Defending Behind The Device
Mobile Application Risks

Tyler Shields

Product Manager and Strategist

Veracode, Inc

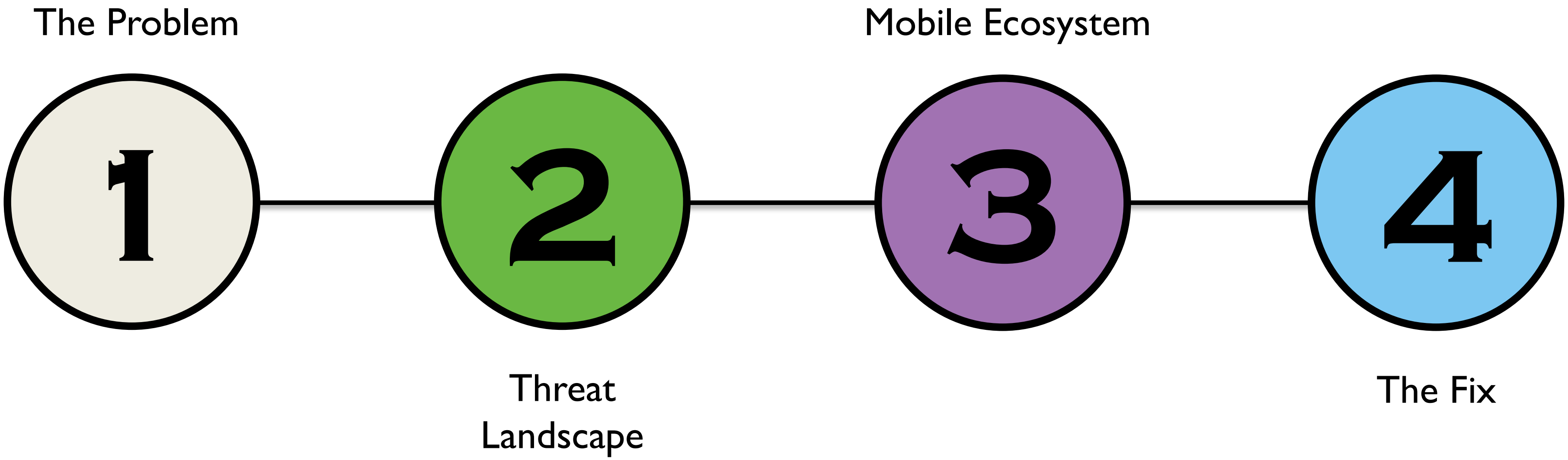
Session ID: MBS-301

Session Classification: Advanced

RSACONFERENCE
EUROPE 2012

Agenda

The "What"



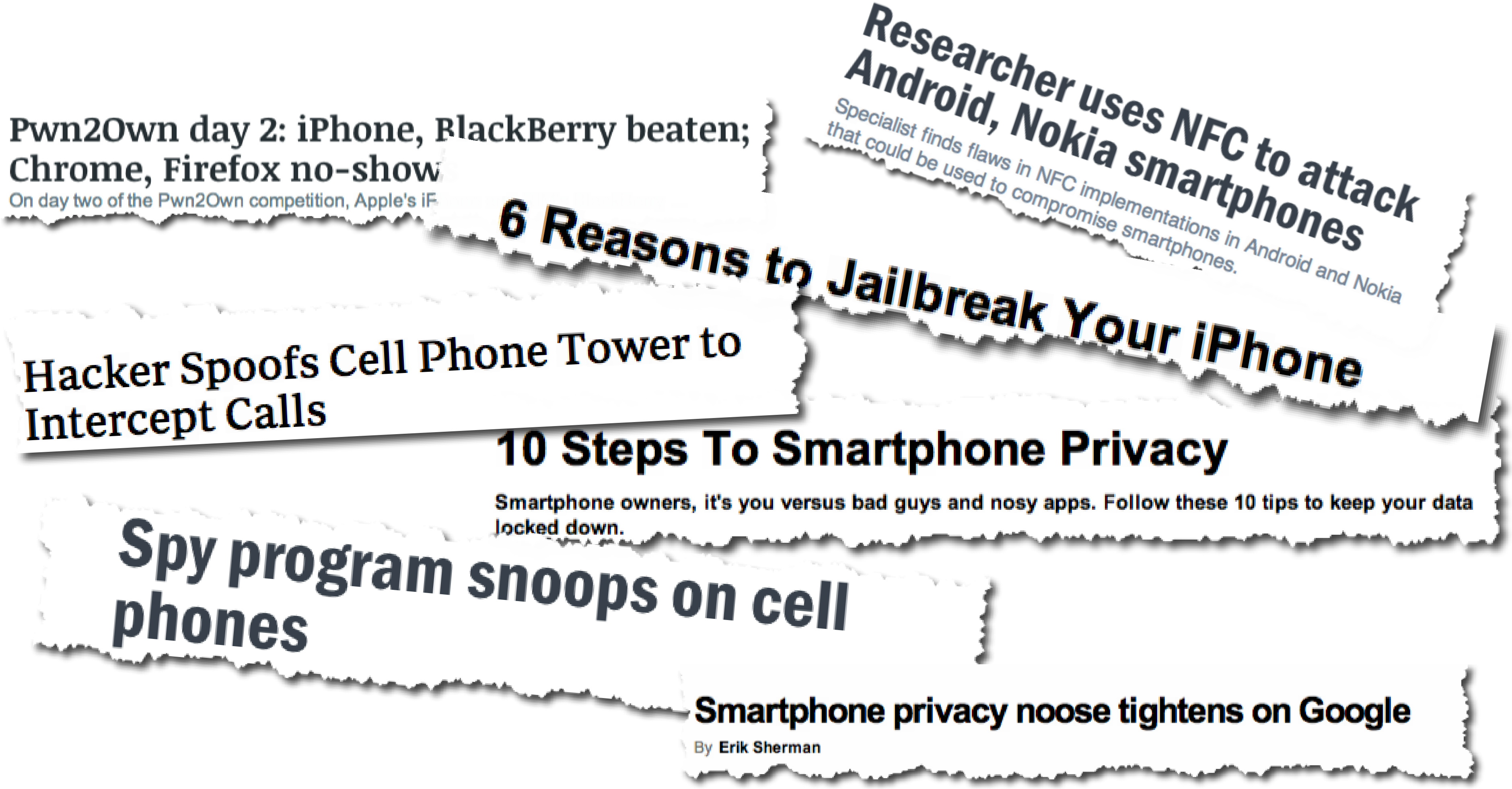
1. The Problem
2. Threat Landscape
3. Mobile Ecosystem
4. The Fix

The Problem

1

What Are The Risks

Define the Threats



Pwn2Own day 2: iPhone, BlackBerry beaten; Chrome, Firefox no-show

On day two of the Pwn2Own competition, Apple's iF

Researcher uses NFC to attack Android, Nokia smartphones

Specialist finds flaws in NFC implementations in Android and Nokia that could be used to compromise smartphones.

6 Reasons to Jailbreak Your iPhone

Hacker Spoofs Cell Phone Tower to Intercept Calls

10 Steps To Smartphone Privacy

Smartphone owners, it's you versus bad guys and nosy apps. Follow these 10 tips to keep your data locked down.

Spy program snoops on cell phones

Smartphone privacy noose tightens on Google

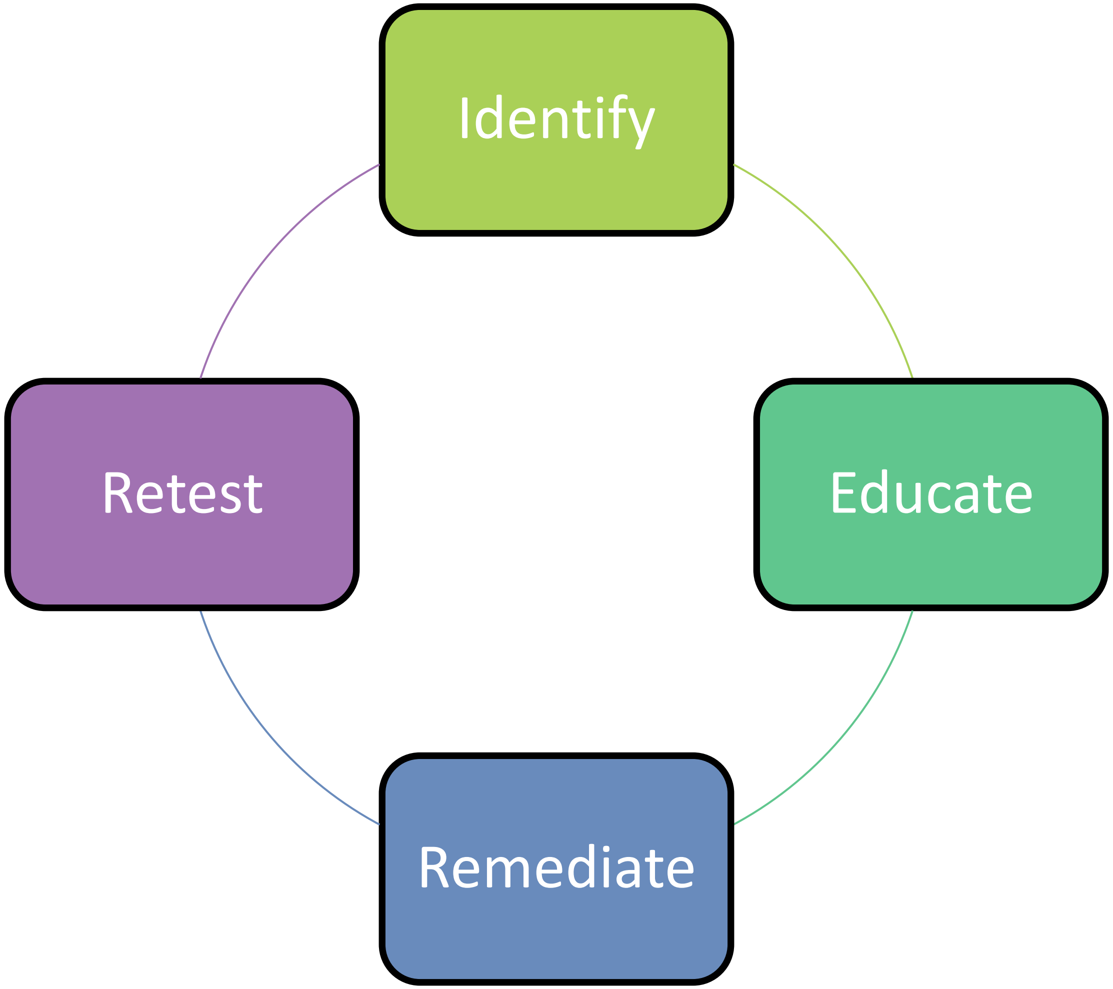
By Erik Sherman

Securing the SDLC

The Developer View

Priorities

1. Vulnerabilities
2. Capabilities
3. Malware



Moving Into The Enterprise

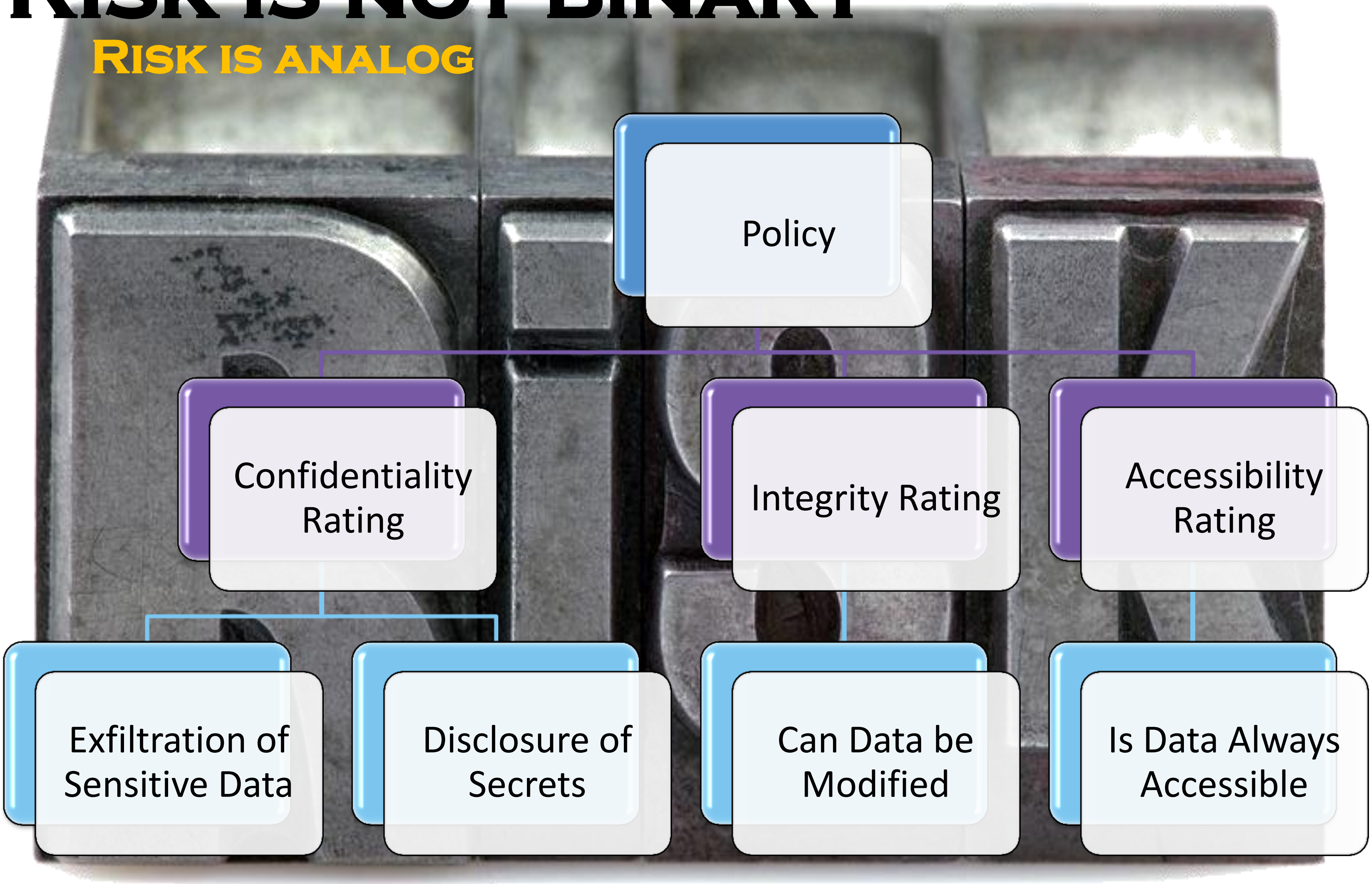
Bring Your Own Device

Priorities

1. Malware
2. Capabilities
3. Vulnerabilities

Risk is not binary

Risk is analog



Policy

Confidentiality Rating

Integrity Rating

Accessibility Rating

Exfiltration of Sensitive Data

Disclosure of Secrets

Can Data be Modified

Is Data Always Accessible

Mobile Crossroads

The Inflection Point

Do you trust the security of your mobile device…

63%

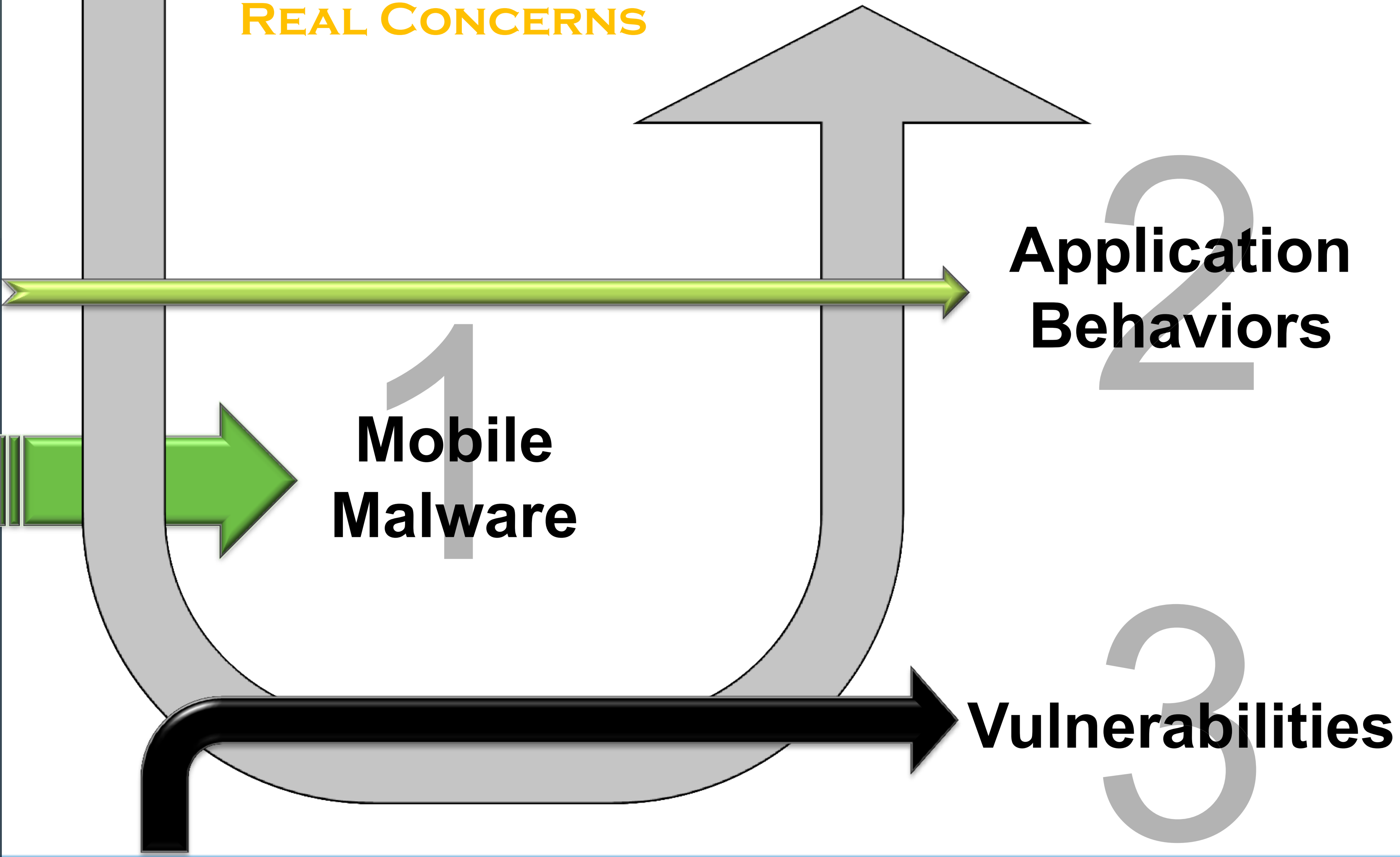
Have yet to make up their minds

Threat Landscape

2

The Mobile Threat Landscape

Real Concerns



1 Mobile Malware

2 Application Behaviors

3 Vulnerabilities

Mobile Malware

The Perfect Storm

Mobile Networks

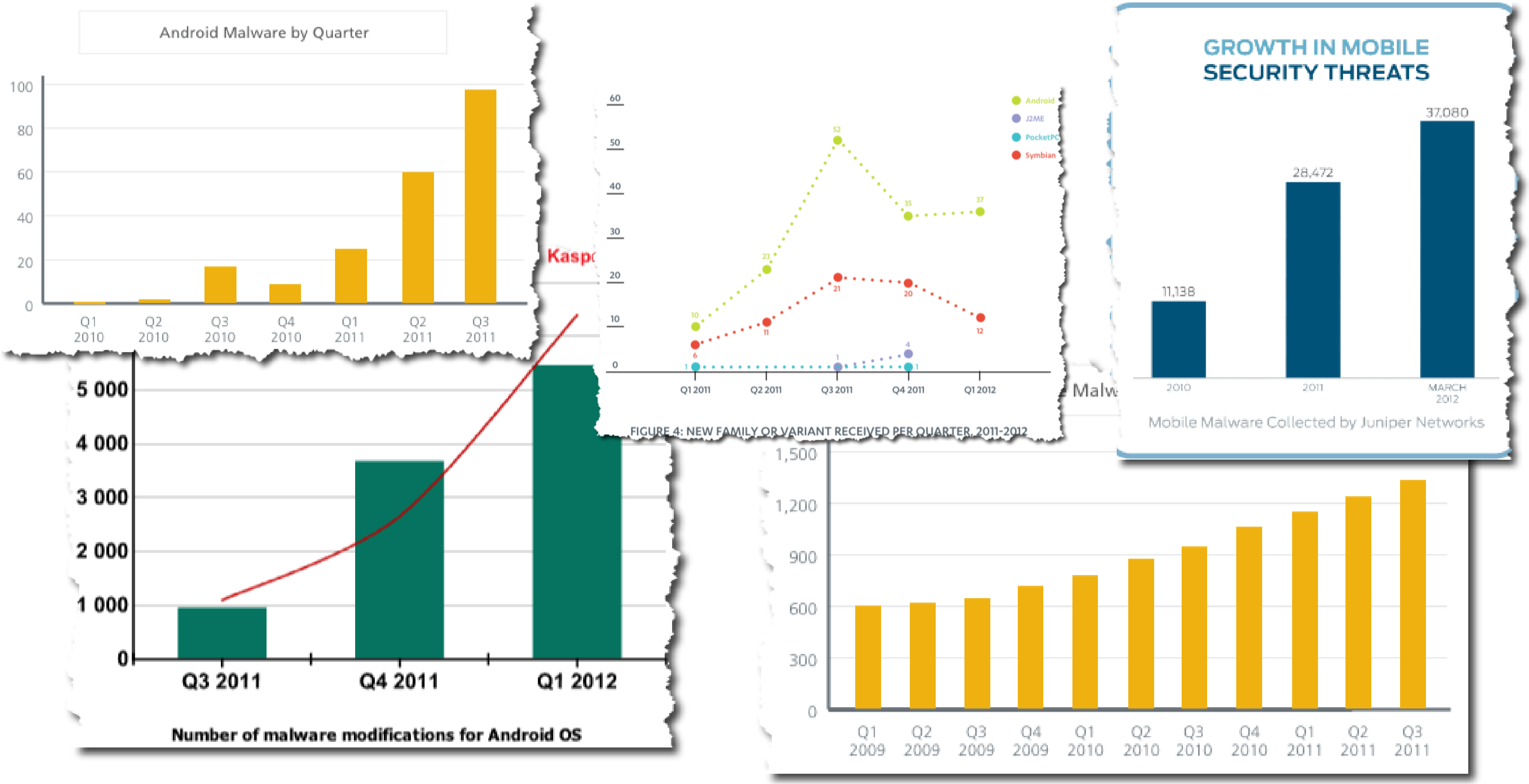
Decentralized
Interconnected
Mobile
Quick Content
Retrieval

Perfect Malware

Decentralized
Interconnected
Mobile
Quick Content Retrieval

Statistics

Yeah Yeah Yeah…



Android Malware by Quarter

Number of malware modifications for Android OS

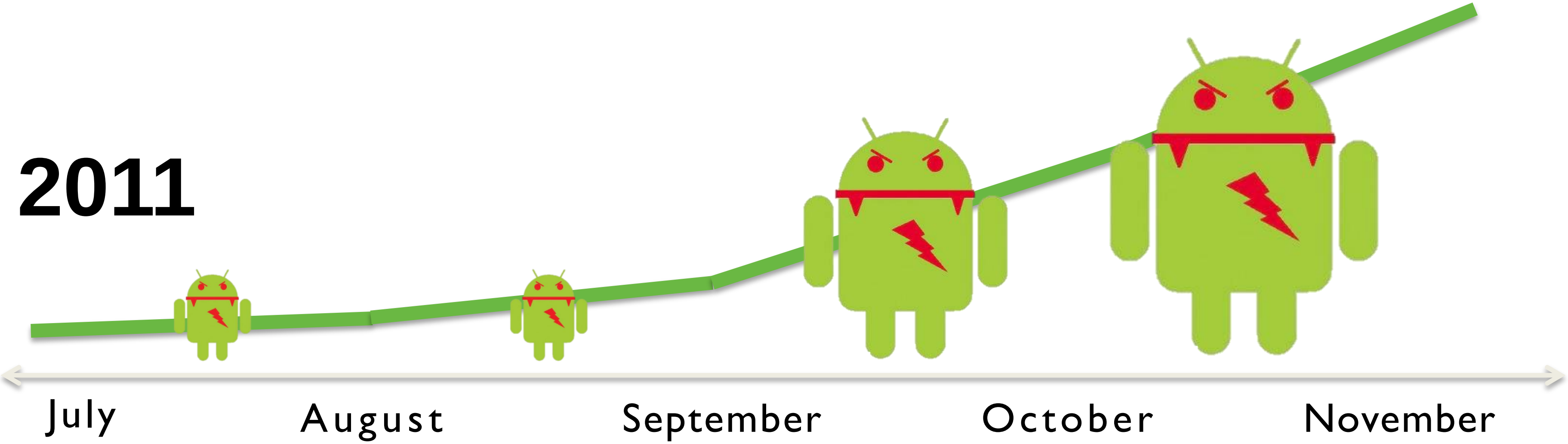
FIGURE 4: NEW FAMILY OR VARIANT RECEIVED PER QUARTER, 2011-2012

GROWTH IN MOBILE SECURITY THREATS

Mobile Malware Collected by Juniper Networks

Malware Timeline

Exponential Growth



Early to the Game

Malware Wave Begins

Exponential Growth

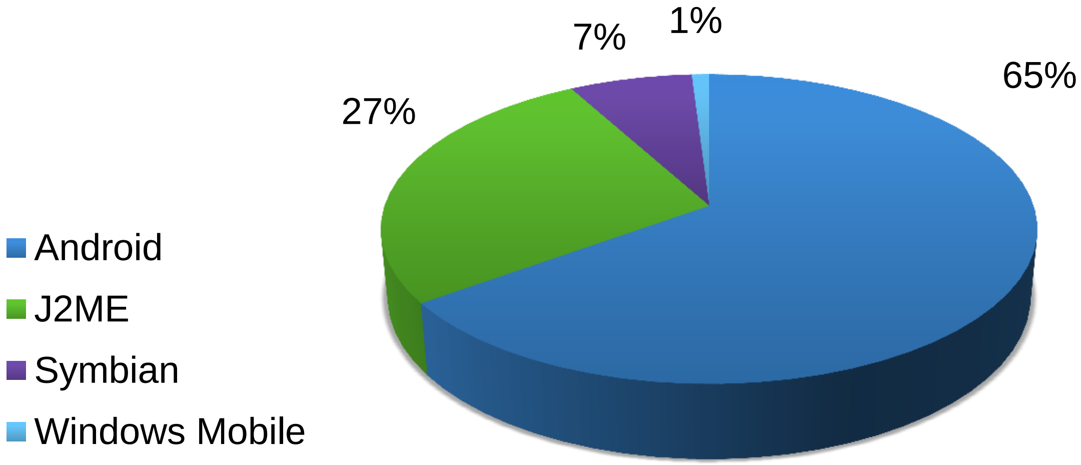
PRIMARY TARGET

WHO GETS TARGETED?

Android Most Targeted (65%)
iOS Absent (<1%)

WHY

- Closed Technology
- Harder to Reverse Engineer
- Stronger OS Security
- Better App Store Security
- No Fragmentation Issue



Distribution of Mobile Threats by Platform 2011

Mobile Malware

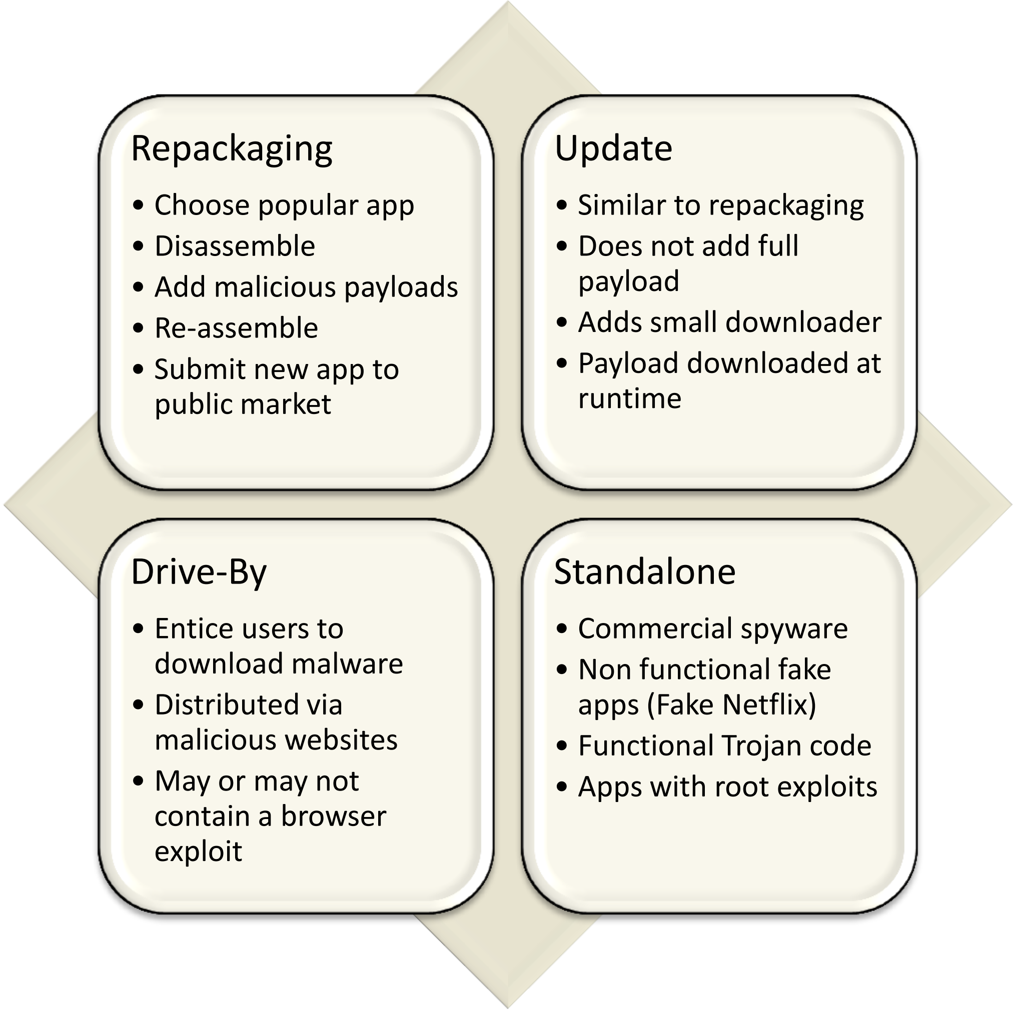
Infection Vectors

86%

7%

<1%

14%



Repackaging

- Choose popular app
- Disassemble
- Add malicious payloads
- Re-assemble
- Submit new app to public market

Update

- Similar to repackaging
- Does not add full payload
- Adds small downloader
- Payload downloaded at runtime

Drive-By

- Entice users to download malware
- Distributed via malicious websites
- May or may not contain a browser exploit

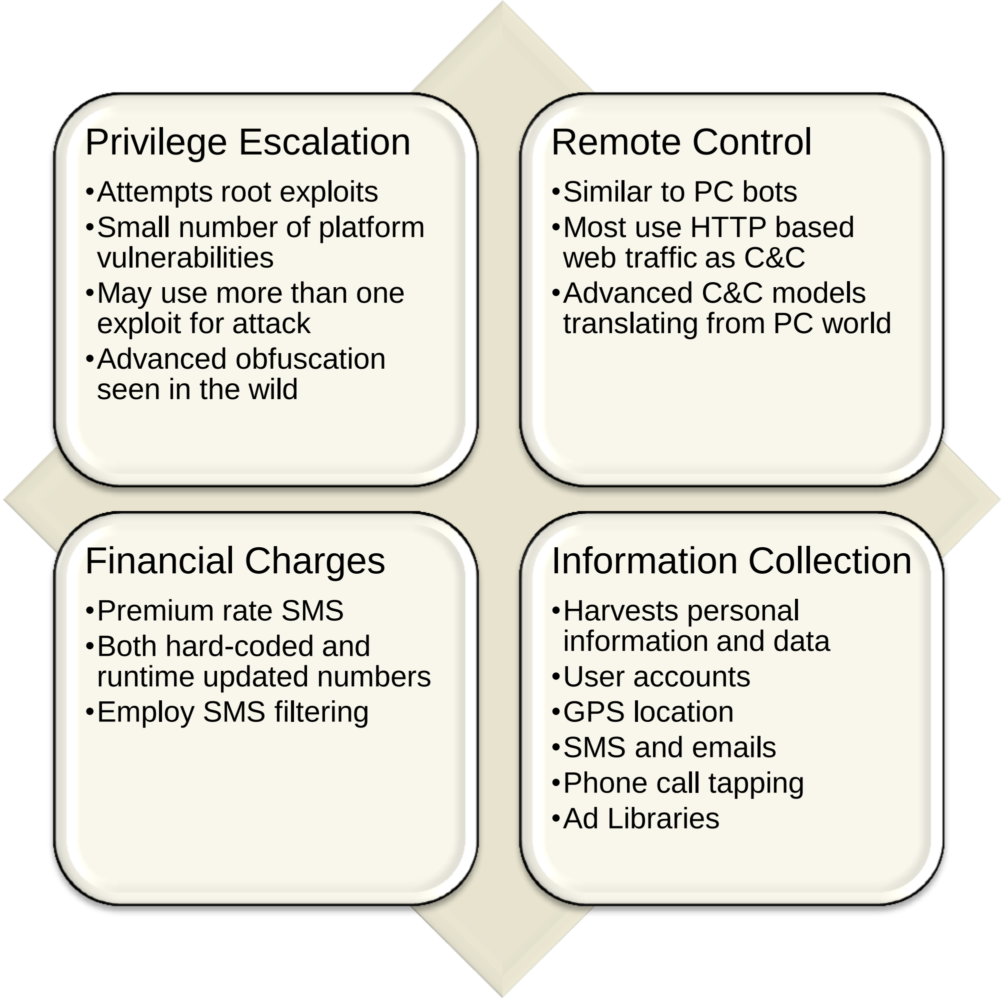
Standalone

- Commercial spyware
- Non functional fake apps (Fake Netflix)
- Functional Trojan code
- Apps with root exploits

Mobile Malware

Malicious payloads

37%



Privilege Escalation

- Attempts root exploits
- Small number of platform vulnerabilities
- May use more than one exploit for attack
- Advanced obfuscation seen in the wild

Remote Control

- Similar to PC bots
- Most use HTTP based web traffic as C&C
- Advanced C&C models translating from PC world

93%

45%
SMS

Financial Charges

- Premium rate SMS
- Both hard-coded and runtime updated numbers
- Employ SMS filtering

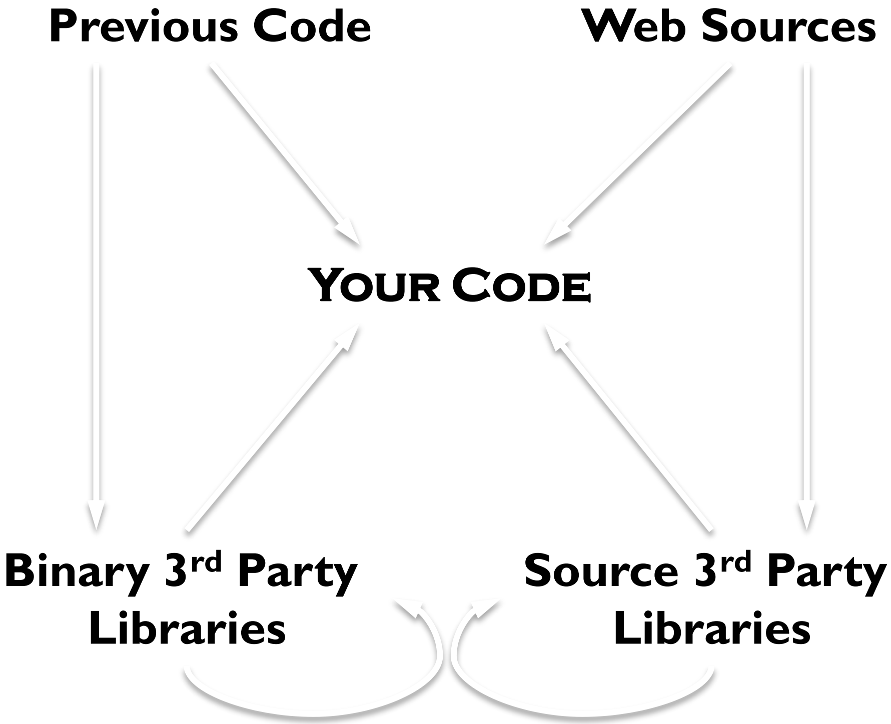
Information Collection

- Harvests personal information and data
- User accounts
- GPS location
- SMS and emails
- Phone call tapping
- Ad Libraries

45%
Phone Number

Application Behaviors

Code reuse and you



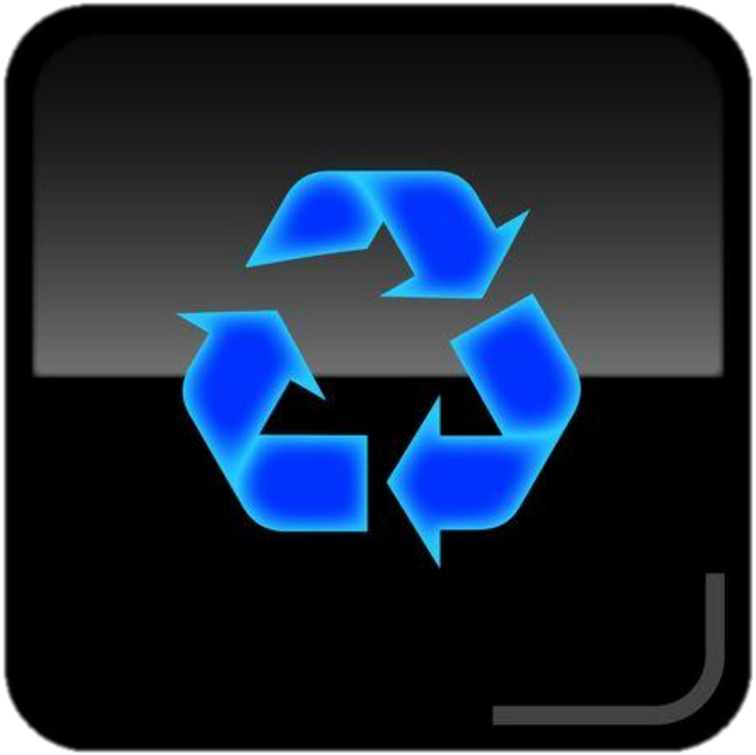
Previous Code

Web Sources

Your Code

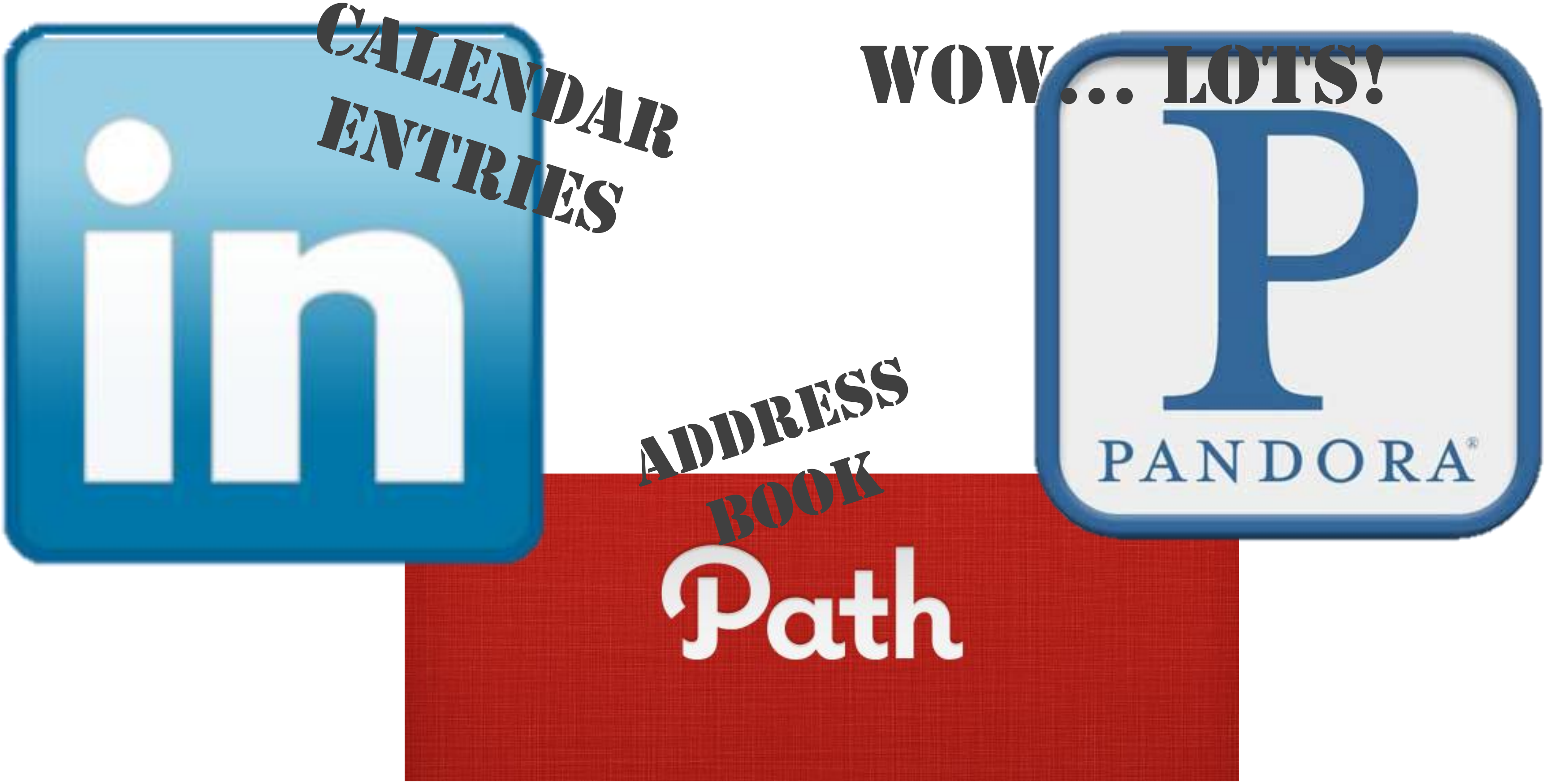
Binary 3rd Party Libraries

Source 3rd Party Libraries



Case studies

Problems in the wild



CALENDAR ENTRIES

WOW… LOTS!

ADDRESS BOOK

Vulnerabilities

Common Code Flaws

- Sensitive data leakage (inadvertent or side channel)
- Unsafe sensitive data storage
- Unsafe sensitive data transmission
- Hardcoded password/keys

Vulnerabilities

Language Inheritance

- Layered APIs on common languages
- Blackberry and Android use Java as a base
- Non-issue for Objective-C (it's own language)

Mobile Ecosystem

3

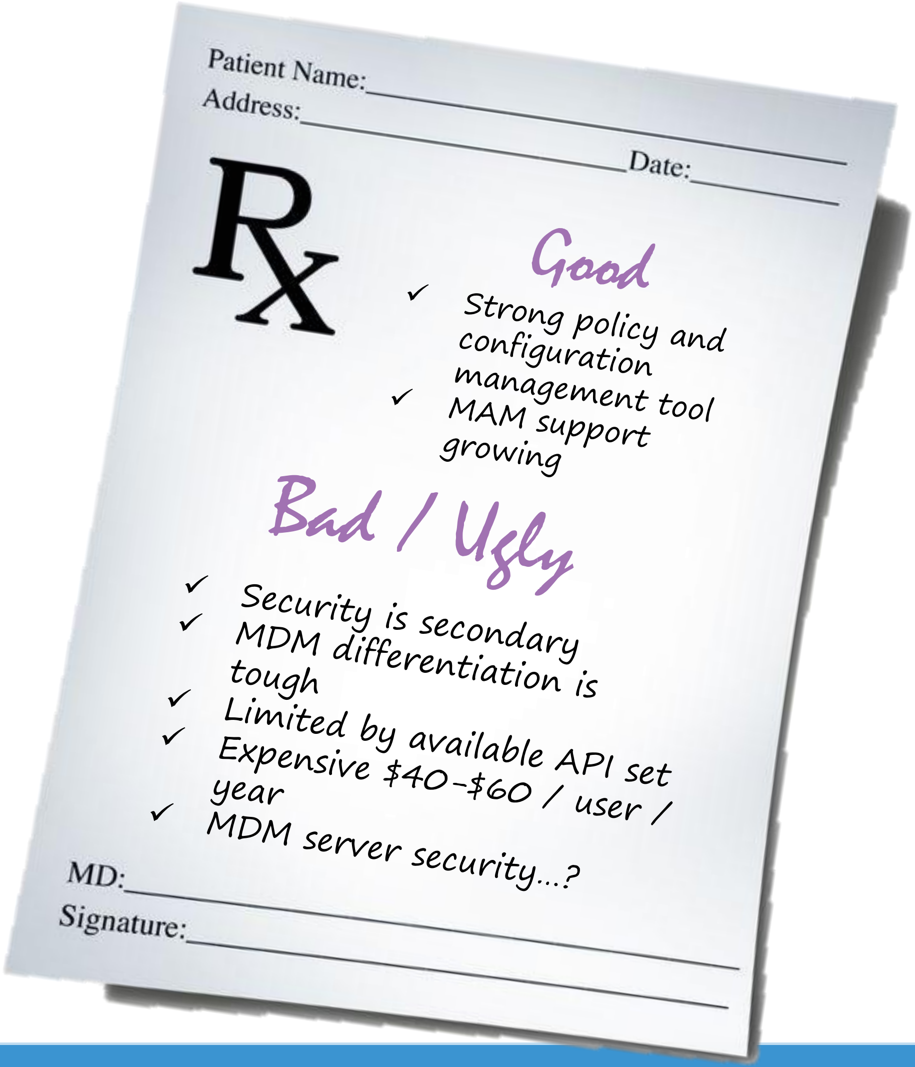
The Mobile Ecosystem

The Players of the Game

Consumer
Public App Stores
MDM Vendors
Enterprise App Stores
Anti-Virus Vendors

MDM Vendors

The Enterprise Choke Point



Patient Name:

Address:

Date:

Rx

Good

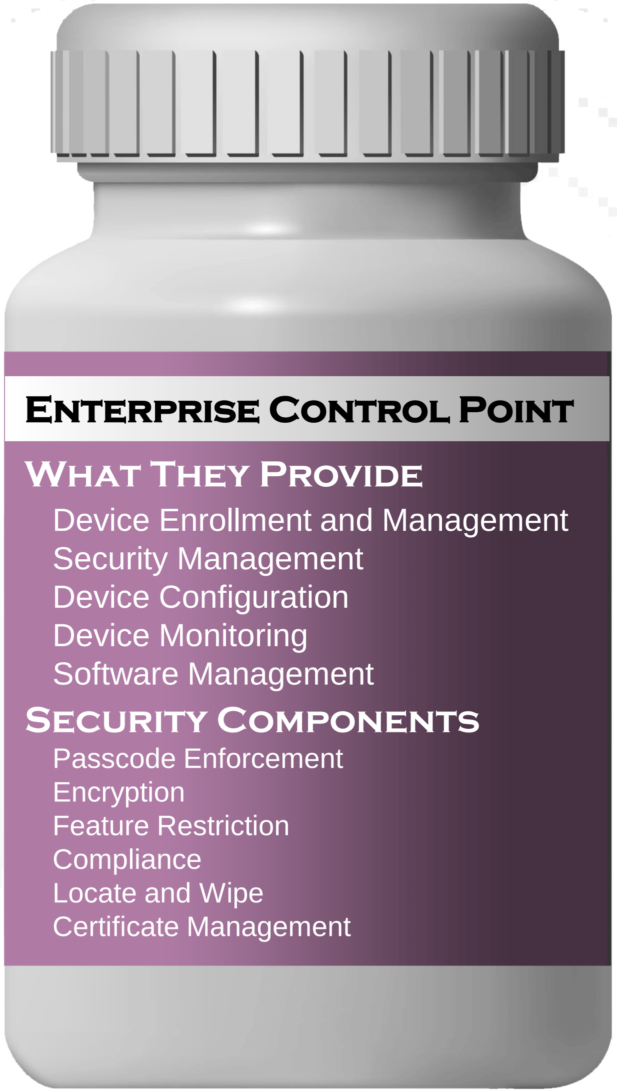
- ✓ Strong policy and configuration management tool
- ✓ MAM support growing

Bad / Ugly

- ✓ Security is secondary
- ✓ MDM differentiation is tough
- ✓ Limited by available API set
- ✓ Expensive $40-$60 / user / year
- ✓ MDM server security…?

MD:

Signature:



Enterprise Control Point

What They Provide

- Device Enrollment and Management
- Security Management
- Device Configuration
- Device Monitoring
- Software Management

Security Components

- Passcode Enforcement
- Encryption
- Feature Restriction
- Compliance
- Locate and Wipe
- Certificate Management

Mobile Anti-Virus

Old Methods Rehashed

Patient Name:

Address:

Date:

Rx

Good

- ✓ Catching known malware
- ✓ Awesome at killing battery life

Bad / Ugly

- ✓ Inability to catch anything unknown
- ✓ Repeat failure – PC space
- ✓ Persistent resource issues
- ✓ Often highly privileged apps
- ✓ "One bug to rule them all"

MD:

Signature:

Old Methods Rehashed

What They Provide

Quarantine and Eradicate Malware

Signature Based Analysis

Security Components

Cloud Analysis

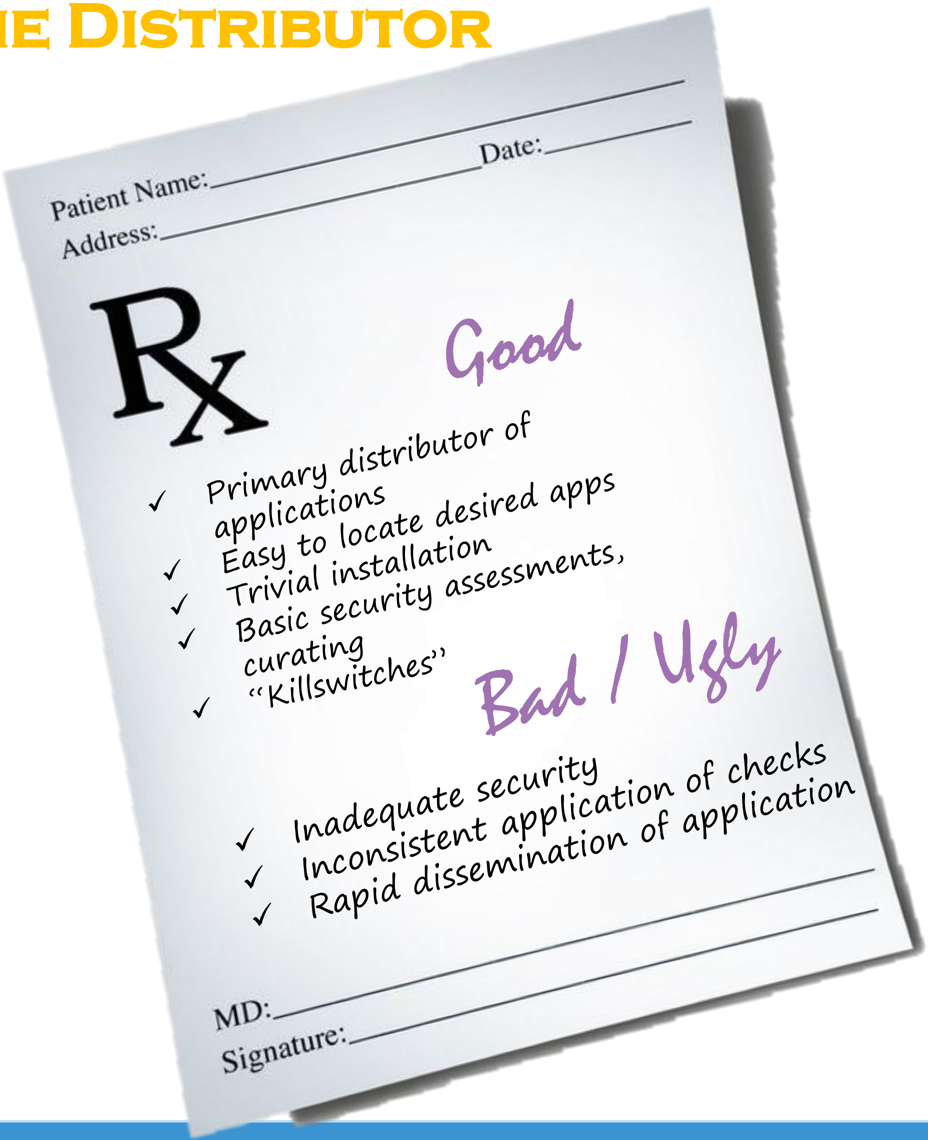
Spam Filtering

Email Attachment Scanning

Data Backup

Application Markets

The Distributor



Patient Name:

Address:

Date:

Rx

Good

- ✓ Primary distributor of applications
- ✓ Easy to locate desired apps
- ✓ Trivial installation
- ✓ Basic security assessments, curating
- ✓ "Killswitches"

Bad / Ugly

- ✓ Inadequate security
- ✓ Inconsistent application of checks
- ✓ Rapid dissemination of application

MD:

Signature:

The Distributor

What They Provide

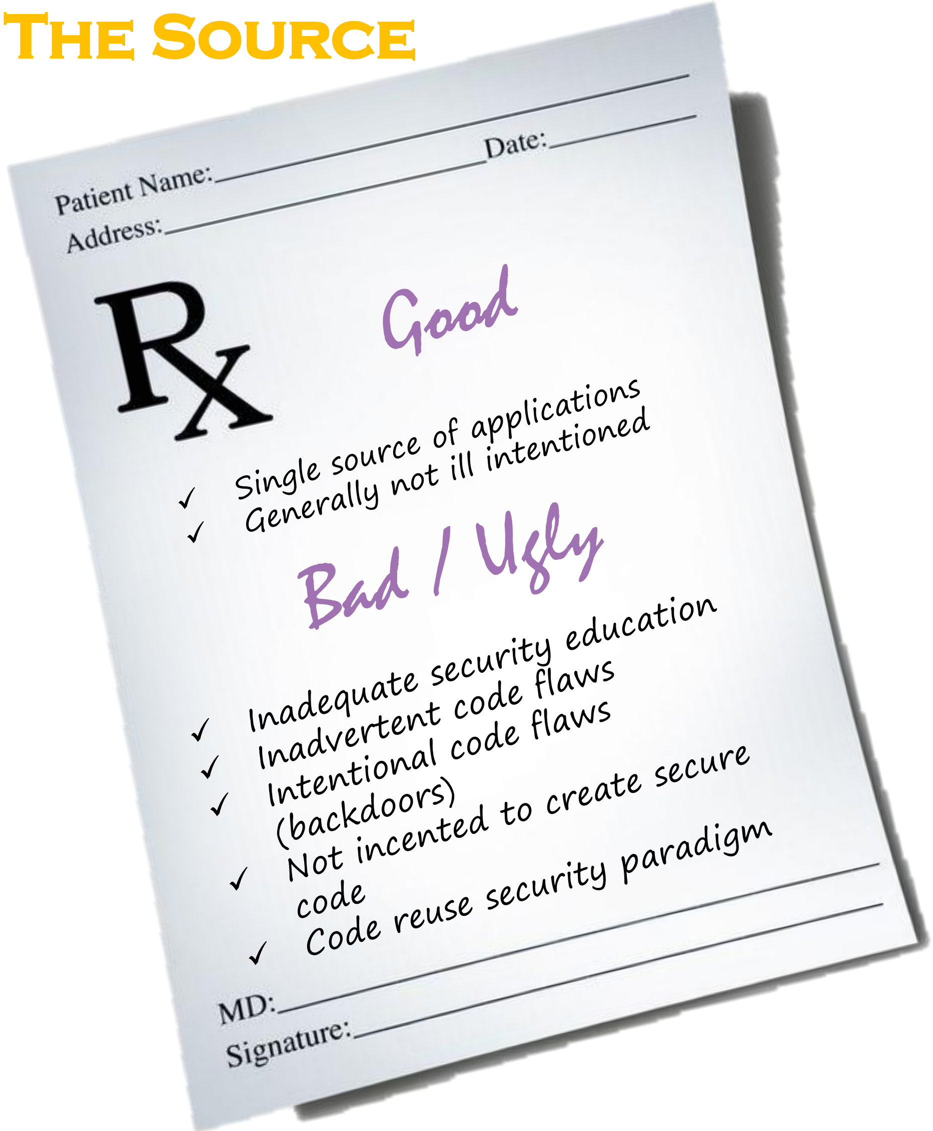
Marketplace for Applications
User Ratings
Application Updates

Security Components

Application Approval Process
Android Bouncer
iOS Scanning

Developers

The Source



Patient Name:
Date:
Address:

℞

Good

- ✓ Single source of applications
- ✓ Generally not ill intentioned

Bad / Ugly

- ✓ Inadequate security education
- ✓ Inadvertent code flaws
- ✓ Intentional code flaws (backdoors)
- ✓ Not incented to create secure code
- ✓ Code reuse security paradigm

MD:
Signature:

The Source

What They Provide

Enterprise Application Development
Consumer Application Development
Cross-platform Expertise

Security Components

Variable on Developer Capabilities

The Fix

4

The Fix

Securing Against Multiple Threats

Behavioral Analysis

Malware Detection

Vulnerability Analysis

Static Behavioral Analysis

Features and Permissions

User Facing

Data Sources

- Location Data
- Contacts
- Email
- SMS Data
- SQL Access
- File System
- Photos
- Phone ID Values

Data Sinks

- HTTP Requests
- Outbound SMS
- Outbound Email
- DNS Requests
- TCP
- UDP
- Vulnerable Code

Mapping

- Trace Sources to Sinks
- Application "Intent"
- Permission Mapping
- Human Intelligence

Code Flow

Data Flow

Dynamic Behavioral Analysis

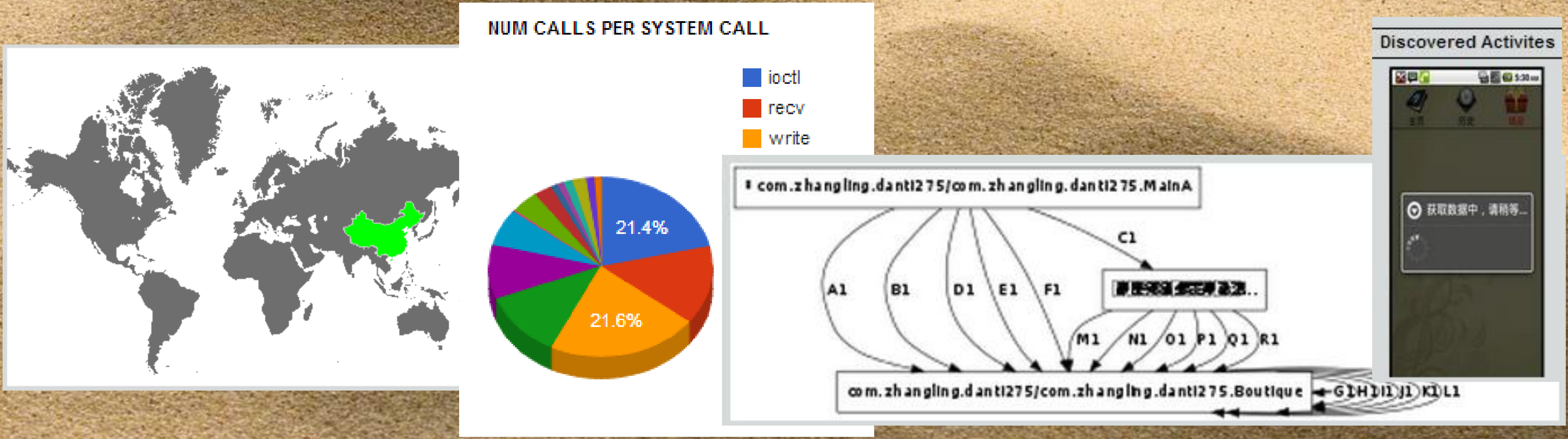
Playing in the Sandbox

Instrumented Analysis

- Sandboxed Emulator
- Instrumented Fuzzy Logic Inputs
- Tracked Outputs
- Tracked System State

Example Data Gathered

- Network Traffic
- CPU Utilization
- Memory Footprint
- Mapping Screen to Functionality



Malware Detection

Learn From Previous Mistakes

Signatures
Signatures
Signatures

Basic Heuristics

Static Analysis

Human Intelligence

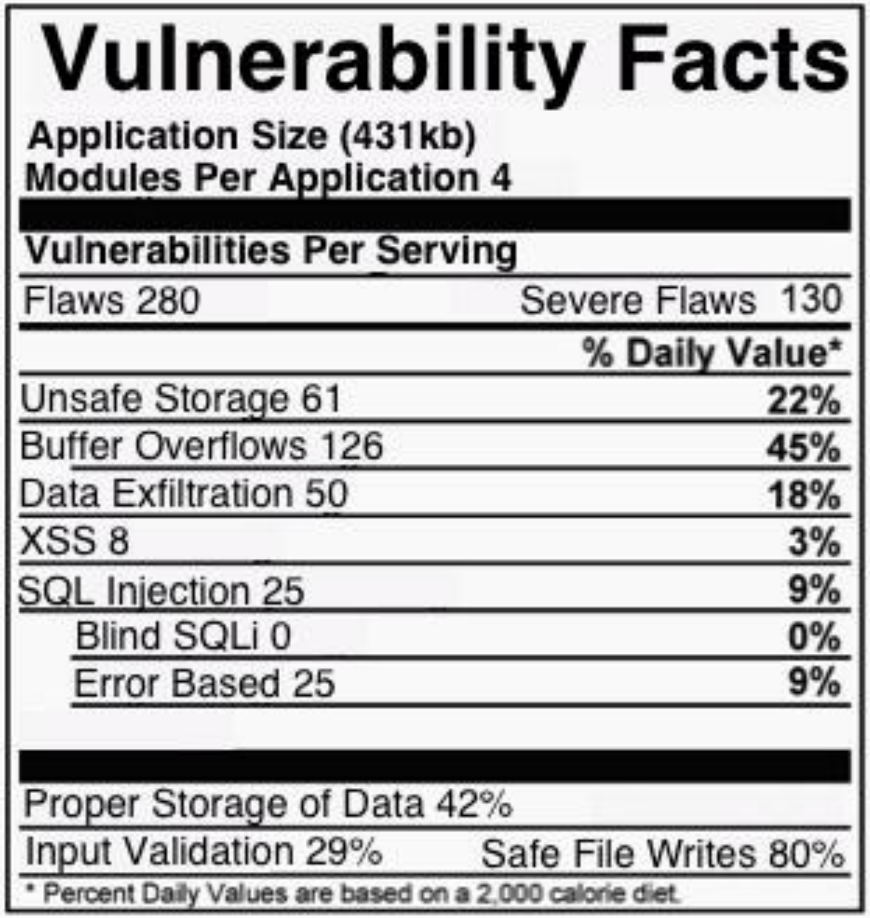
Dynamic Analysis

Vulnerability Analysis

Find the Flaws

Environmental Flaws

Application Flaws



Vulnerability Facts

Application Size (431kb)
Modules Per Application 4

Vulnerabilities Per Serving

Flaws 280	Severe Flaws 130
	% Daily Value*
Unsafe Storage 61	**22%**
Buffer Overflows 126	**45%**
Data Exfiltration 50	**18%**
XSS 8	**3%**
SQL Injection 25	**9%**
Blind SQLi 0	**0%**
Error Based 25	**9%**

Proper Storage of Data 42%

Input Validation 29% Safe File Writes 80%

* Percent Daily Values are based on a 2,000 calorie diet.

Strategic Control Points

Security and Power

- Application Markets
- MDM
- Anti-Virus
- Enterprise

Enterprise Developers

Consumer Developers

Outsourced Developers

COTS Developers

… Developers

Enterprise Fixes

De-Risk B.Y.O.D

Policy

Process

Technical Controls

The Road Ahead

Where do we go from here?

Capabilities Mapping + Malware Detection + Vulnerability Analysis = A Safer Mobile Path

Sources

Show me the data

@txs

tshields@veracode.com

- http://www.juniper.net/us/en/local/pdf/additional-resources/7100155-en.pdf
  Juniper Network Trusted Mobility Index
- http://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/History-of-Mobile-Malware.pdf
  A History of Malware – Trend Micro
- http://www.cs.berkeley.edu/~afelt/felt-mobilemalware-spsm.pdf
  A Survey of Mobile Malware In The Wild – UC Berkeley
- http://www.securelist.com/en/analysis/204792222/Mobile_Malware_Evolution_Part_5
  Mobile Malware Evolution Part 5 – Kaspersky Labs
- http://www.csc.ncsu.edu/faculty/jiang/pubs/OAKLAND12.pdf
  Dissecting Android Malware: Characterization and Evolution – Yajin Zhou and Xuxian Jiang
- http://www.fiercemobilecontent.com/story/apples-new-ios-6-adds-deep-facebook-integration-dumps-google-maps/2012-06-11
  Apple's new iOS 6 adds deep Facebook integration, dumps Google Maps
- http://www.net-security.org/secworld.php?id=13050
  LinkedIn Privacy Fail
- http://www.trailofbits.com/resources/mobile_eip_2.pdf
  Mobile Exploit Intelligence Project – Trail of Bits
- http://www.net-security.org/secworld.php?id=12418
  Social Mobile Apps Found Storing User's Content Without Permission

- And More…. Contact me if you need something specific I may have left out…