iMAS
iOS Mobile Application Security

Gregg Ganley Gavin Black

Problem

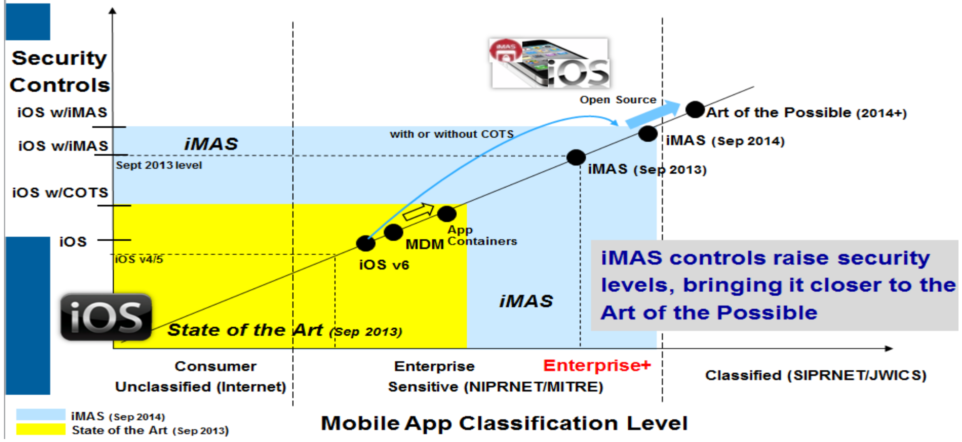
- iOS is considered secure, but out of the box security is not enough
- Simple device passcodes enable easy compromise of applications and data

Solution

- Patient/employee empowerment with secure mobile
- Additional security controls beyond Apple
- Reduce iOS app attack surface
- Extends security with or without MDM and commercial solutions
- Open source available

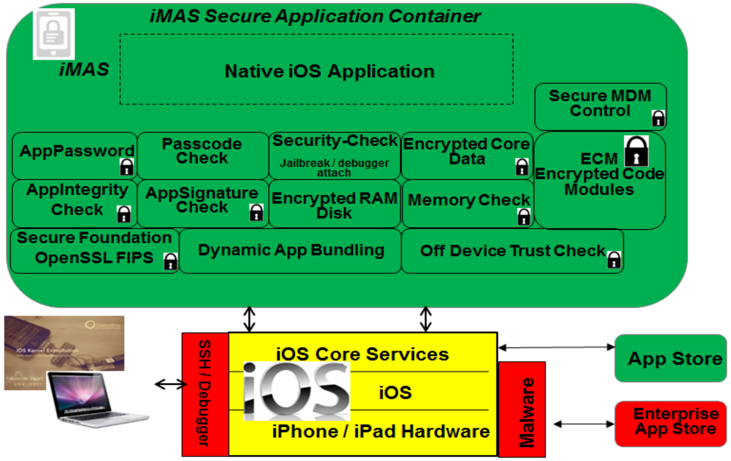
  project-imas.github.com
- Raise iOS app security levels - closer to the Art of the Possible

iMAS App Security "trade-space" Comparison Sep 2013



iMAS controls raise security levels, bringing it closer to the Art of the Possible

iMAS Secure Application Framework



Security Areas:

- App authentication
- Data at rest protection
- App at rest security
- Device Passcode check
- Jailbreak detection
- Debugger attach detect
- Encrypted SQLite
- FIPS compliance
- Lighting Connector Off Device Trust
- Dynamic application security bundle
- Secure Keychain
- Memory scrub after use
- Dynamic memory usage check
- Remote Wipe

🟩 Tolerable Security Risk

- Security Controls beyond Apple iOS
- Reduces iOS app attack surface
- Vetted, prioritized security control set
- Open source, grow community

Open Source
github.com/project-imas

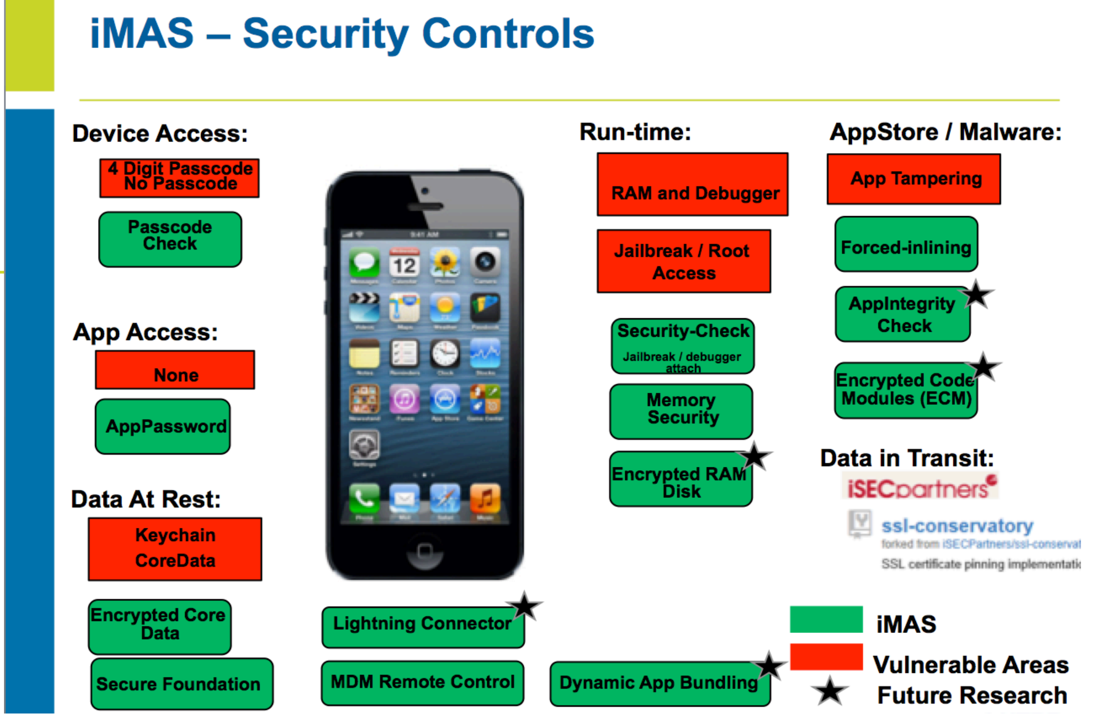
Approved for Public Release; Distribution Unlimited. 13-1012

Contact

- **Github:**
  project-imas.github.com

- **POC:**
  - MITRE, Bedford MA
  - Gregg Ganley
    - 781-271-2739
    - gganley@mitre.org
  - Gavin Black
    - 781-271-4771
    - gblack@mitre.org

MITRE



iMAS – Security Controls

Device Access:

- 4 Digit Passcode No Passcode
- Passcode Check

App Access:

- None
- AppPassword

Data At Rest:

- Keychain CoreData
- Encrypted Core Data
- Secure Foundation

Lightning Connector ★

MDM Remote Control

Run-time:

- RAM and Debugger
- Jailbreak / Root Access
- Security-Check Jailbreak / debugger attach
- Memory Security
- Encrypted RAM Disk ★

Dynamic App Bundling ★

AppStore / Malware:

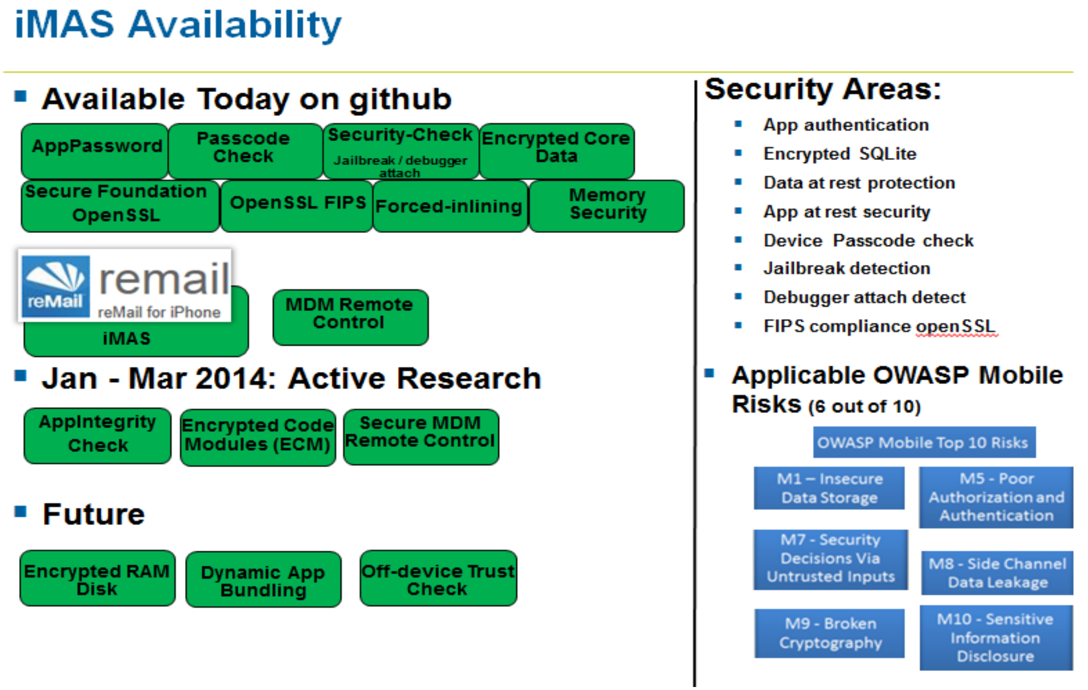
- App Tampering
- Forced-inlining
- AppIntegrity Check ★
- Encrypted Code Modules (ECM) ★

Data in Transit:

iSECpartners

ssl-conservatory
forked from iSECPartners/ssl-conservat
SSL certificate pinning implementatio

🟩 iMAS
🟥 Vulnerable Areas
★ Future Research



iMAS Availability

- **Available Today on github**

AppPassword | Passcode Check | Security-Check Jailbreak / debugger attach | Encrypted Core Data | Secure Foundation OpenSSL | OpenSSL FIPS | Forced-inlining | Memory Security

remail reMail reMail for iPhone iMAS

MDM Remote Control

- **Jan - Mar 2014: Active Research**

AppIntegrity Check | Encrypted Code Modules (ECM) | Secure MDM Remote Control

- **Future**

Encrypted RAM Disk | Dynamic App Bundling | Off-device Trust Check

Security Areas:

- App authentication
- Encrypted SQLite
- Data at rest protection
- App at rest security
- Device Passcode check
- Jailbreak detection
- Debugger attach detect
- FIPS compliance openSSL

- **Applicable OWASP Mobile Risks** (6 out of 10)

OWASP Mobile Top 10 Risks

- M1 – Insecure Data Storage
- M5 - Poor Authorization and Authentication
- M7 - Security Decisions Via Untrusted Inputs
- M8 - Side Channel Data Leakage
- M9 - Broken Cryptography
- M10 - Sensitive Information Disclosure