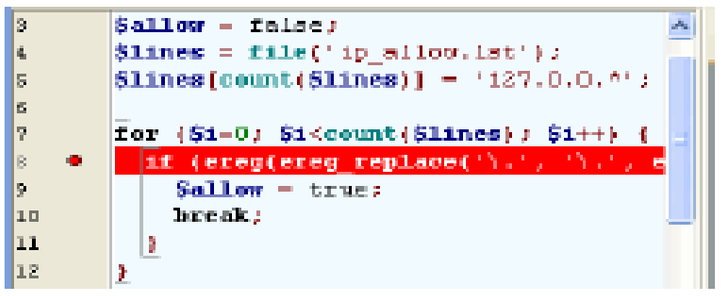
Development kit

Inspection tool
e.g. Androguard

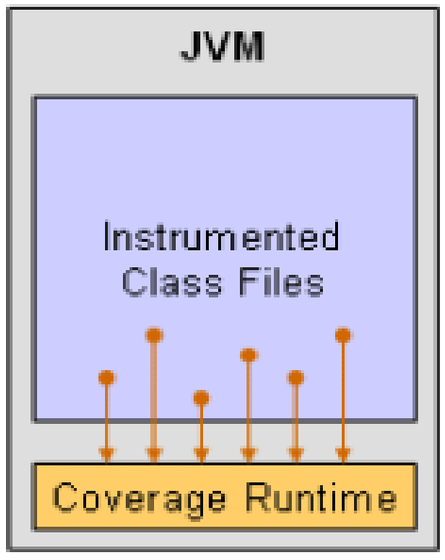
Decompile
e.g. JEB



Disassembler
e.g. IDA



Debugger
e.g. GDB, JDWP



Instrumenting
e.g. ADBI, DDI

4- Mitigation Techniques

How to increase the apps security?

- Software support:
  - Obfuscation
  - Tamper proofing
  - White-Box Crypto
- Hardware support:
  - Secure Element
  - Trusted Execution Environment
  - TPM
- Cloud:
  - Secure element in the cloud
  - Tokenization
  - Key rotation / software update

Mixing countermeasures increase the security

How to anticipate attacks?

- Collaboration:
  - Between software supplier and SDK developer (developer guidance)
  - Between SDK developer and issuer (issuer guidance)
  - With the laboratory (Evaluation report, rating, guidance)

- Evaluation:
  - Find your weaknesses before they hurt !!!
  - Good marketing tool (if successful)
  - Evaluation **vs** Plug and Pray

5- Conclusion

How to anticipate attacks?

- Smartphones are not secure platforms
- Malware allow attackers to scale rapidly
- Collaborate with your partners to develop according guidance
- Do not neglect the documentation and guidance
- Composition, ratings, delta evaluation are still to be finalized but to be considered already
- Book a slot with the lab
- Prepare for Battle !!!


Questions
or Remarks?

riscure

Challenge your security

Contact: Alan MARZEC (marzec@riscure.com)

Intl Sales and Bus. Development Manager

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America
550 Kearny Street, Suite 330
San Francisco CA 94108
USA
Phone: +1 650 646 99 79

inforequest@riscure.com