RSA CONFERENCE ASIA PACIFIC 2013

BYOD AND NEXT-GENERATION MOBILE SECURITY

Joseph Gan
V-Key Inc

Session ID: MBS-W02
Session Classification: General Interest

Next-Generation Computing

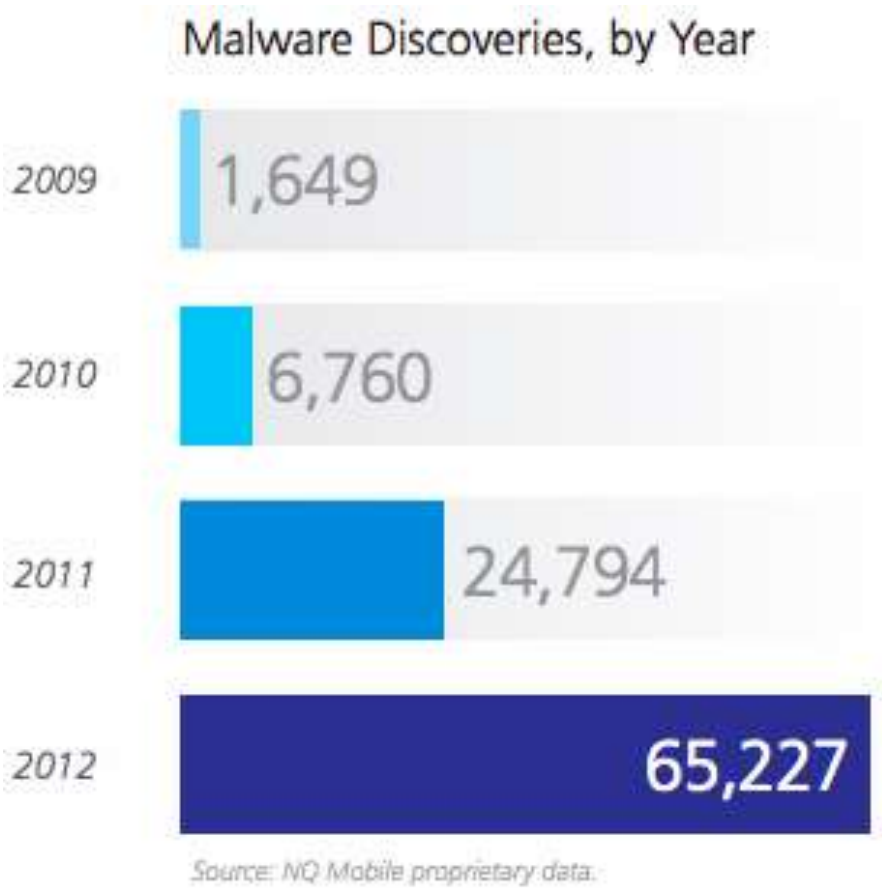
- Mobile enterprise apps

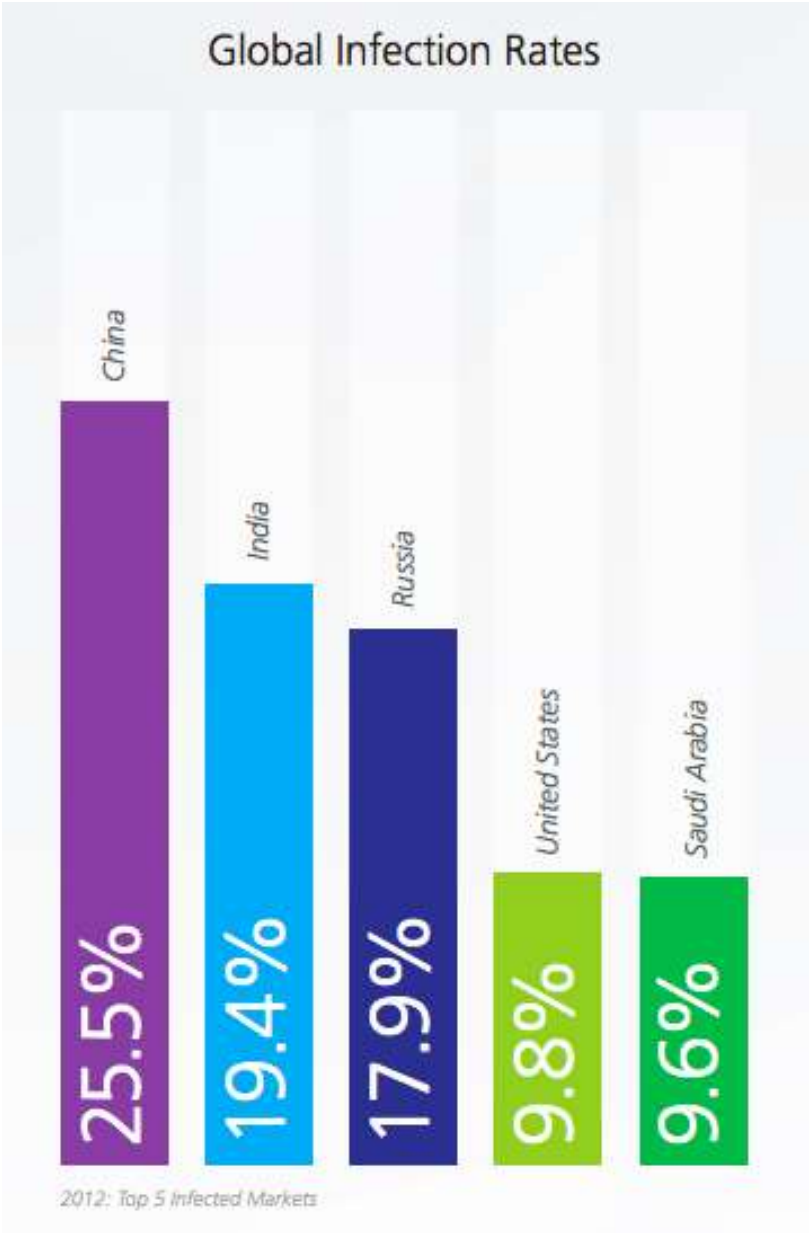
- Mobile payments

- Mobile authentication

- Mobile banking

Mobile: Secure?





Mobile OS: Different?

iOS, Android Vulnerabilities Found at HP's Mobile Pwn2Own Event

Both iOS and Android fall to hackers at the H is it?

By **Sean Michael Kerner** | September 21, 2012

Serious Vulnerability Leaves Samsung Exynos Powered Devices Open To Data Wipes, Bricking

Killian Bell (5:00 am PDT, Dec 17th)

Like 6 Tweet 5 1

ynos-powered smartphones
an provide attackers with
alicious apps that can
ck their handset.

who has tested it on a
amsung devices, and even

n APK that successfully
erSU app "on any Exynos4-
loit include:

Samsung Galaxy S3 LTE

Apple provides 197 security reasons to upgrade to iOS 6

Summary: *Now that iOS 6 is available, Apple has revealed what security vulnerabilities exist and have been patched in its latest mobile OS.*

By Michael Lee | September 20, 2012 -- 00:37 GMT (17:37 PDT)

Follow @mukimu

There are now 197 new reasons for iPhone, iPod Touch, and iPad users to upgrade to iOS 6, with Apple closing the same number of vulnerabilities in its mobile operating system.

The company released its security bulletin for the new version of iOS today, revealing what security flaws have existed in previous versions.

Vulnerabilities include three different ways of completely bypassing iOS' passcode lock, and at least 10 different ways of running arbitrary code. The latter types of vulnerabilities are what enable users to jailbreak their devices.

Motivations for Mobile Attacks

Mobile Malware: Growth Stuns, Storms and Threatens

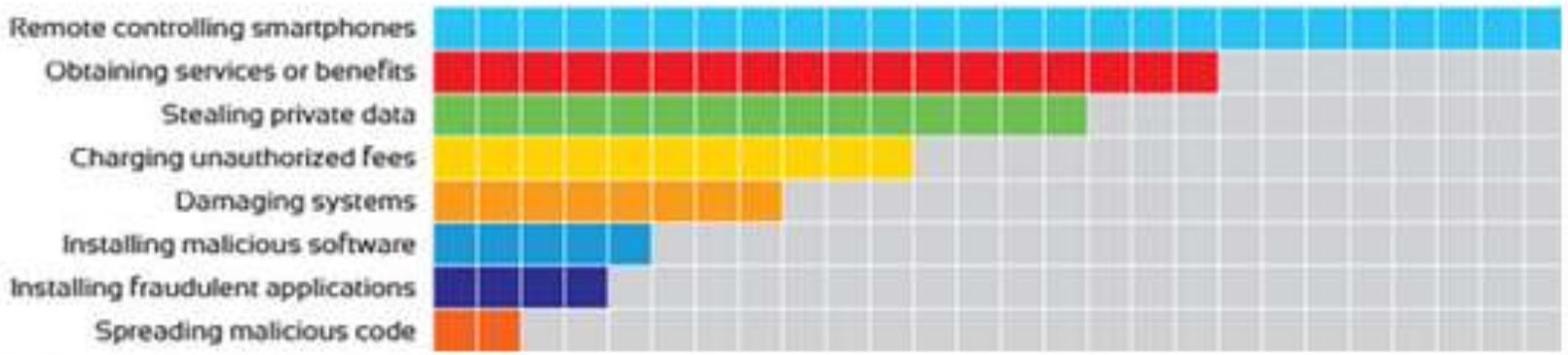
Author: Gina Smith

Most people are clueless about the prevalence among global Android malware. Or mobile malware in general. As Jim Morrison of The Doors famously said in his written poetry, "Wake up!" Scroll down to hear it.

WHAT ARE CYBER CRIMINALS DOING WITH SMARTPHONES?

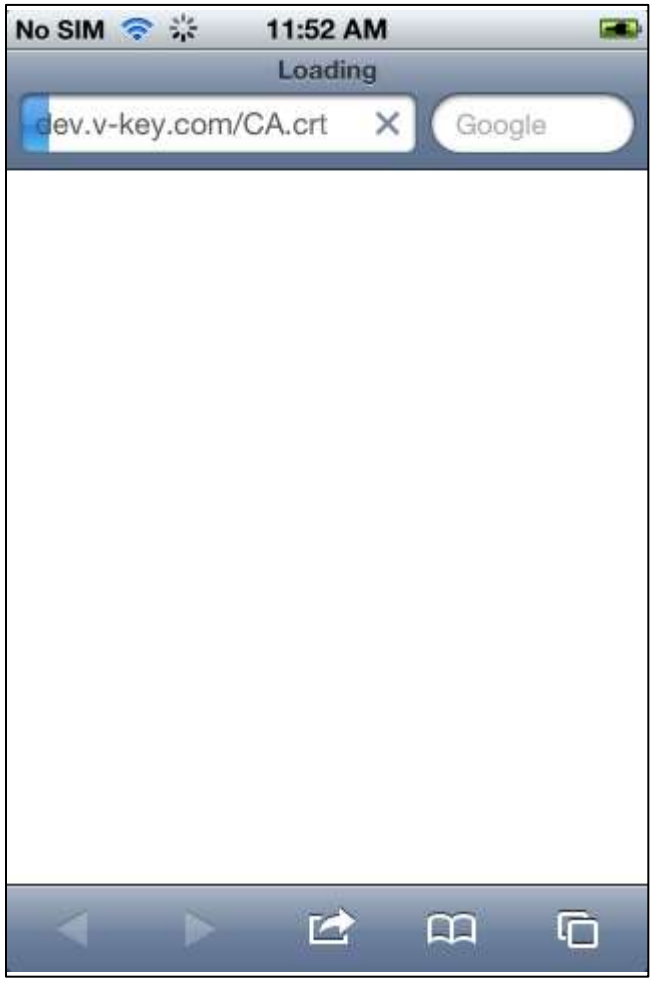
Cyber criminals had 8 primary motivations for creating malware.

MALWARE/PERCENTAGE OF MALWARE



Mobile Spywares… + more!

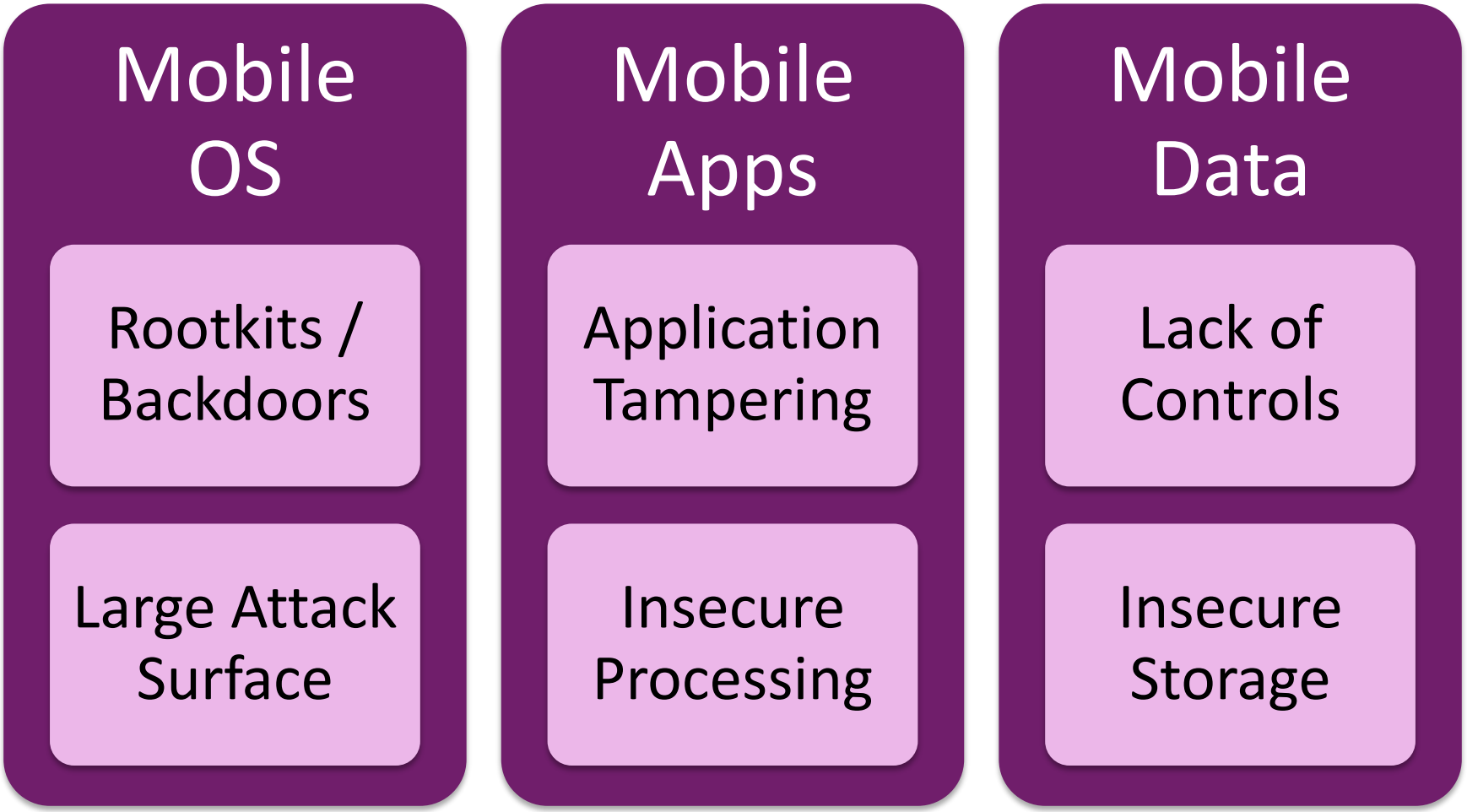
SSL: Encrypted?



Problematic Data Security

- Have we solved mobile data security?
  - Passcode locks
  - iOS: Keychain
  - Full Disk Encryption
  - App-specific encryption
- Ummm… no.
  - OS has access to all “encrypted” data
  - Apps have access to their own data – of course!
  - …and therefore, so do the trojans and spyware.
- We only have “lost device” data protection.
- Problem: apps and data moving to the mobile device.

State of Mobile Security



Existing Best Practices

- Mobile application development
  - Data-at-Rest
    - Don’t store data on the mobile device by yourself!
    - If you do, at least use the encrypted storage and Keychain
  - Data-in-Transit
    - SSL certificate pinning to guard against MITM
  - Risk Mitigation
    - Consider blocking jailbroken / rooted devices, especially for in-house apps
    - Consider using second-factor authentication
- Not perfect solutions, but raise the bar for attackers

Existing Third-Party Solutions

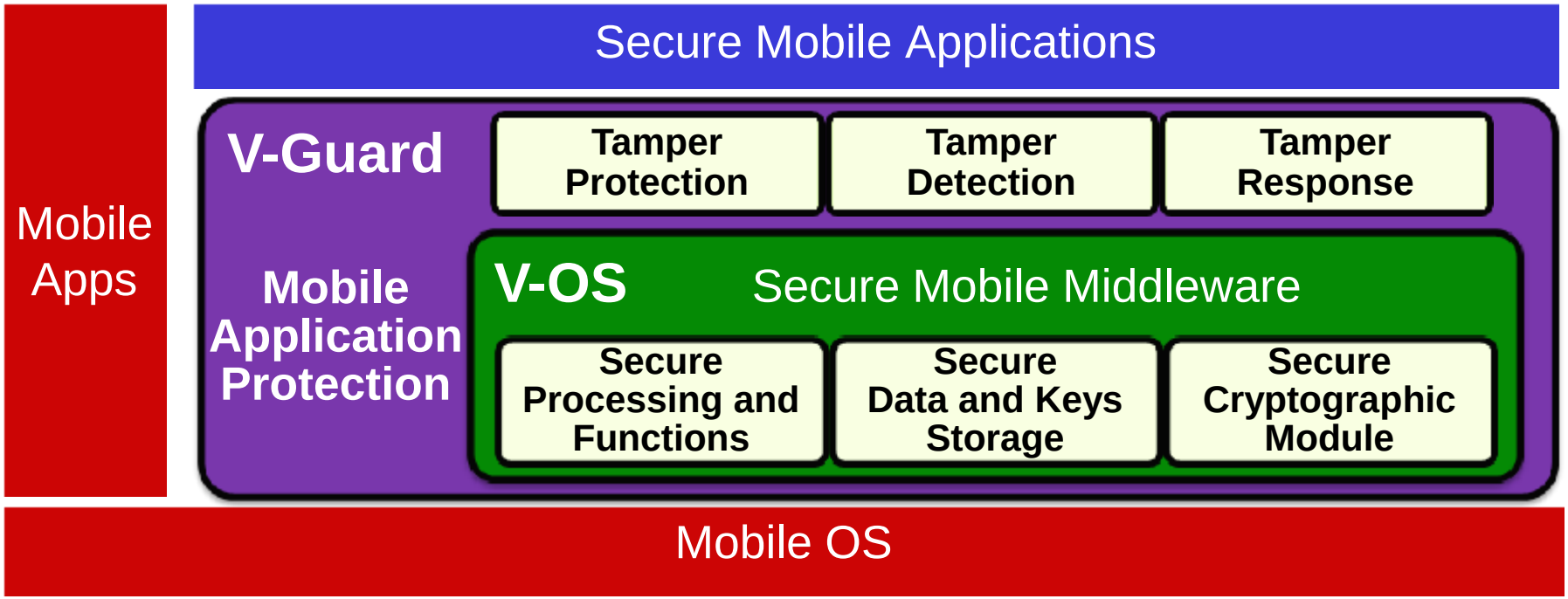
	Mobile Anti-Virus	Sandboxed Apps	Device Virtual.	App Wrapping
What users are supported?				
Public / Consumers	✓			
Enterprise / Employees	✓	✓	✓	✓
How well does it work?				
Control over apps and data		✓	✓	✓
Blocking common threats	✓			✓
Blocking advanced attacks				
How is the user experience?				
Little visible impact to user			✓	✓
Supports any mobile device	✓	✓		✓

App Wrapping: Pros and Cons

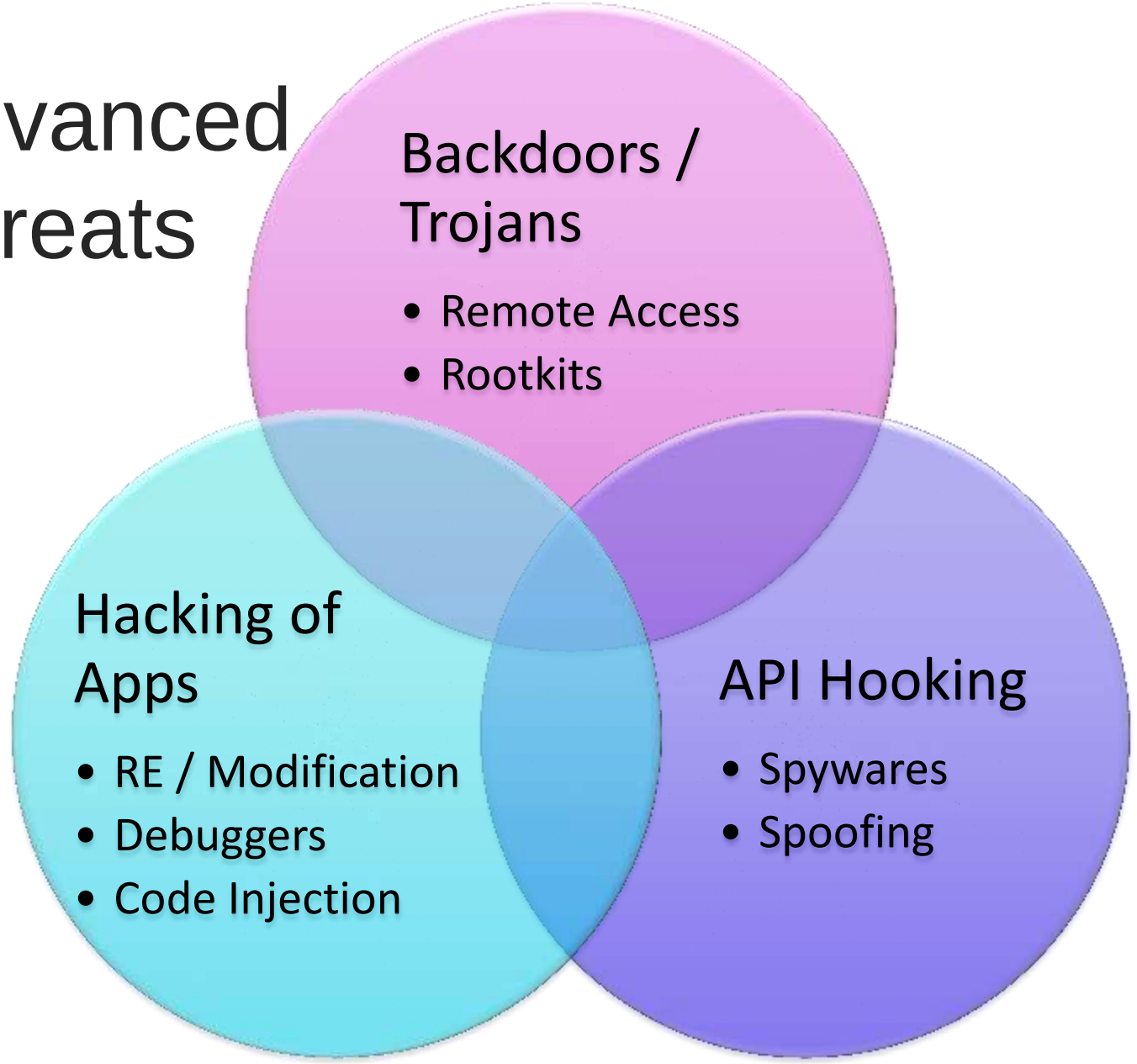
- Pros
  - Arguably the best solution available
  - Provides protection for any mobile application
  - Various options available for source code
  - Provides the best security control with the least user impact
- Cons
  - Lack of support for public-facing applications
  - Limited protected against even common threats
  - Lack of protection against advanced threats

Background: V-Key's Approach

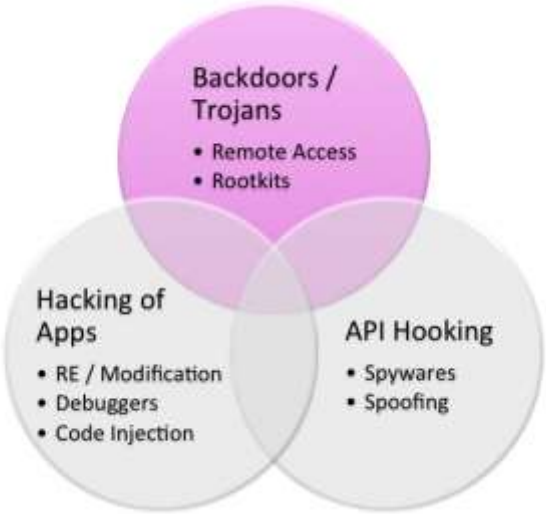
- Application virtual machine acts as reverse sandbox
- Protection layer guards against advanced threats



Advanced Threats

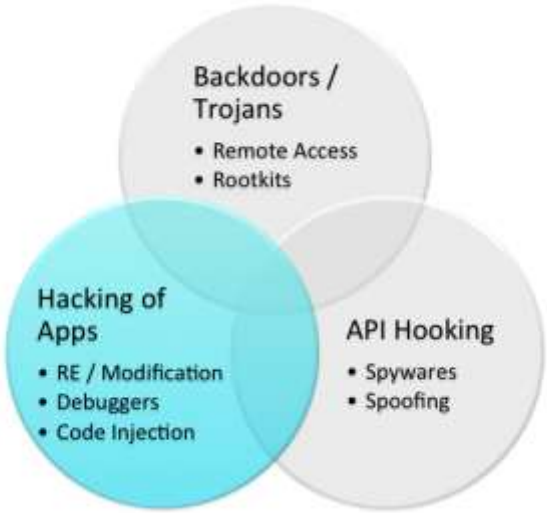


Backdoors / Trojans



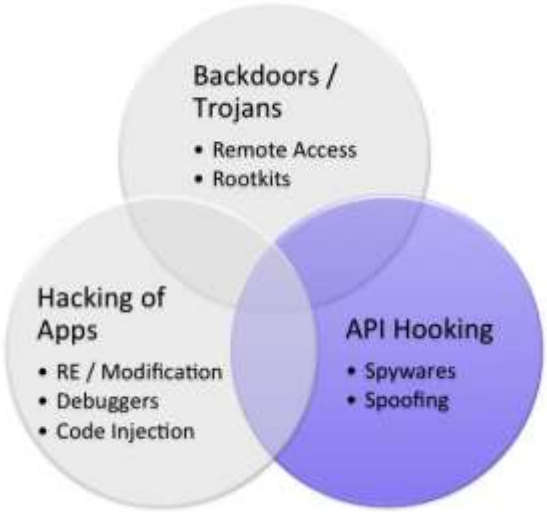
- Threats
  - Remote access trojans
  - Rootkits
- Protections
  - Running daemon detection
    - e.g., checking the launchctl list of running daemons
  - Checking root services and files
    - e.g., check for root-privilege files, not just /bin/su
  - Checking ports, system processes
    - e.g., extracting ports and processes using sysctlnametomib()

Hacking of Apps



- Threats
  - Reverse engineering / modification
  - Debugger misuse / code injection
- Protections
  - Anti-debugging mechanisms
    - e.g., various ptrace calls and checks
  - Application integrity checks
    - e.g., checking hash of entire application package
  - Runtime code injection detection
    - e.g., hooking onto “dyld_callback_add()”
  - Secure processing in virtual sandbox

API Hooking



- Threats
  - Spywares (e.g., keyloggers)
  - Device / location spoofing
- Protections
  - Load-time library detection
    - e.g., looking for “ikg.dylib”
  - Function call integrity checks
    - e.g., verifying “[UIKeyboardImpl callShouldInsertText:]”
  - Check for misused permissions (Android)
    - e.g., heuristics could include “android.permission.RECEIVE_SMS”

Conclusion

- Mobile threats to your apps and data are very real
- Existing mobile best practices help to some extent
- Limited options to counter advanced mobile threats
- Security is tough – approach your vendors for help!
- Also, check out our 2nd talk tomorrow on "Developing an Enterprise Mobile Security Strategy"
- Come to our booth (G1) to find out more

Questions?