Android

Building a Secure Open Source Platform

Google

#RSAC

RSACONFERENCE2014

The Android Security Philosophy

Effective security is invisible and evokes calm.

Google

#RSAC

RSACONFERENCE2014

Layered Security

Clarity in the Data

Google

#RSAC

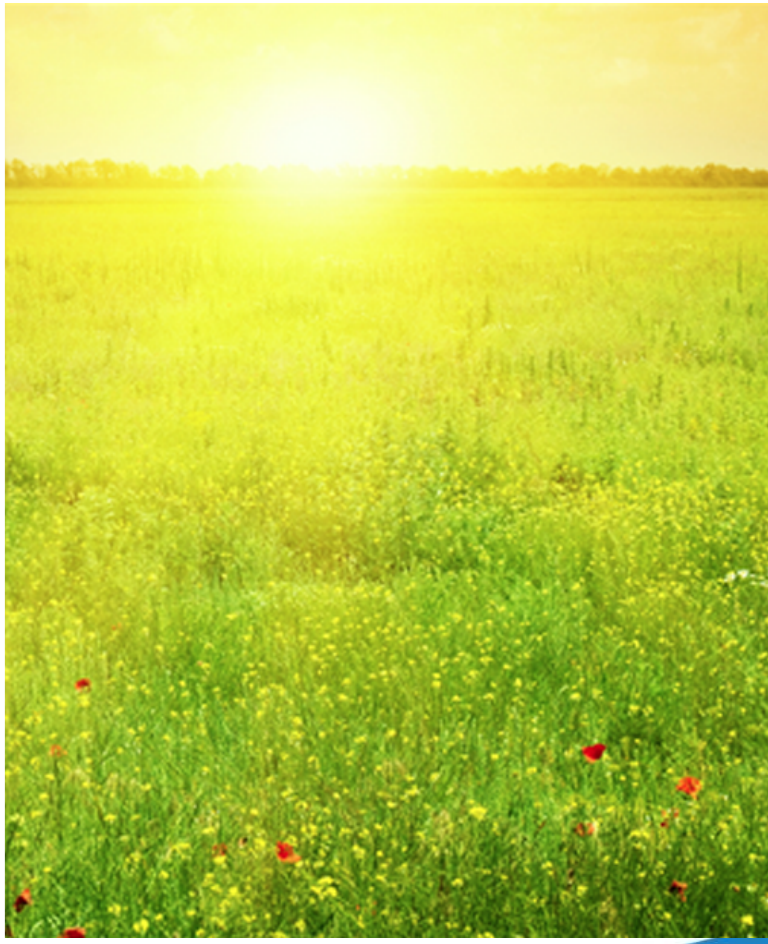
RSACONFERENCE2014

Platform

Services

Innovation

Layered Security



Google

#RSAC

RSACONFERENCE2014

A platform for applications

Google

#RSAC

RSACONFERENCE2014

The Android Security Model

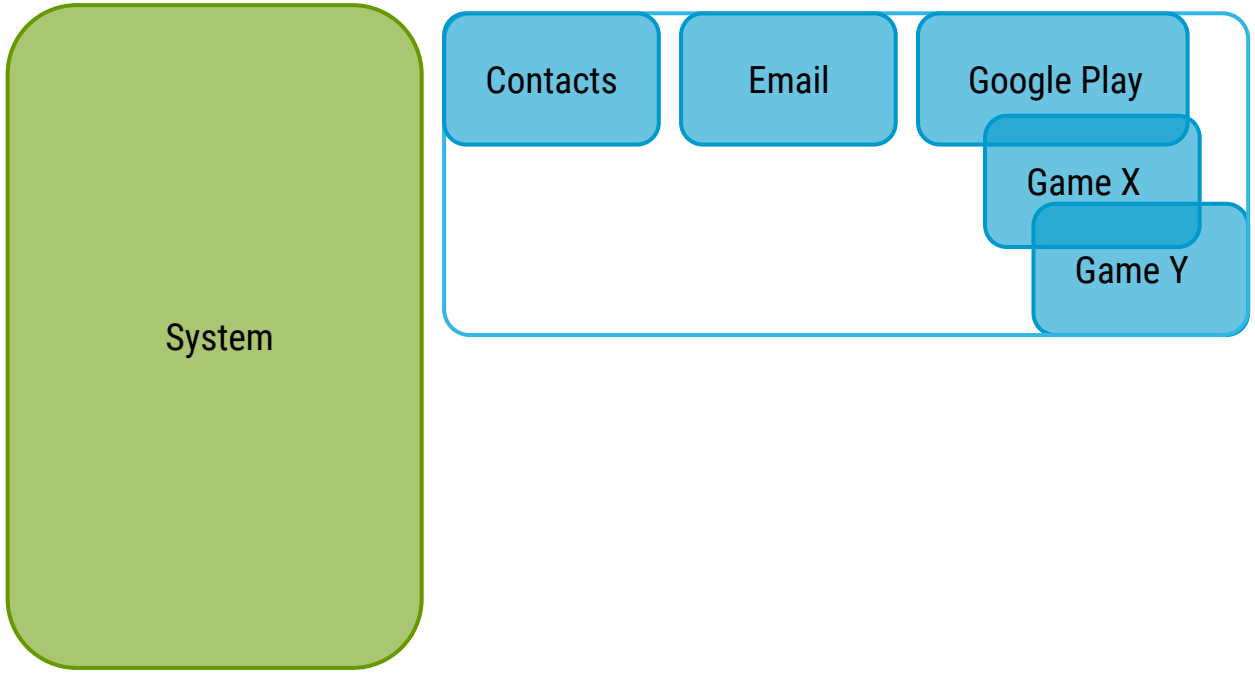
Application isolation (even from the OS)

Android verifies application signature and assigns an application sandbox at install time.

Application Sandboxes (including system) isolate data by running each app as its own UID.

Inter-process communication (IPC) requires mutual request.

IPC and services may be protected by permissions.



Google

#RSAC

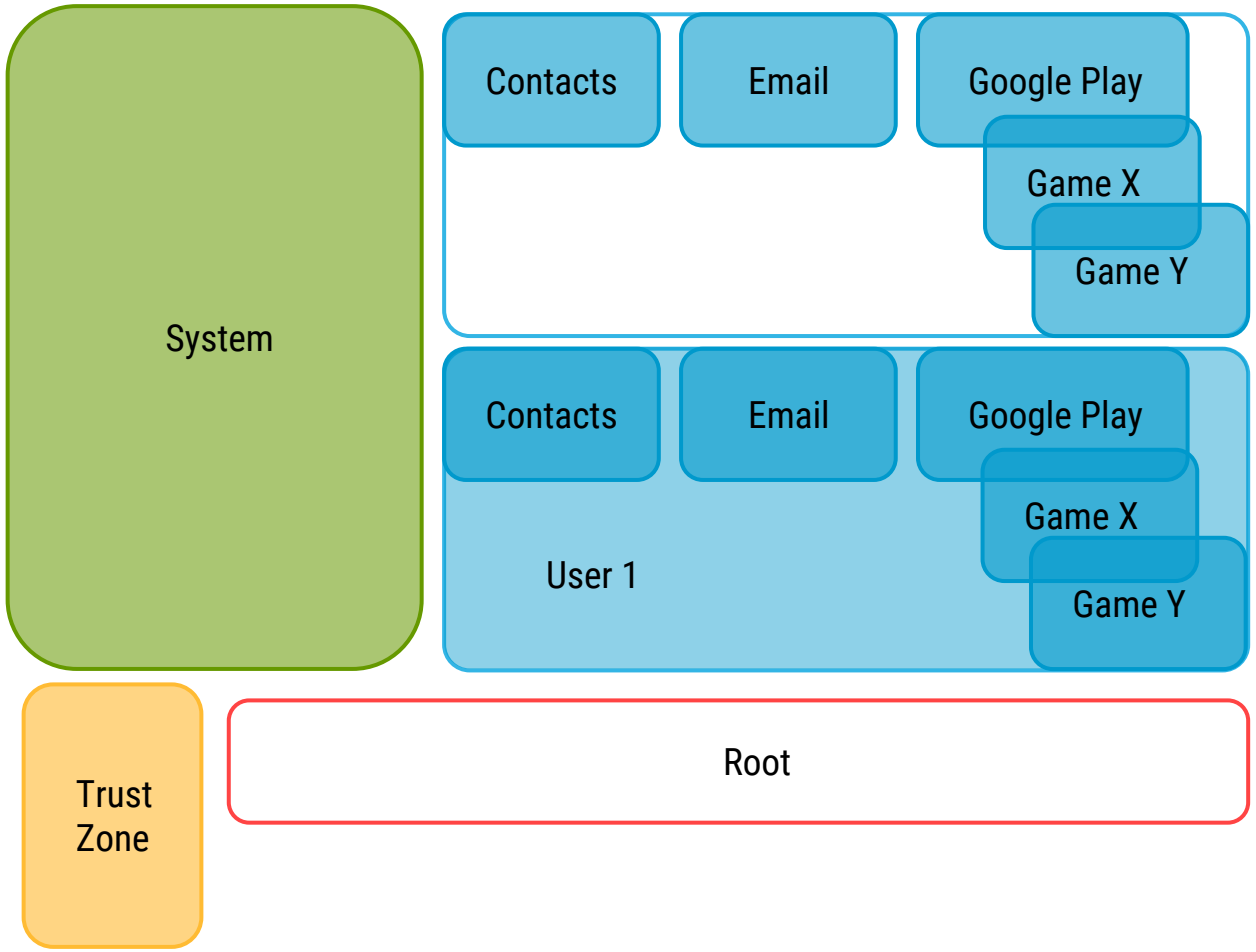
RSACONFERENCE2014

The Android Security Model

Multi-user and Hardware Crypto added in Android 4.1

Application sandbox extended to groups of applications -- preventing IPC across the user boundary

Developer key store protected from root compromise



Google

#RSAC

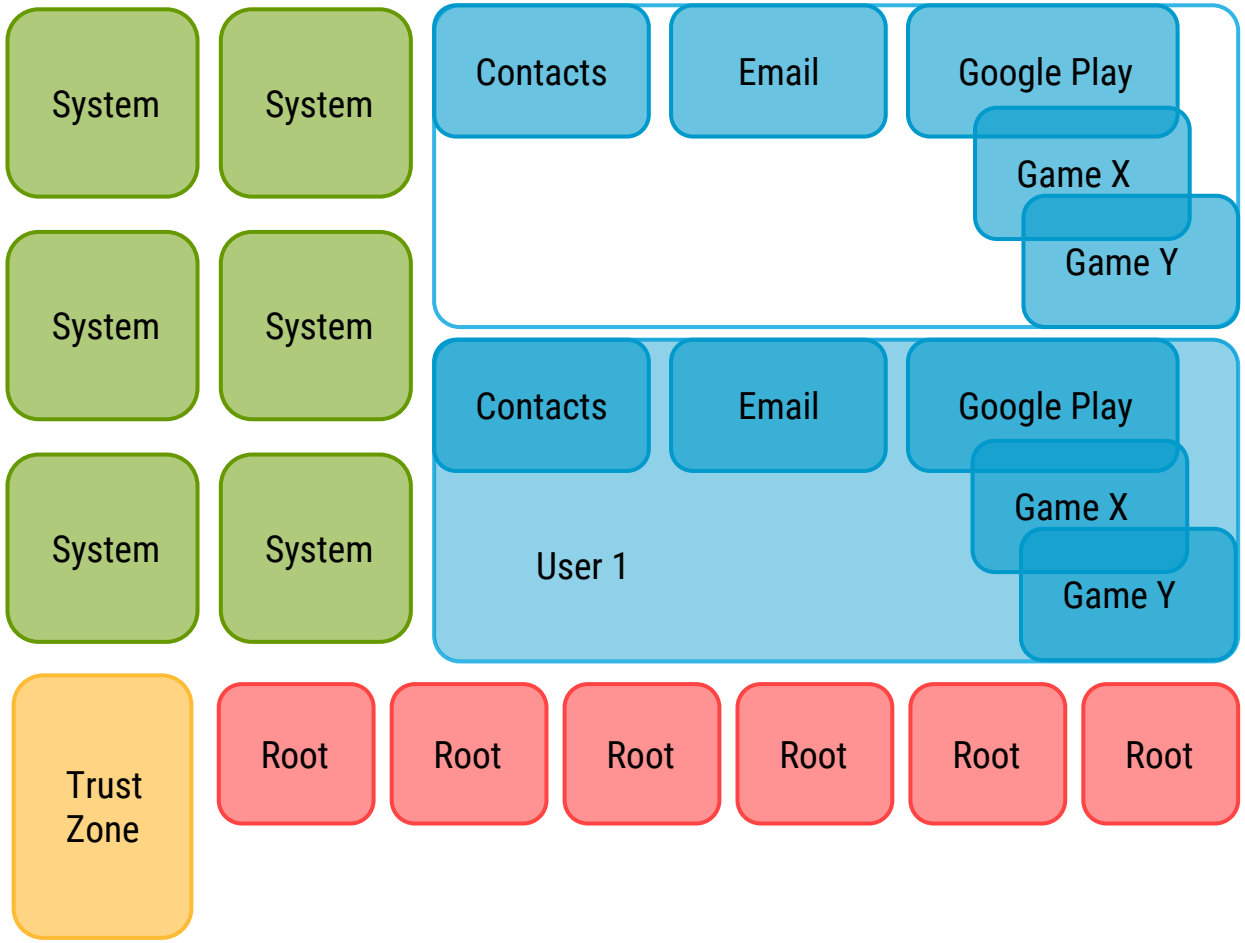
RSACONFERENCE2014

The Android Security Model

SELinux added in Android 4.3

Segmentation of system and root UID with constrained SELinux policies

Central security policy allows audit of system & root applications

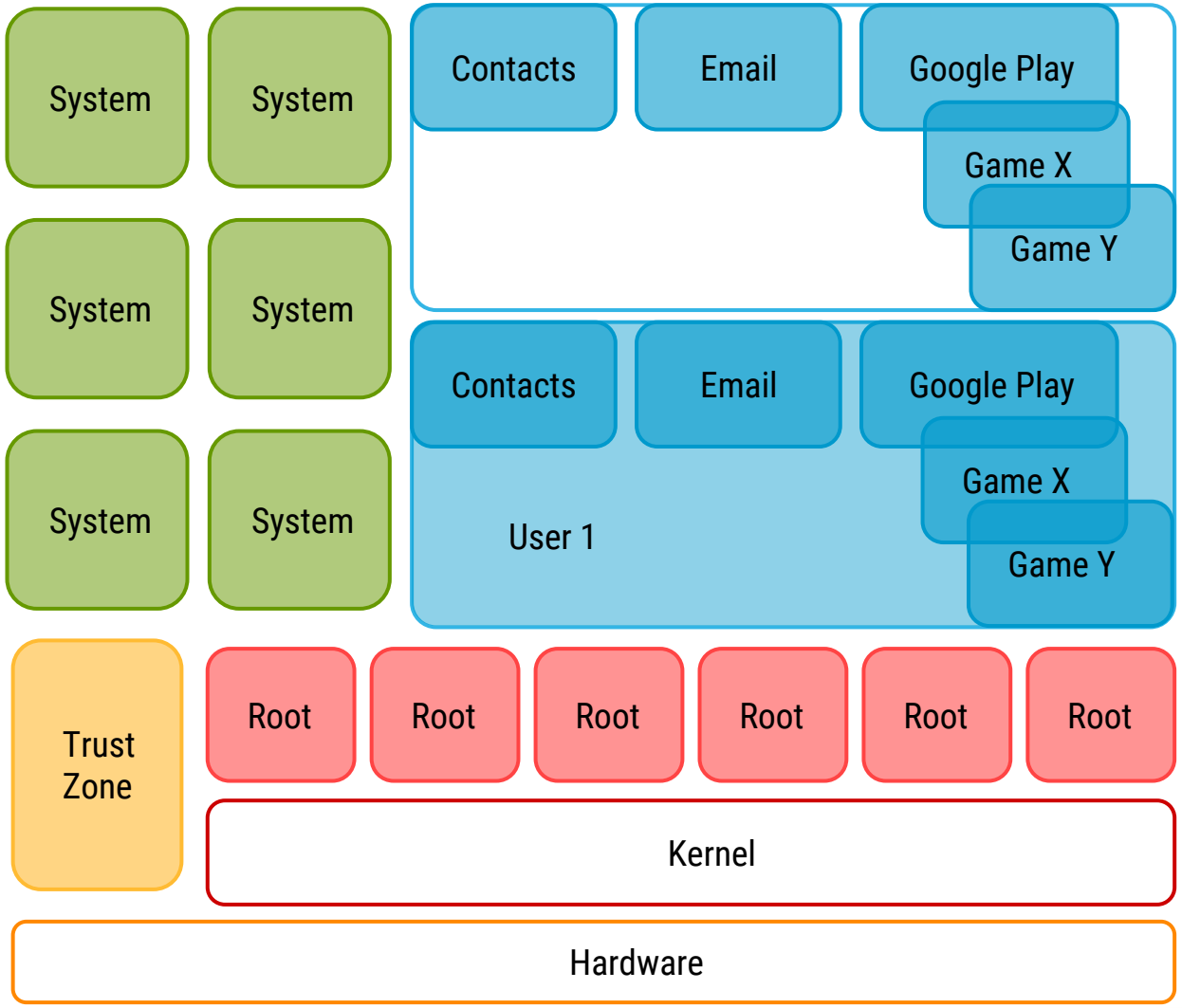


The Android Security Model

Enabling isolation and integrity at the lowest levels

Experimental features in 4.4 provide integrity checking for the full stack.

Supply chain threats are also a focus of research efforts.



Android Hardening

On-device defenses against known and future attacks

Attack Surface Reduction

- ✓ Sandboxes
- ✓ Permissions
- ✓ SELinux

Exploit Mitigation

- ✓ FTRAPV
- ✓ ASLR
- ✓ Fortify Source

Google

Common Security Services

Highly visible, minimally effective, evoke fear.

Google

#RSAC

RSACONFERENCE2014

Ideal Security Services

Invisible, effective, evokes calm.

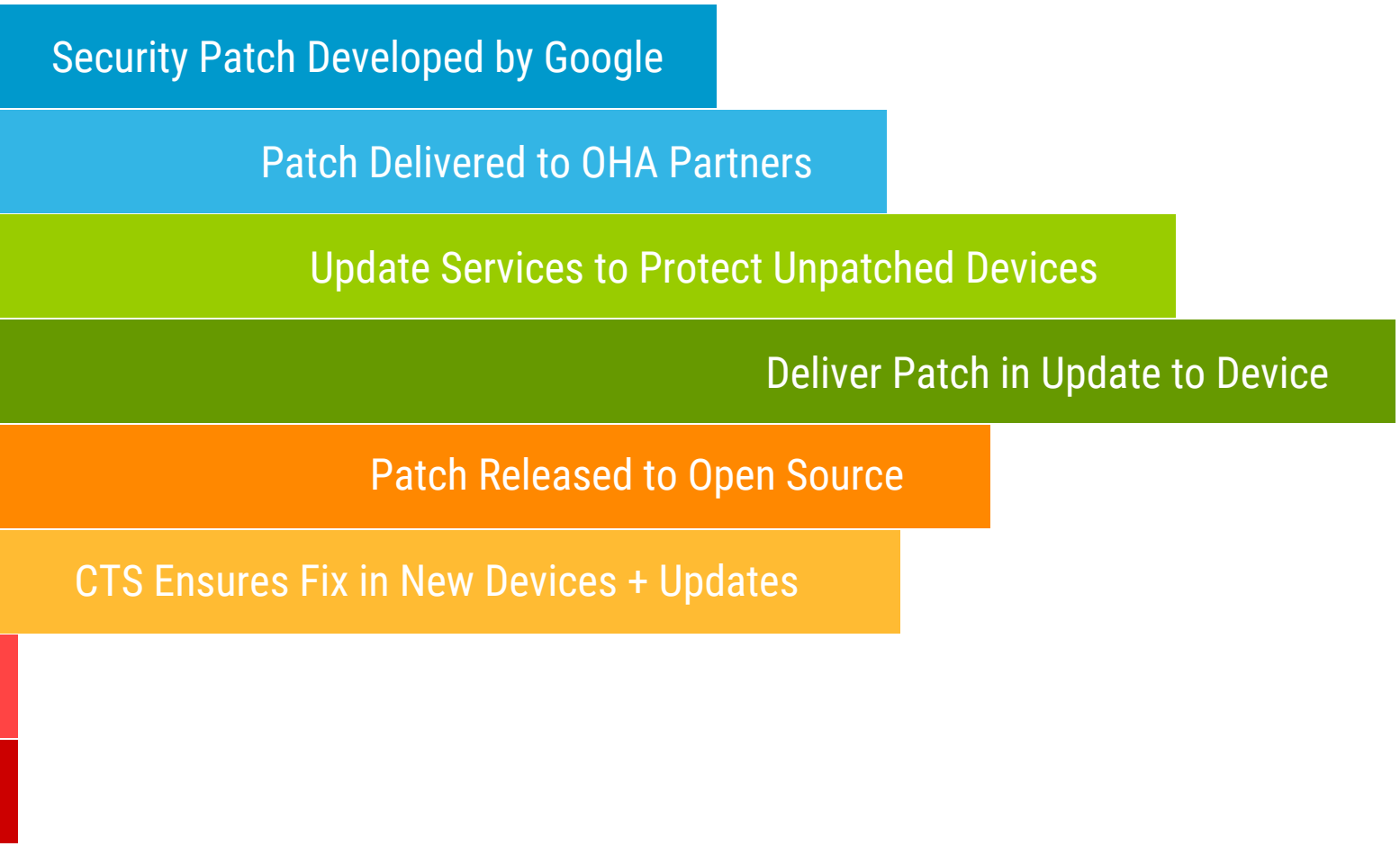
Google

#RSAC

RSACONFERENCE2014

Android Security Updates

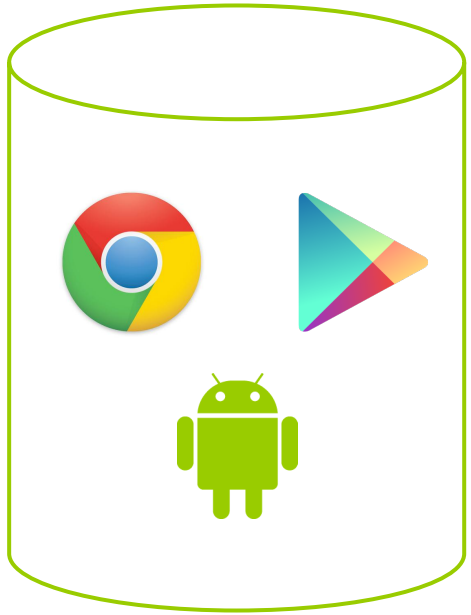
Vulnerability remediation services



Google

Google Security Services for Android

Comprehensive, integrated suite of security services



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

Millions of new pieces of data including apps, developers, app behavior, relationships, and third-party analyses are added every day.

Google

Google Play

Is a security service

- **Block Distribution of Potentially Harmful Apps**
- Maintain Relationship With Developers
- Encourage Security Best Practices
- Application Updates
- User & Developer Services

Google

Verify Apps

Extending security services beyond Google Play

- Apps are verified prior to install
- Warn for or block Potentially Harmful Applications
- Available on Android 2.3+ with Google Play
- Over 20 million installs verified every day
- **Soon with constant on-device monitoring**

Google

#RSAC

RSACONFERENCE2014

Android Safety Net

Services to detect & protect against known & future attacks

Detect

- SMS Abuse Tracking
- 0-day detection
- Failed exploit detection
- SELinux logs analysis

Protect

- Real-time SMS Warnings
- Certificate Pinning
- Certificate Blacklisting
- Inter-app firewall
- SELinux policy update

Google

#RSAC

RSACONFERENCE2014

Walled Gardens Eventually Begin to Crumble

Google

#RSAC

RSACONFERENCE2014

Open Ecosystems Thrive on Innovation

Google

#RSAC

RSACONFERENCE2014

Foster Security Innovation

1

Enable security solutions on top of the platform

2

Foster security innovation in the platform

3

Directly support research as well as development

Google

Consumer & Enterprise Security Investment

50+

device policy solutions available

5,000,000+

installs through Google Play

20+

consumer security solutions available

100,000,000+

installs through Google Play

Diverse Sources of Platform Innovation

hundreds

OEMS build devices
with Android

thousands

contributors to Android
Open Source project

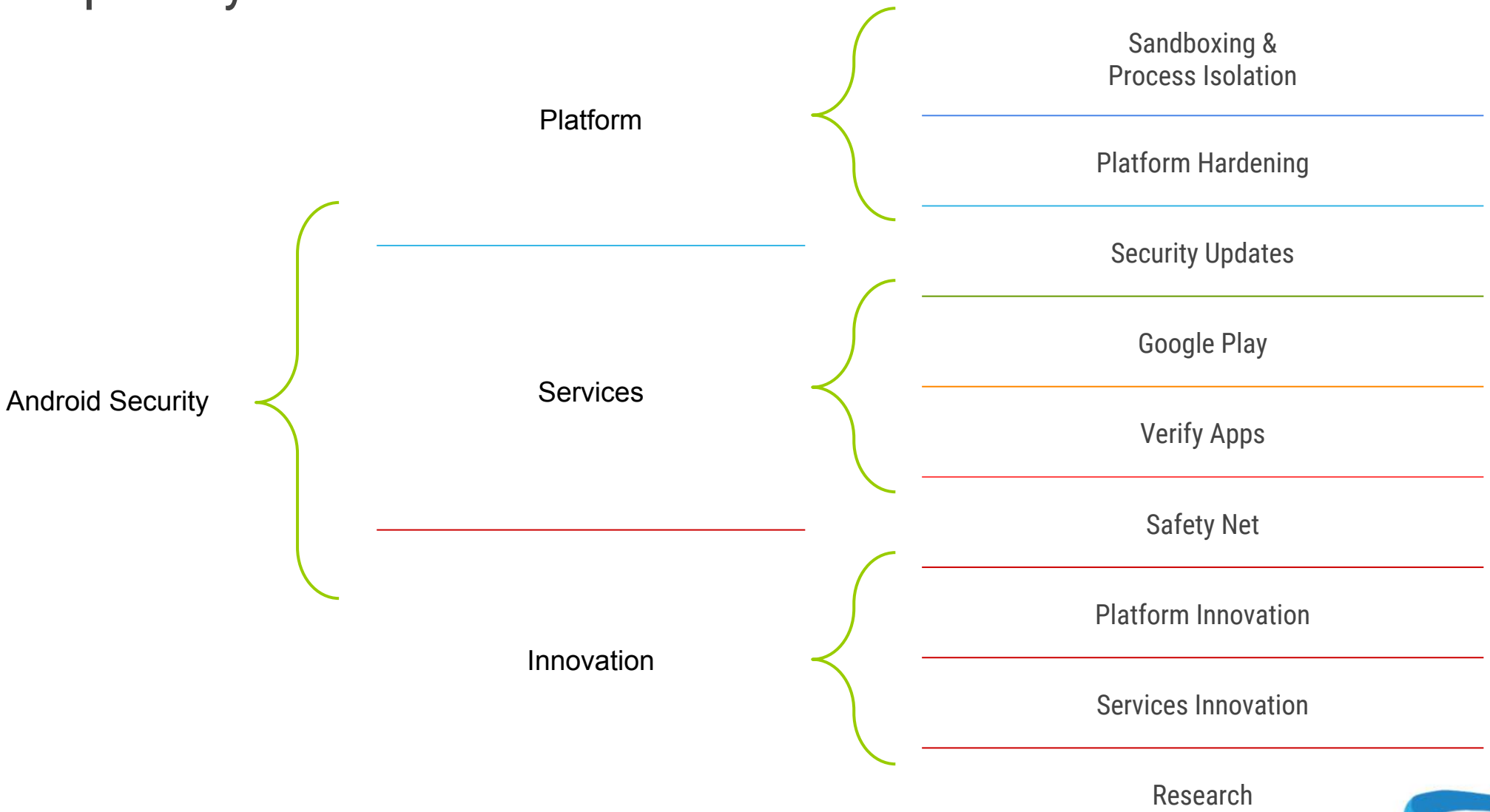
thousands

unique devices are
available to consumers

millions

lines of code in
Android Open Source

Multiple Layers of Defense



Google

#RSAC

RSACONFERENCE2014

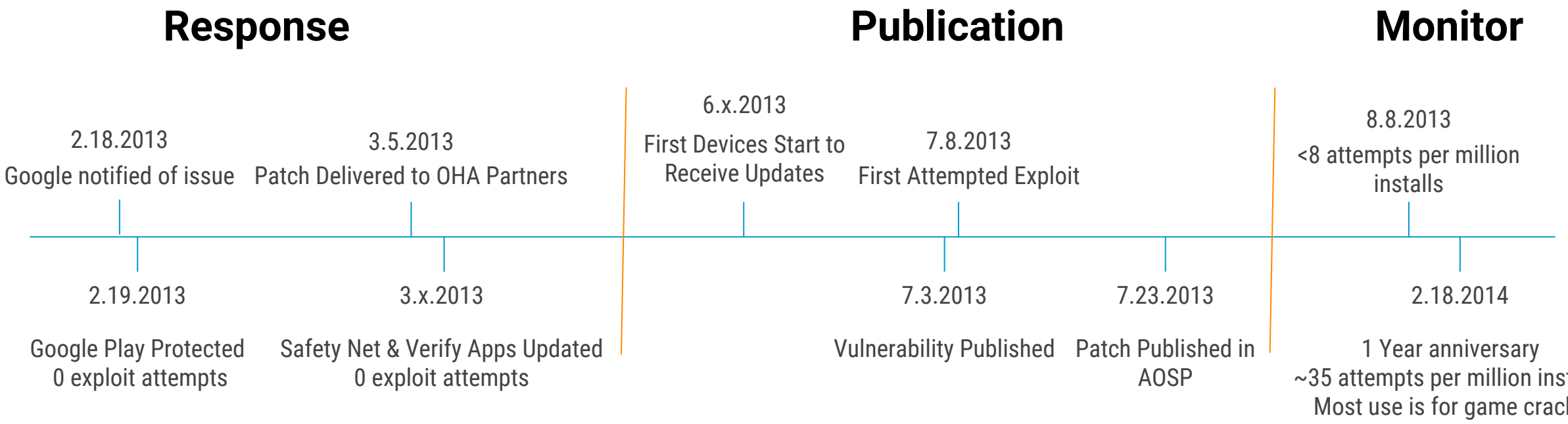
Google

#RSAC

RSACONFERENCE2014

Timeline of Security Response

Masterkey vulnerability



Google

#RSAC

RSACONFERENCE2014

Multiple Layers of Defense

Applied to the Masterkey vulnerability

100% of Google Play downloads were safe

Most user devices protected by Google services prior to first exploitation

Leading devices updated before first exploit

No evidence of exploitation before disclosure at BlackHat

Attacks are specific to one key -- so must be highly targeted (heterogeneity protects users)

Ecosystem-wide monitoring shows very low attempted exploitation (game cracks, testing)

Google

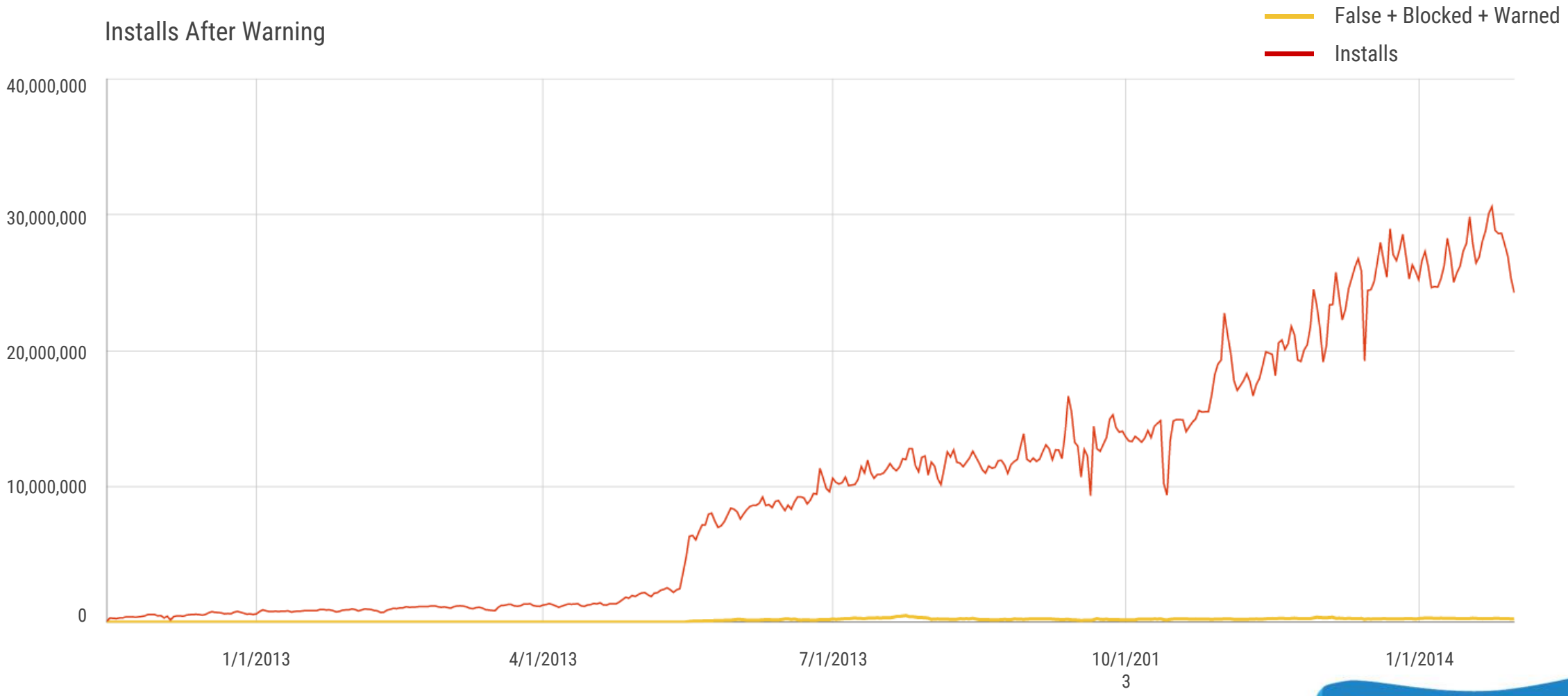
Understanding Specific Threats to Users

Threat	News Headline	Unique APKs	Installs from Unknown Sources	Installs (estimated)
Master Key	99% of devices vulnerable	1231	< 8 in a million	<1 in a million
Droid Kung Fu	Android Malware Steals Sensitive Data Avoids AV Detection	10,000+	<5 in a million	<1 in a million
Obad	Now being distributed by mobile botnets	14	<1 in a million	<1 in a million
Androrat	Androrat Remote Access Trojan is Cheaper and More Dangerous than Ever	241	< 1 in a million	<1 in 10 million

Google

*This data collected from 11/152012 to 8/15/2013 and previously published at VirusBulletin 2013. The total number of installs outside Google Play is not known, the estimate in the last column is a blended average across all install channels and assumes that Verify Apps is seeing approximately 50% of installs outside of Google Play.

Analyzing 4 Billion Installs from Outside Google Play

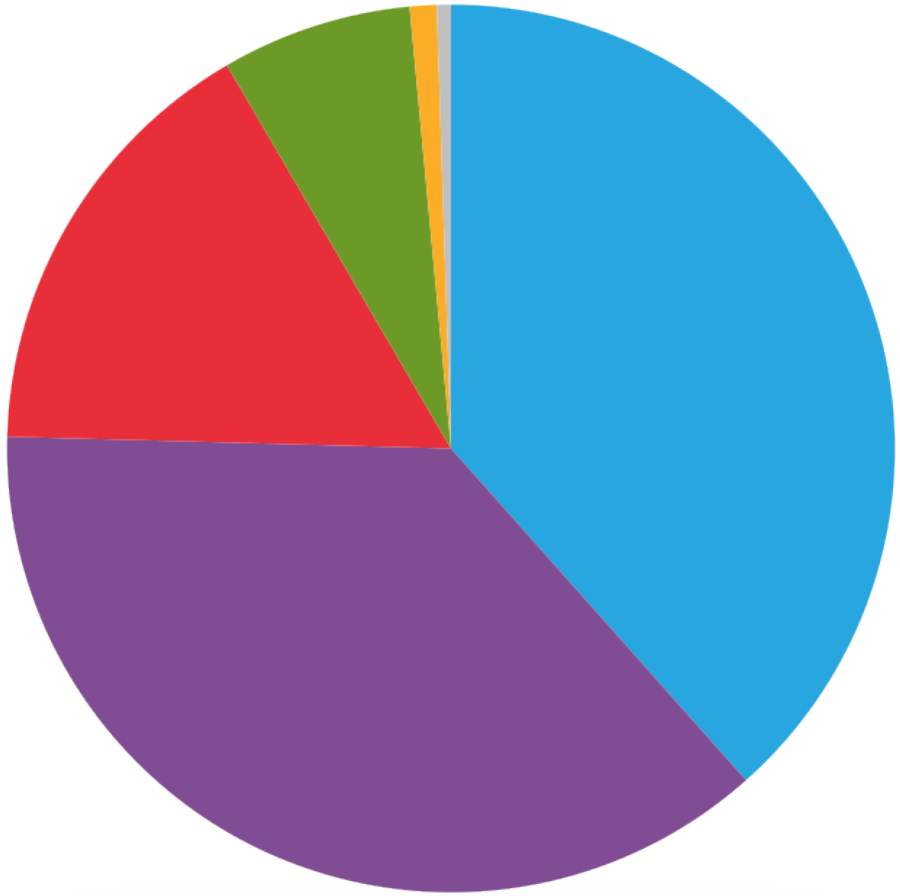


*Data collected from users of Verify Apps who install of applications outside of Google Play. Data covers period from 11/15/ 2012 to 2/18/2014.

Most Common PHA is Non-Malicious Rooting

PHAs Installed (per million installs)

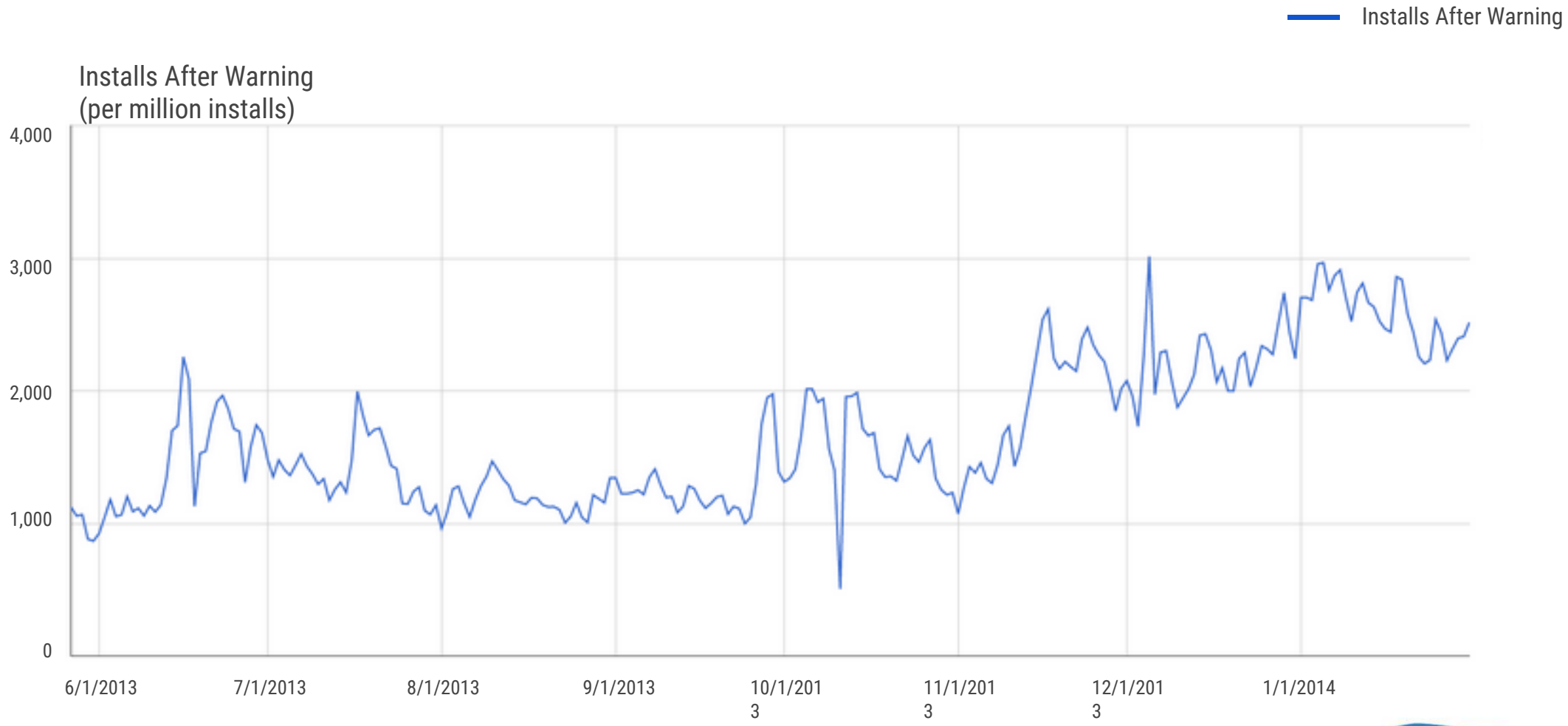
671	Non-Malicious Rooting
646	Known Bad Source
282	SMS Fraud
121	Spyware
17	Trojan
9	Other (Backdoor, Phishing, Malicious Exploit, Windows)



Google

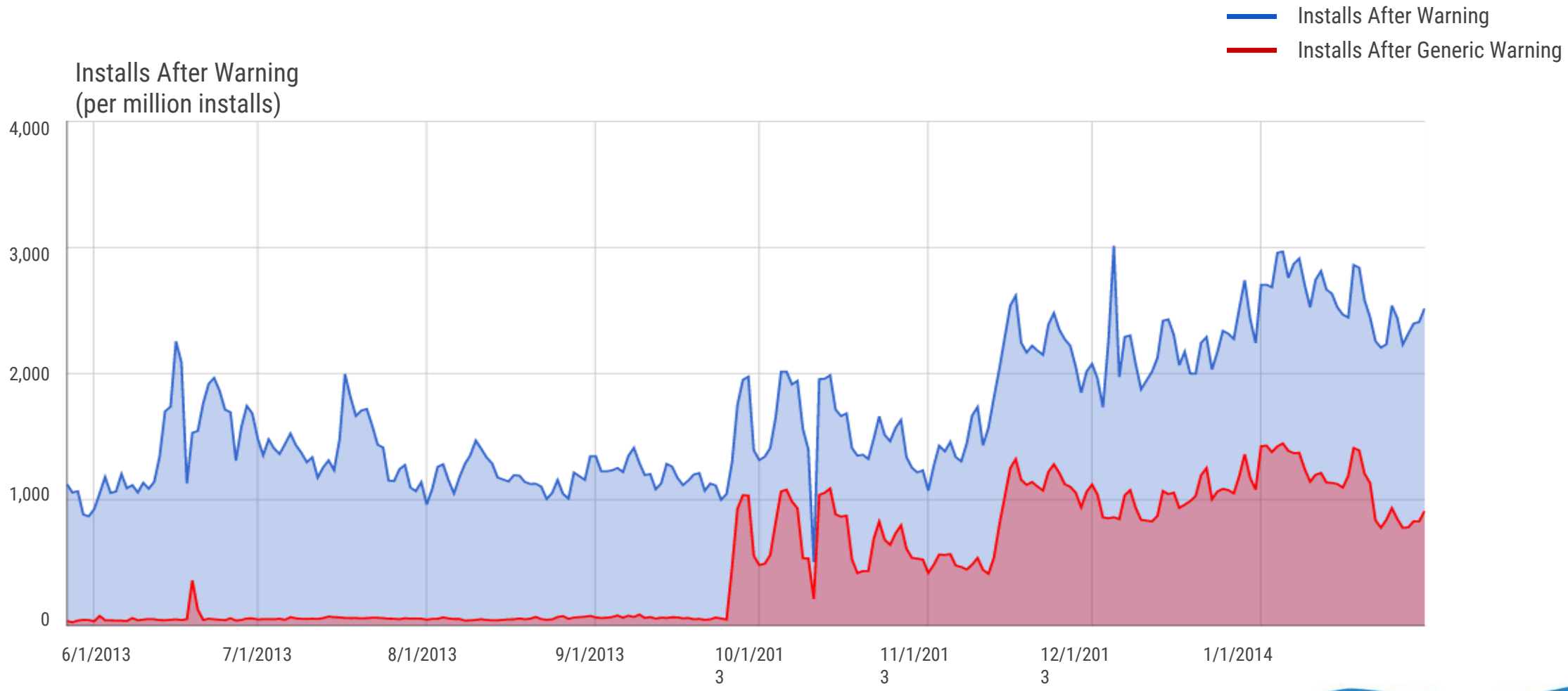
*Data collected from users of Verify Apps who install of applications outside of Google Play. Data covers period from 11/15/ 2012 to 2/18/2014.

Potentially Harmful App Installs Low & Stable



*Data collected from users of Verify Apps who install of applications outside of Google Play. Data covers period from 6/1/ 2012 to 2/18/2014.

Better detection of polymorphic apps



*Data collected from users of Verify Apps who install of applications outside of Google Play. Data covers period from 6/1/ 2012 to 2/18/2014.

Multiple Layers of Defense

Applied to the Potentially Harmful Apps

100% of devices have sandboxes and permissions

95% of devices have Verify Apps

Most devices only install from trusted sources

~.8% of app installs from unknown sources receive a warning

<0.18% of apps from unknown sources are installed after a warning

<.001% of installed apps attempt to evade runtime defenses

<?% of installed apps evade runtime defenses and cause harm

Google

*Data collected from users of Verify Apps who install of applications outside of Google Play. Data covers period from 11/15/ 2012 to 2/18/2014.

A closing thought...

As an industry, we should provide better data about actual risk and focus more attention on calming users while protecting them.

Google

#RSAC

RSACONFERENCE2014

Android

Building a Secure Open Source Platform

aludwig@google.com
security@android.com

Google

#RSAC

RSACONFERENCE2014