Making the Android ecosystem safer

Adrian Ludwig
Director, Android Security
Payment Received
Google Maps is putting Europe's human-traffickers out of business

Mass migration guided by mobiles and social media

Photograph: Herbert P Oczeret/EPA
Multi-layered security for everyone

App security
Operation system integrity and application sandboxes built-in.

Data protection
Data encryption, keystore, and secure lockscreens built-in.

Exploit Mitigation
Hardened media stack, updateable webview, ASLR, NX built in.
Android Safety Net
A data-driven, endpoint security solution built to protect Android users
1+ billion devices protected
400 million device scans per day
6 billion apps checked per day
Verify Apps  Sensor Network  Android Device Manager  APIS
Application Review Process

Static Analysis

Heuristic and Similarity Analysis

SafetyNet

Dynamic Analysis

Signatures

Third-party Reports

FETCH

ANALYSIS

SCORE ENGINE

HUMAN REVIEW

APPROVED
(SAFE)

REJECTED
(NOT SAFE)
Security Services Woven Into An Ecosystem

Google Play
- Install Apps
  - Apps
    - Knowledge PHA or not
      - Best practices
  - App X
  - App Y
  - App Z
  - Attest API

Android
- App Sandbox
- Verified Boot
- Encryption
- App Install Checks

Application Analysis
- Static
- Dynamic
- Reputation
  - Etc.

Knowledge PHA or not
- Data
  - App installs
  - Install Source

Chrome
- Smart Lock
- Device Manager
- Safe Browsing
- SafetyNet
- Verify Apps

Other Google Services
- Search
- Drive
- Ads
- Etc.

SafetyNet Analysis
- Exploit Detection
  - ACE
  - SIC
  - Etc.

Knowledge Risk Signal
- Data
  - Rare Apps

Device Data
- Events
- Measurements
- Configurations
  - Etc.
Establishing Ground Truth
Vulnerabilities and Exploits are Newsworthy

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Initial Claim Headline</th>
<th>Peak exploitation after public release (per install)</th>
<th>Exploitation before public release (absolute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Key</td>
<td>99% of devices vulnerable</td>
<td>&lt; 8 in a million</td>
<td>0</td>
</tr>
<tr>
<td>FakeID</td>
<td>82% of Android users at risk</td>
<td>&lt;1 in a million</td>
<td>0</td>
</tr>
<tr>
<td>Stagefright</td>
<td>95% of devices vulnerable</td>
<td>None confirmed</td>
<td>None confirmed</td>
</tr>
</tbody>
</table>

• Majority of PHAs stay within the Security model (e.g. no exploits)
• Social Engineering is typical distribution mechanisms
Android Devices with Known PHA

Source: Android Security 2015 Year in Review
Android Devices with Known PHA

Source: Android Security 2015 Year in Review
Using Data to Protect Users
80% Reduction of Russian Bank Phishing Trojans

Affected devices in Russia
Affected devices worldwide

Source: Android Security 2015 Year in Review
Enabling Application Security
Application Security Improvement

Over 100,000 apps fixed in 2015
SafetyNetApi.attest

Protecting millions of app events every day
Improving Transparency
nexus  Pixel

Monthly Security Updates
Monthly Security Bulletins
3 years from device availability
Android Security Monthly Process

Month 0
- Partner Bulletin
  (Patch, Backports, Severity Guidance)

Month 1
- Public Security Bulletin
  AOSP Updated
  Device OTAs Begin

Month 2
- Compatibility Requirement

Other Remediations: SafetyNet, Google Play, Verify Apps
Enabling more (effective) security research
g.co/AndroidSecurityRewards

Over $1 million paid to date
Open Ecosystems Foster Innovation

- **millions** of lines of code in Android Open Source
- **thousands** of unique devices
- **hundreds** of OEMs and security solutions
security@android.com