IBM SolutionsConnect 2015

Seize the Moment. Dive into Next Generation Technologies.

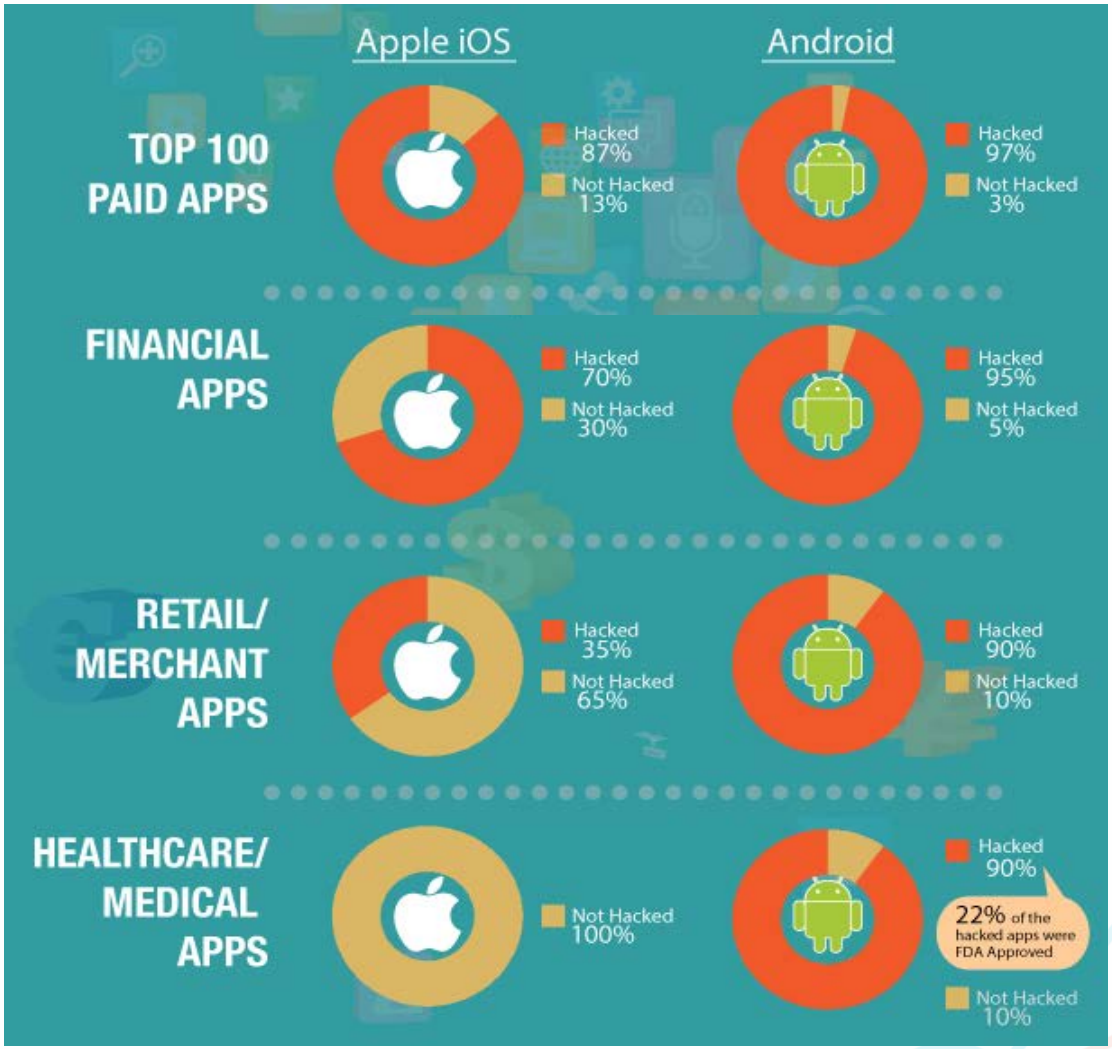
Securing Mobile Apps with App-Hardening and Run-Time Protection

Arxan Application Protection for IBM Solutions

Rich Lord – Vice President, Asia-Pacific

Arxan Technologies

Mobile Apps Are under Attack



Arxan: State of Security in the App Economy, 2014

- Majority of top 100 paid Android and iOS Apps are available as hacked versions on third-party sites ("State of Security in the App Economy", Arxan, 2014)
- "86% of Mobile Malware is legit apps repackaged with malicious payloads" (NC State University, 2012)
- "It is trivial for an attacker to hijack a legitimate Android application" (Alcatel-Lucent Kindsight Security Labs Malware Report, Q4 2013)
- "First known malware that can infect installed iOS apps … First in-the-wild malware to install third-party apps on non-jailbroken iOS devices." (Palo Alto Networks discovering WireLurker malware, Nov 2014)

Mobile Apps Are Vulnerable to Attacks

Confidentiality Risk

(Reverse Engineering or Code Analysis Vulnerabilities)

- **Sensitive information** can be exposed
- Applications can be reverse-engineered back to the **source code**
- Code can be lifted and **reused or repackaged**

Integrity Risk

(Code Modification or Code Injection Vulnerabilities)

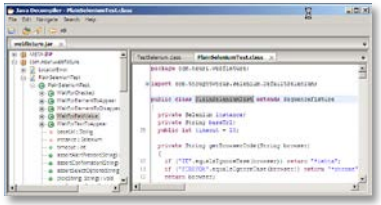
- Application binaries can be **modified**
- **Run-time behavior** of applications can be altered
- **Malicious code** can be injected or hooked into applications

Anatomy of Mobile App Attacks

1. **Define the exploit and attack targets**

Security controls
Sensitive functionality
Proprietary IP / data
Malware distribution

2. **Open up and examine the app**



Reverse-engineer app contents

Extract and steal confidential data

3. **Create a hacked version or distribute an exploit**

Create a tampered, cracked or patched version of the app

Release / use the hacked app

Use malware to infect/patch the app on other devices

https://www.arxan.com/how-to-hack-a-mobile-application

Lots of Automated Hacking Tools Can Be Used

Category	Example Tools
App decryption / unpacking / conversion	• Clutch • APKTool, dex2jar
Static binary analysis, disassembly, decompilation	• IDA Pro, Hopper • JEB, JD-GUI, Baksmali • Class, symbol, string dumping
Runtime binary analysis (debugging, tracing)	• GDB, ADB • Introspy, Snoop-It
Runtime manipulation, hooking, code injection, method swizzling, patching	• Cydia Substrate, Theos suite • Cycript, CInject • Hex editors
Malware / trojan injection	• Dendroid, AndroRAT
Jailbreak detection evasion	• xCon, tsProtector
Integrated weaponized toolsets	• AppUse, Snoop-It, iNalyzer

- Automated, free or low-cost tools lower barriers to hacking
- Many breaches and exploits can be created in hours or less
- Unprotected apps are easy prey for these hacking tools

Security For Apps in the Wild

Application Environment

Centralized, trusted environment
- Web apps
- Data center custom apps

Attackers do not have easy access to application binary

Distributed or untrusted environment "Apps in the Wild"
- Mobile Apps
- Internet of Things / Embedded
- Packaged Software

Attackers can easily access and compromise application binary

Application Security Model

Vulnerability Analysis and Flaw Remediation

Vulnerability Analysis and Flaw Remediation

"Build It Secure"

+

Application Hardening and Run-Time Protection

"Keep It Secure"

Experts Recommend Protecting Applications

"Lack of Binary Protection" is an OWASP Top Ten Mobile Risk

Analysts

Gartner

FORRESTER

451 Research

"Make application self-protection a new investment priority, ahead of perimeter and infrastructure protection."
"It should be a CISO top priority." - Gartner

"It ('application hardening and run-time protection') is a critical component in the strategy to secure enterprise software, embedded systems, mobile apps and the much-bandied 'Internet of Things'." - 451

Consultants

cigital

VIAFORENSICS

"Implement resistance against runtime manipulation and leverage code obfuscation to complicate reverse engineering, and use anti-tamper mechanisms" – viaForensics Best Practices Guide

Arxan Application Self-Protection

Defend
against
compromise

- Advanced Obfuscation
- Encryption
- Pre-Damage
- Metadata Removal

Detect
attacks at
run time

- Checksum
- Debug Detection
- Resource Verification
- Jailbreak/Root Detection
- Swizzling Detection
- Hook Detection

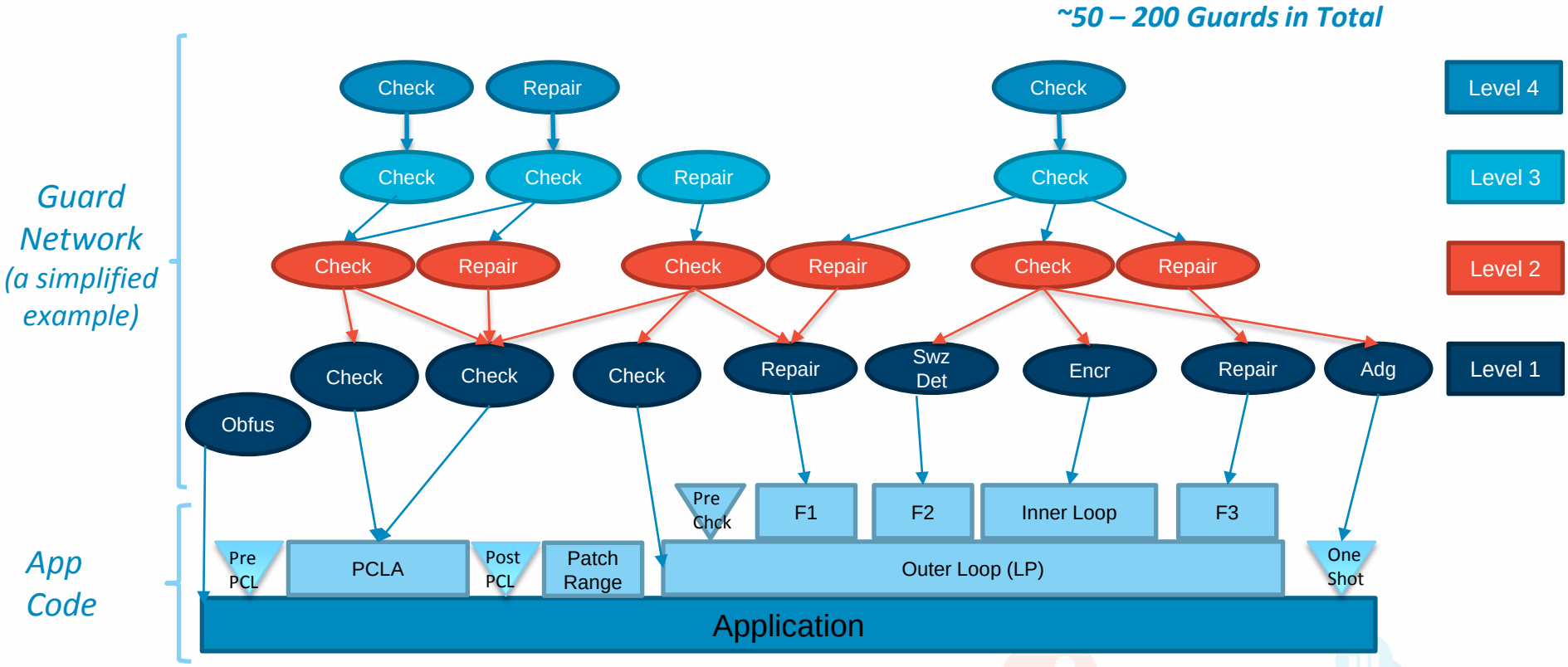
React
to ward off
attacks

- Shut Down (Exit, Fail)
- Self-Repair
- Custom Reactions
- Alert / Phone Home

Protected Application

- Self-defending
- Tamper-resistant
- Hardened against hacking attacks and malware exploits

Arxan Multi-Layered Protection – An Illustration



- Multi-Layered Guard Network with Defense in Depth
  (first Guard layer protects code, additional Guard layers protect lower-level Guards)
- Risk-Based, Custom Created for Each Application
- Randomized Binary Implementation for Automated Variability (every build looks different)

Steps to Protect an Application with Arxan

Identify risks and define what requires protection.

1

Original App
(to be released)

Arxan GuardSpec

2

Defines which Guards to place in mobile app to protect the app, and where to place them.

Arxan Protection Engine
(Guard Injection Engine)

Engine automates insertion of Guard Network in the app during the normal build process, without any need to modify source code.

3

Arxan Guards

Many different Guard types; thousands of Guard instances.

Protected App
(now ready for release)

4

Protected version of app with Guards dissolved into binary, cannot be identified or isolated. No accompanying libraries, or need to connect to Arxan at run-time.

Arxan Customer Examples

Sample customers:

- Multiple Leading Financial Services companies
  - 3 Top 10 Multi-National Bank
  - Multiple Retail Banks
  - Top 2 Credit and Debit Card Providers
  - Top Tier Mobile Wallet Providers
  - Top Tier Mobile Payment Providers
  - Mobile Gift Card and Point Card Providers
- 7 of top 10 Digital Media firms
- 4 of top 5 Software Eng. ISVs
- 3 of top 5 High-Tech vendors
- 4 of top 5 Gaming companies
- Multiple Critical Infrastructure companies Enterprise customer base
- Arxan-protected applications deployed today on over 500M devices
- Over 700 Customer Apps protected

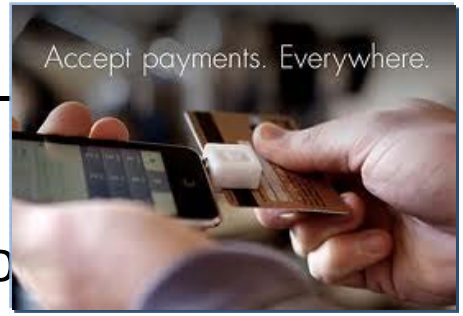
Arxan Case Example in Mobile Financial Services

- **CIO challenge: Drive mobile app innovation without compromising security and company assets**
  - External customer apps (B2C)
  - Internal employee apps (B2E)
- **Identified multiple hacking attack risks and targets for apps "out in the wild"**
  - Bypassing security controls, getting unauthorized access
  - Sensitive information exposure
  - Inserting exploits or malware, cloning applications
  - Exposing app internals and vulnerabilities
- **Used Arxan to protect mobile apps against attacks** (>15 apps protected to date)
- **CIO won CIO 100 Award for innovation**

Arxan Mobile Payment App Protection Case Example

- **Goal:** Secure the Customers mobile payment application for Android and iOS and also enable them to expand to new markets overseas

- **Challenge:** The security team at Customer is concerned about their internal encrypted storage keys and crypto code being reversed as well as some IP (Business logic, Jailbreak detection, etc.) contained in the mobile app. Brand protection is paramount.



- **Arxan Solution:**
  - Arxan's code hardening (EnsureIT® for Andro
    Apple iOS) to protect layers of their code
  - Protection of Java and Native code (Objective C, C++)
  - Key Hiding with Arxan TransformIT

Why IBM and Arxan?

- ✓ 'Gold standard' protection strength
  - Multi-layer Guard Network
  - Static & Run-Time Guards
  - No binary signatures or agents, no single point of failure
  - Customizable to your application
  - Automated randomization for each build
- ✓ No disruption to SDLC or source code with unique binary-based Guard injection
- ✓ Cross platform support -- > 7 mobile platforms alone
- ✓ Proven
  - Protected apps deployed on over 500 million devices
  - Hundreds of satisfied customers across Fortune 500
- ✓ Unique IP ownership: 10+ patents
- ✓ Integrated with other IBM security and mobility solutions

Additional Resources

IBM / Arxan White Paper: Securing Mobile Apps in the Wild
State of the Mobile App Security Report

http://www-03.ibm.com/software/products/en/arxan-application-protection

IBM / Arxan Short Demos: Securing Mobile Apps in the Wild

- Risks for mobile apps and how to protect them
- How to protect mobile apps against attacks
- Demo of how easy it is to hack an app

http://www.arxan.com/solutions/arxan-mobile-app-protection-with-ibm/

IBM SolutionsConnect 2015

Seize the Moment. Dive into Next Generation Technologies.

Thank You