Android Security
Data from the Frontlines

security@android.com
aludwig@google.com
Goal of this talk

Provide insight into overall Android security strategy.
Discuss data that is being used to guide our efforts.
Enable you to make more informed risk decisions.
Strategy  Data
The Android Security Model

Application Isolation
- Sandboxes
- Permissions
- Trustzone

Device Integrity
- Data Encryption

Platform Hardening
- SELinux
- ASLR
- Exploit mitigation

Android For Work
- Profiles
- Enterprise services

See RSA Conference Presentation from 2014, or https://source.android.com/devices/tech/security/ for more information
Google Security Services for Android

- Google Play
- Safebrowsing for Chrome
- Verify Apps
- Android Safety Net
- Device Manager

Decisions are based on billions of data points (including apps, developers, app behavior, relationships, and third-party analyses) captured every day.
An Open Security Ecosystem

billions of users protected

millions of code in Android Open Source

thousands of unique devices

hundreds of OEMs, ISVs, and security solutions
## Layered Ecosystem Security Strategy

<table>
<thead>
<tr>
<th>Trusted Android Platform</th>
<th>Google Security Services</th>
<th>Open Ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-device defenses against attacks</td>
<td>Comprehensive, integrated suite of security services available to all</td>
<td>Embracing security innovation for long term security advantage</td>
</tr>
</tbody>
</table>

**Clarity in the Data**
Malware myths and assumptions

Most devices aren’t protected.

Malware is increasing.

(All) malware can compromise everything.

The problem is too hard, the bad guys are going to win.
What does the data show?
Verify Apps

✅ Apps are verified prior to install

✅ Provides periodic background scans

✅ Warn for or block Potentially Harmful Applications
Android Safety Net verifies over 1 billion devices

Source: Google Safety Net Data
Less than 1% of devices have a PHA installed

Source: Google Safety Net Data
Use of Google Play reduces PHA exposure

Devices with Known PHA (Except Rooting)
Rate of install of PHAs was reduced by 50% in 2014

Fraction of Installs that Result in Known PHA Being Installed (Excluding Russia)

Regional variations are significant (and unique)
Install trends for PHAs vary by capability

Fraction of Installs that Result in Known PHA of the Given Category Being Installed

Install trends have a characteristic shape by “type”

Fraction of Install Attempts that Result in Known PHA of the Given Category Being Installed

Source: Google Safety Net Data
Spyware installs are down 90% in 2014

Fraction of Installs that Result in Known Spyware Being Installed, Worldwide

Spyware installs were reduced across major locales
Commercial spyware is less than 0.02% of installs

Source: Google Safety Net Data
Ransomware is less than 0.03% of installs

Source: Google Safety Net Data
SMS Fraudware installs are down over 60% in 2014

Fraction of Install Attempts that Result in SMS or WAP Fraud Being Installed

SMS Fraudware installs are down over 90% since 2013

Source: Google Safety Net Data
Overturning Malware Myths and Assumptions

Android users have built-in protection.

Risky devices get better protection.

Mobile malware can be classified and isolated.

Mobile malware is not increasing.

The good guys can win.
Let’s try that on a harder problem.
Exploitation myths and assumptions

- All devices have vulnerabilities.
- All vulnerabilities can be exploited.  
- Exploitation can’t be seen or stopped.  

The bad guys will win.
What does the data show?
Find the exploit.
Multiple Security Layers Provide Protection and Insight

Google Play
Verify Apps
Safety Net
Permissions
Sandboxes and Isolation
Exploit Mitigation
Updates
Some exploits can be seen (and stopped)

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>News Headline</th>
<th>Unique APKs</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>1231</td>
<td>&lt; 8 in a million</td>
<td>0</td>
</tr>
<tr>
<td>FakelID</td>
<td>82% of Android users at risk</td>
<td>258</td>
<td>&lt;1 in a million</td>
<td>0</td>
</tr>
</tbody>
</table>

Masterkey data collected from 11/15/2012 to 8/15/2013 and previously published at VirusBulletin 2013. Fake ID data collected from 11/15/2012 to 12/11/2014 and previously published at

Source: Google Safety Net Data
Platform level failed exploit detection

In a heterogeneous ecosystem, logging failed attacks on patched devices may provide insight into the exposure of unpatched devices.

Note: Your mileage may vary.
Android Safety Net

Detect
- SMS Abuse Tracking
- 0-day detection
- Failed exploit detection
- SELinux logs analysis
- Rare App Collection

Protect
- Real-time SMS Warnings
- Certificate Pinning
- Certificate Blacklisting
- Inter-app firewall
- SELinux policy update
Network behaviors may indicate attempted MiTM

Fraction of SSL Connections Downgraded to SSLv3 for Top Countries

Source: Google Safety Net Data
Local state may indicate compromise

Source: Google Safety Net Data
Key elements of security model

Source: Google Safety Net Data
Exploitation myths and assumptions

Multiple layers of protection.

Some vulnerabilities are not exploited.

So far, limited evidence of malicious exploitation.

The good guys can win if we use layers of protection wisely.
Conclusion(s)

Strategy:
- Multiple layers of protection for Android ecosystem
- Multiple layers of protection for Android users

Data:
- Less than 1% have a PHA; <.15% for Google Play users
- Overall install rate reduced by 50% in 2014
- Specific types / families reduced even more:
  - SMS by 90%
  - Spyware by 60%
- Exploitation of vulnerabilities still below visibility thresholds
Android

Data From the Front Lines

aludwig@google.com
security@android.com