Priorities for Securing the Mobile Ecosystem
Qualcomm Mobile Security Summit

Marc Kolaks
Patrick McCanna
AT&T Mobile Endpoint Security

Formed ~ 2010 to focus solely on:

- Devices in our portfolio
- Apps (Owned, Licensed, Preloaded, Internal (enterprise) or of interest because of potential impact (e.g. use of network resources)

By 2012, we found that a lot of bandwidth of our pre-launch team was following up on post-launch threats, so we formed a dedicated Mobile Endpoint Threat team

Now – we are seeing other pressures to change our approach...
Complexity

Over 1050 Unique Devices on Network

Over 750 stock and non-stock devices approved in 2016

Over 150 Unique Chipsets

Dozens of Chipset Providers

3 flavors of cellular technologies: GSM, UMTS, LTE

Radios supporting 22 different cellular bands across 2G/3G/4G and EDGE, GPRS, GSM, HSDPA, HSPA+, HSUPA, LTE, MBMS, UTMS

8 flavors of Wi-Fi, ANT/ANT+

4 types of Bluetooth

NFC

FM Radio with RDS data capability

GLONASS, GPS

Sensors for Fingerprint, accelerometer, gyro, proximity, compass, barometer, ambient light, RGB, geomagnetic, ...

Messaging via SMS, MMS, Email, Push Mail

Audio/Video Processing supporting MP4, DivX, xVid, WMV, H2.64, MP3, WAV, WMA, eAAC+ and FLAC

OS with over 12 Million lines of code

300 stock applications and almost 100 device features that call over 60 3rd party libraries supporting over 2 million 3rd party applications from official app sources

Oh – and two cameras

Over 1050 Unique Devices on Network

Over 150 Unique Chipsets

Dozens of Chipset Providers

3 flavors of cellular technologies: GSM, UMTS, LTE

Radios supporting 22 different cellular bands across 2G/3G/4G and EDGE, GPRS, GSM, HSDPA, HSPA+, HSUPA, LTE, MBMS, UTMS

8 flavors of Wi-Fi, ANT/ANT+

4 types of Bluetooth

NFC

FM Radio with RDS data capability

GLONASS, GPS

Sensors for Fingerprint, accelerometer, gyro, proximity, compass, barometer, ambient light, RGB, geomagnetic, ...

Messaging via SMS, MMS, Email, Push Mail

Audio/Video Processing supporting MP4, DivX, xVid, WMV, H2.64, MP3, WAV, WMA, eAAC+ and FLAC

OS with over 12 Million lines of code

300 stock applications and almost 100 device features that call over 60 3rd party libraries supporting over 2 million 3rd party applications from official app sources

Oh – and two cameras

Over 1050 Unique Devices on Network

Over 150 Unique Chipsets

Dozens of Chipset Providers

3 flavors of cellular technologies: GSM, UMTS, LTE

Radios supporting 22 different cellular bands across 2G/3G/4G and EDGE, GPRS, GSM, HSDPA, HSPA+, HSUPA, LTE, MBMS, UTMS

8 flavors of Wi-Fi, ANT/ANT+

4 types of Bluetooth

NFC

FM Radio with RDS data capability

GLONASS, GPS

Sensors for Fingerprint, accelerometer, gyro, proximity, compass, barometer, ambient light, RGB, geomagnetic, ...

Messaging via SMS, MMS, Email, Push Mail

Audio/Video Processing supporting MP4, DivX, xVid, WMV, H2.64, MP3, WAV, WMA, eAAC+ and FLAC

OS with over 12 Million lines of code

300 stock applications and almost 100 device features that call over 60 3rd party libraries supporting over 2 million 3rd party applications from official app sources

Oh – and two cameras

Over 1050 Unique Devices on Network

Over 150 Unique Chipsets

Dozens of Chipset Providers

3 flavors of cellular technologies: GSM, UMTS, LTE

Radios supporting 22 different cellular bands across 2G/3G/4G and EDGE, GPRS, GSM, HSDPA, HSPA+, HSUPA, LTE, MBMS, UTMS

8 flavors of Wi-Fi, ANT/ANT+

4 types of Bluetooth

NFC

FM Radio with RDS data capability

GLONASS, GPS

Sensors for Fingerprint, accelerometer, gyro, proximity, compass, barometer, ambient light, RGB, geomagnetic, ...

Messaging via SMS, MMS, Email, Push Mail

Audio/Video Processing supporting MP4, DivX, xVid, WMV, H2.64, MP3, WAV, WMA, eAAC+ and FLAC

OS with over 12 Million lines of code

300 stock applications and almost 100 device features that call over 60 3rd party libraries supporting over 2 million 3rd party applications from official app sources

Oh – and two cameras
Priorities for Securing the Mobile Ecosystem

Creates pressure (and reasons) to reduce pre-launch security reviews

Industry Improvements
- OS’s getting better
- OEMs getting better
- Research getting better
- Crowdsourced Research - BugBounty

Move focus from Pre-Launch to better supporting Post-Launch

Reduced product launch cycle

- Over 750 stock and non-stock devices approved in 2016
- Over 1050 Unique Devices on Network
- Over 150 Unique Chipsets

Supporting over 2 million 3rd party applications from official app sources

OS with over 12 million lines of code

300 stock applications and almost 100 device features that call over 60 3rd party libraries

Research getting better
Crowdsourced Research - BugBounty

© 2017 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
Priorities for Securing the Mobile Ecosystem

We need to adjust the pre-launch cycle for better post-launch threat response

How do we better respond to post launch threat?

By transitioning some of our pre-launch activities from assessment to gathering as much information as we can about the devices, building an inventory of these attributes and continuing to work with the industry to improve response to issues.
Priorities for Securing the Mobile Ecosystem

Pre-launch testing: old model

- Device Security
  - Testing, Preload app assessment
- Vendor Interaction
- Publicly Reported Info

Device attribute
- Data Collection

Resource Consumption

Pre-Launch

Post-Launch
New approach

- Device Attribute
  - Data Collection
  - Device Security Testing, Preload app assessment
- Vendor Interaction
  - Bug Bounty/Security Researchers
- Pre-Launch
- Post-Launch

Resource Consumption
Mobile Threat Priorities
Why Threat Priorities?
Priorities for Securing the Mobile Ecosystem

Threat Priorities

- Malicious Mobile App
- Man in the Middle
- Insecure Mobile App
- Messaging Attacks
- Phishing
- Browser Exploitation
- Baseband Exploitation
- Vulnerable Web App Usage
Malicious Mobile Apps
Malicious Mobile Apps

Malicious Mobile Apps perform unauthorized actions or steal information.

For example, they steal passwords, photos or location information about the victim.

Consumer:
• Safe App Sources
• Platform Controls
• Mobile A/V

Enterprise:
• Secure Ent. App Stores
• EMM

OEMs:
• Evaluate Alternative Appstore Strategies

MNOs:
• Flow Identification for Malware traffic
• Messaging

Platform:
• Intent Security
Priorities for Securing the Mobile Ecosystem

Man In The Middle
## Man In The Middle

### Threat

A man-in-the-middle attack is a situation where a hacker can intercept network traffic to inspect or modify network traffic (e.g. login) in order to compromise into a mobile or workstation.

### Countermeasures

**Consumer:**
- VPNs
- Education (Browser Security, App Security Risks)

**Enterprise:**
- VPNs
- Cert Pinning
- Unit Testing for Invalid Certs

### Opportunities

**OEMs:**
- Better native VPN Support

**Platform:**
- Appstore detection of invalid certs
- Explore TLS policy for apps
Priorities for Securing the Mobile Ecosystem

Insecure Mobile Applications
### Insecure Mobile Apps

**Threat**

Well-meaning, authentic applications that are easy for hackers to compromise.

The user's application data & usage may be inadequately protected or the application’s vulnerabilities may be useful in obtaining access to a victim's device.

**Countermeasures**

**Consumer:**
- Breach notification services
- Valid app store sources
- Avoid rooting

**Enterprise:**
- Static & dynamic analysis
- App security testing against a rooted, pre 4.1 environment
- Don’t over-depend on platform controls

**Opportunities**

**OEMs:**
- Consumer Education

**Platform:**
- Consumer Education
Messaging Attacks
## Messaging Attacks

### Messaging Attacks
Messaging attacks compromise the handset through maliciously crafted SMS or Over The Top Messaging

Developers frequently don't know that malicious SMS messages can be used to interrogate a device.

### Countermeasures

**Consumer:**
- Device & Software Updates
- Anti-Malware Apps

**Enterprise:**
- Developer Education

### Opportunities

**OEMs:**
- Security-oriented fuzz testing of messaging client implementation

**Platform:**
- CTS tests for SMS security?
Priorities for Securing the Mobile Ecosystem

Browser Exploitation
## Browser Exploitation

**Threat**

Browser threats occur when a victim accesses a website that tampers with browser behavior. They exploit the web browser: chrome, safari, firefox, IE, explorer, etc.

### Consumer:
- Browser Based Guidance
- Apply OS updates
- Apply all browser updates
- Consider anti-malware apps

### Enterprise:
- Web Proxies

### OEMs:
- Keep executing on software updates
- Be careful with web-bluetooth

### Platform:
- Keep executing on webview updates
- Keep executing on Chrome Safe Browsing
Phishing
### Phishing

**Phishing** is the act of masquerading as a trustworthy person or service and sending a message to a victim that entices them to disclose private data.

Could be SMS, OTT Messaging, Email or other approaches

<table>
<thead>
<tr>
<th>Threat</th>
<th>Countermeasures</th>
<th>Opportunities</th>
</tr>
</thead>
</table>

**Consumer:**
- Education

**Enterprise:**
- Education

**OEMs:**
- Education

**Platform:**
- Education
Vulnerable Web App Usage
## Vulnerable Web App Usage

Vulnerable web apps are the reason most consumers get hacked. The consumer does nothing wrong.

A service the mobile user depends upon is compromised. In an exploit, Mobile Apps installed on the device send information to compromised service.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Countermeasures</th>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerable Web App Usage</strong></td>
<td><strong>Consumer:</strong></td>
<td><strong>OEMs:</strong></td>
</tr>
<tr>
<td></td>
<td>• Breach Notification Services</td>
<td>• N/A</td>
</tr>
<tr>
<td></td>
<td><strong>Enterprise:</strong></td>
<td><strong>Platform:</strong></td>
</tr>
<tr>
<td></td>
<td>• Breach Notification Services</td>
<td>• N/A</td>
</tr>
</tbody>
</table>
Baseband Exploitation
**Baseband Exploitation**

Baseband exploits are sophisticated attacks that target the radio of a mobile device.

Baseband exploits should generally be considered in the realm of "APT." Most likely to be applied to target VIPs

**Consumer:**
- OS Updates
- 2G Disablement Switch*

**Enterprise:**
- OS updates
- Boutique devices

* (Where available)

**OEMs:**
- Security Fuzz testing of radios
- Keep executing on OS updates

**Platform:**
- Keep executing on OS updates
Additional Perspectives

NIST Mobile Threat Catalogue:
https://pages.nist.gov/mobile-threat-catalogue/

MITRE ATTACK (Adversarial Tactics, Techniques & Common Knowledge)
https://attack.mitre.org/wiki/Main_Page

NIAP device security protection profile:
https://www.niap-ccevs.org/Profile/Info.cfm?id=381
Questions?

Marc.kolaks@att.com
Patrick.mccanna@att.com

@patrickmccanna