ANDROID SECURITY

Perception vs Reality

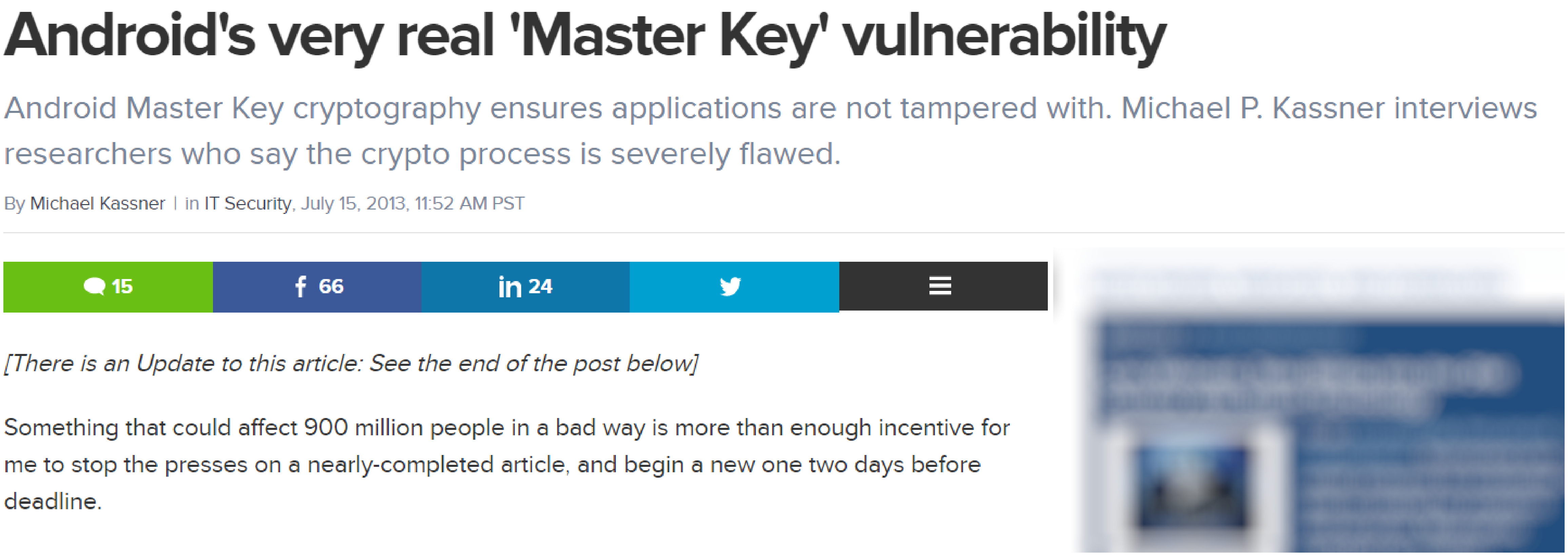
Pietro Maggi

EMEA SW Consultant Sales Engineer

ZEBRA

Is Android secure?

ZEBRA



Android's very real 'Master Key' vulnerability

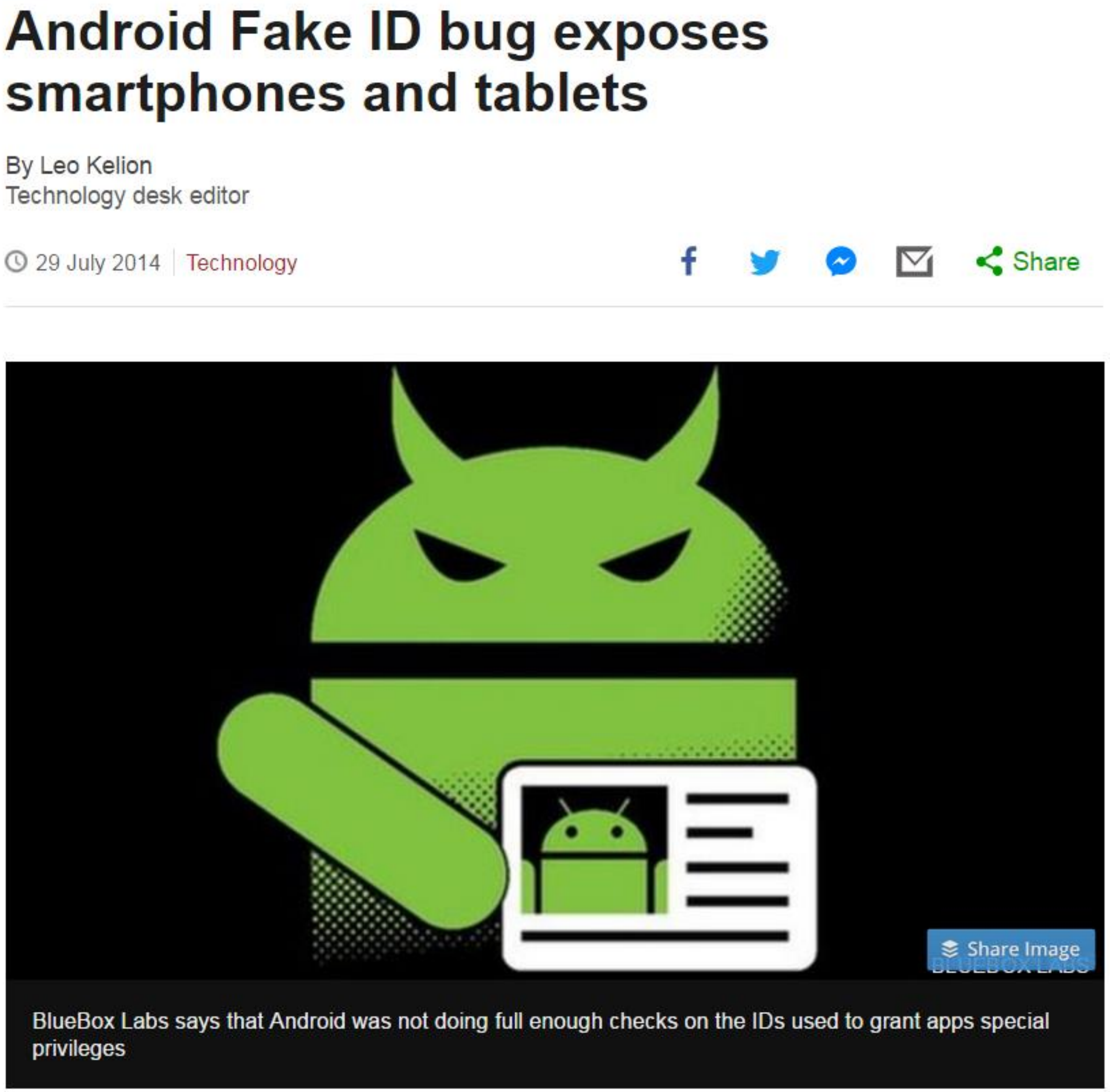
Android Master Key cryptography ensures applications are not tampered with. Michael P. Kassner interviews researchers who say the crypto process is severely flawed.

By Michael Kassner | in IT Security, July 15, 2013, 11:52 AM PST

[There is an Update to this article: See the end of the post below]

Something that could affect 900 million people in a bad way is more than enough incentive for me to stop the presses on a nearly-completed article, and begin a new one two days before deadline.

http://www.techrepublic.com/blog/it-security/androids-very-real-master-key-vulnerability/



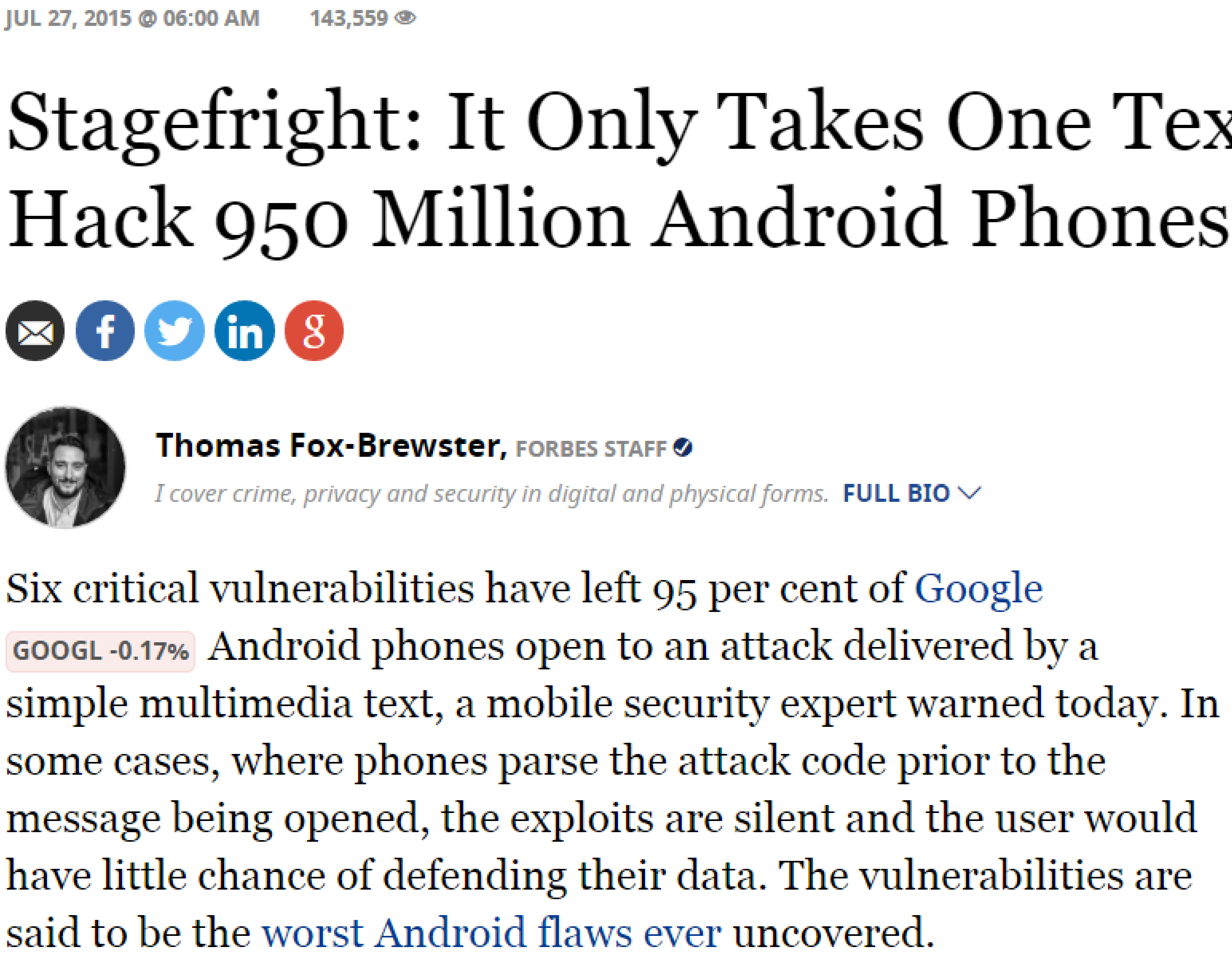
Android Fake ID bug exposes smartphones and tablets

By Leo Kelion
Technology desk editor

29 July 2014 | Technology

BlueBox Labs says that Android was not doing full enough checks on the IDs used to grant apps special privileges

http://www.bbc.com/news/technology-28544443



JUL 27, 2015 @ 06:00 AM 143,559

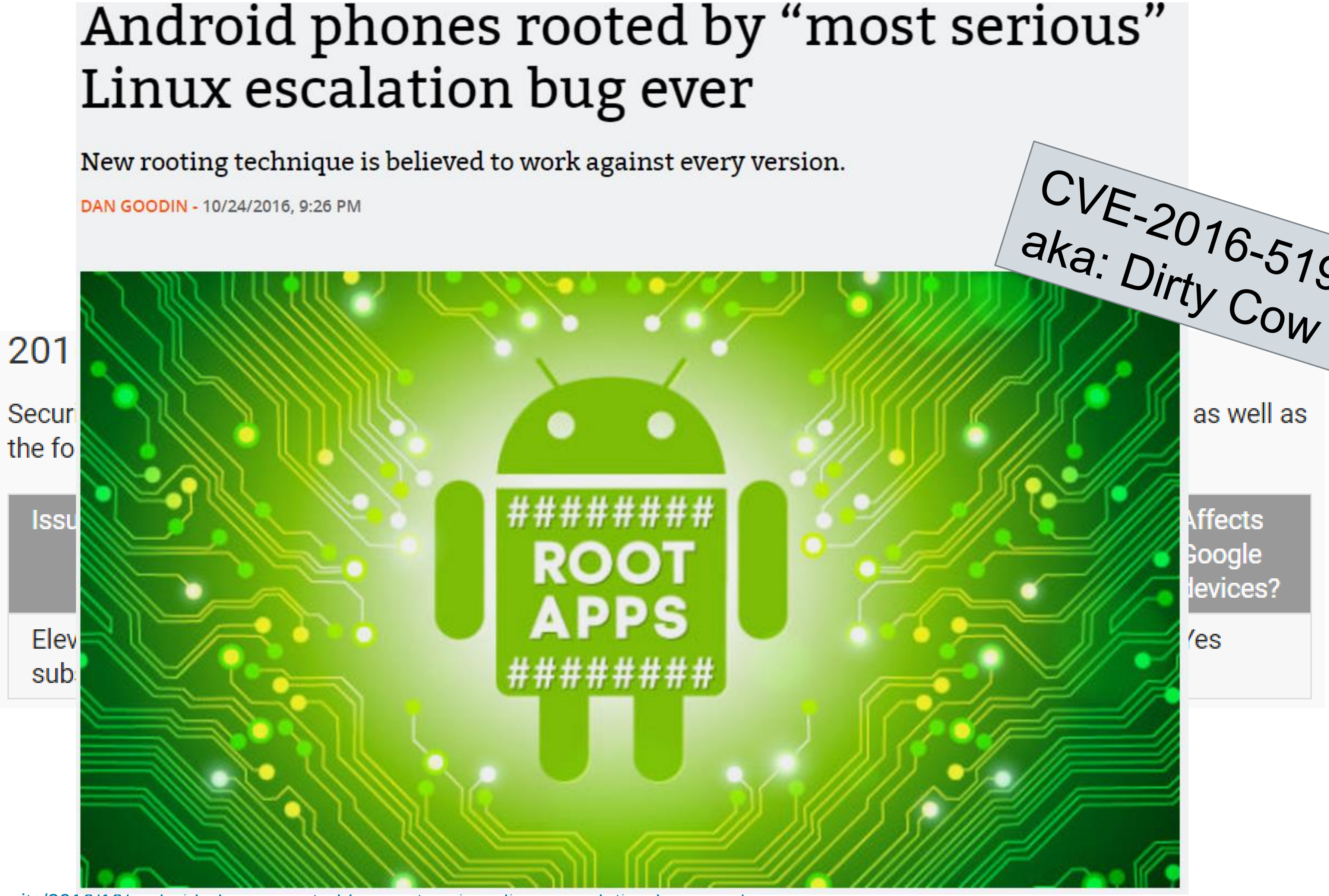
Stagefright: It Only Takes One Text To Hack 950 Million Android Phones

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. **FULL BIO**

Six critical vulnerabilities have left 95 per cent of Google GOOGL -0.17% Android phones open to an attack delivered by a simple multimedia text, a mobile security expert warned today. In some cases, where phones parse the attack code prior to the message being opened, the exploits are silent and the user would have little chance of defending their data. The vulnerabilities are said to be the worst Android flaws ever uncovered.

https://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/



Android phones rooted by "most serious" Linux escalation bug ever

New rooting technique is believed to work against every version.

DAN GOODIN - 10/24/2016, 9:26 PM

201

Secur … as well as
the fo

Issu	ffects oogle levices?
Elev sub	'es

CVE-2016-5195
aka: Dirty Cow

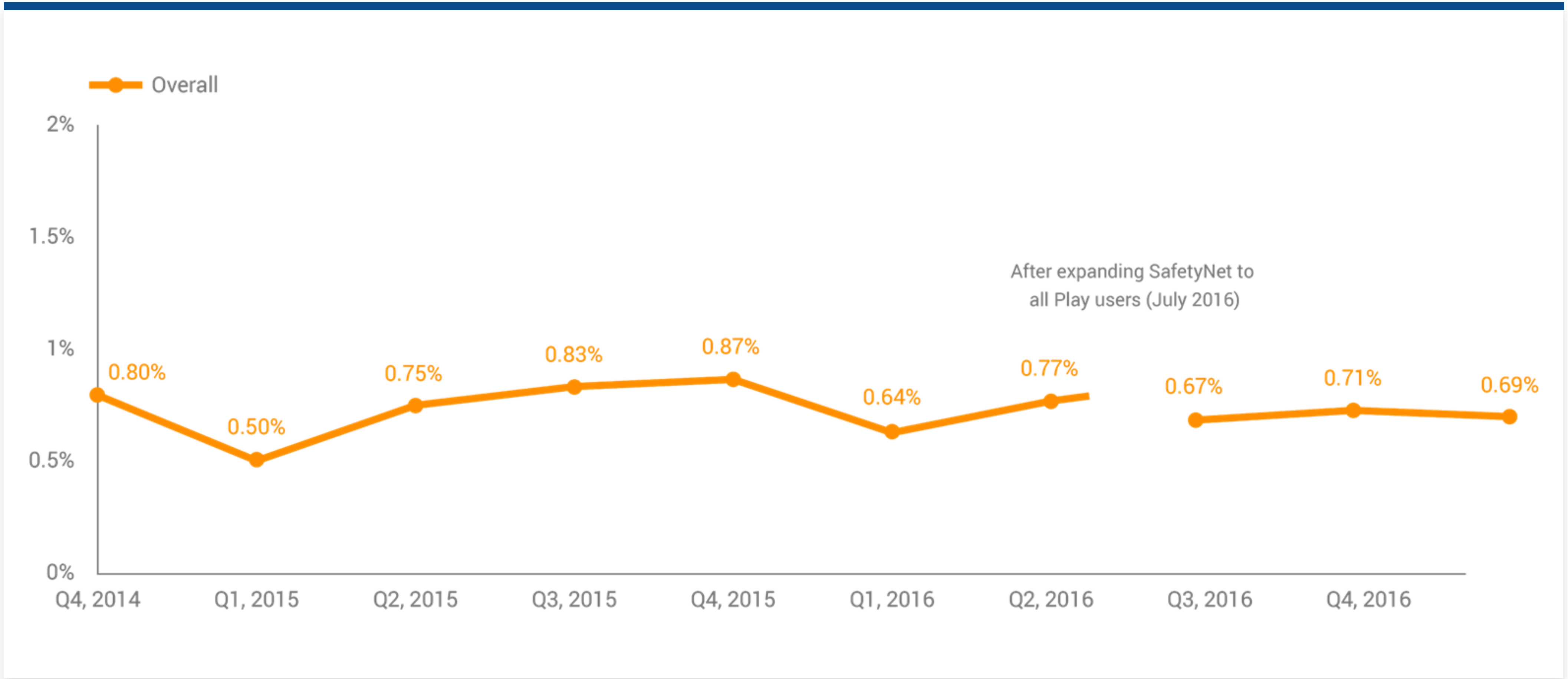
https://arstechnica.com/security/2016/10/android-phones-rooted-by-most-serious-linux-escalation-bug-ever/
https://source.android.com/security/bulletin/2016-11-01.html

Using Data to Monitor Risk: Exploits

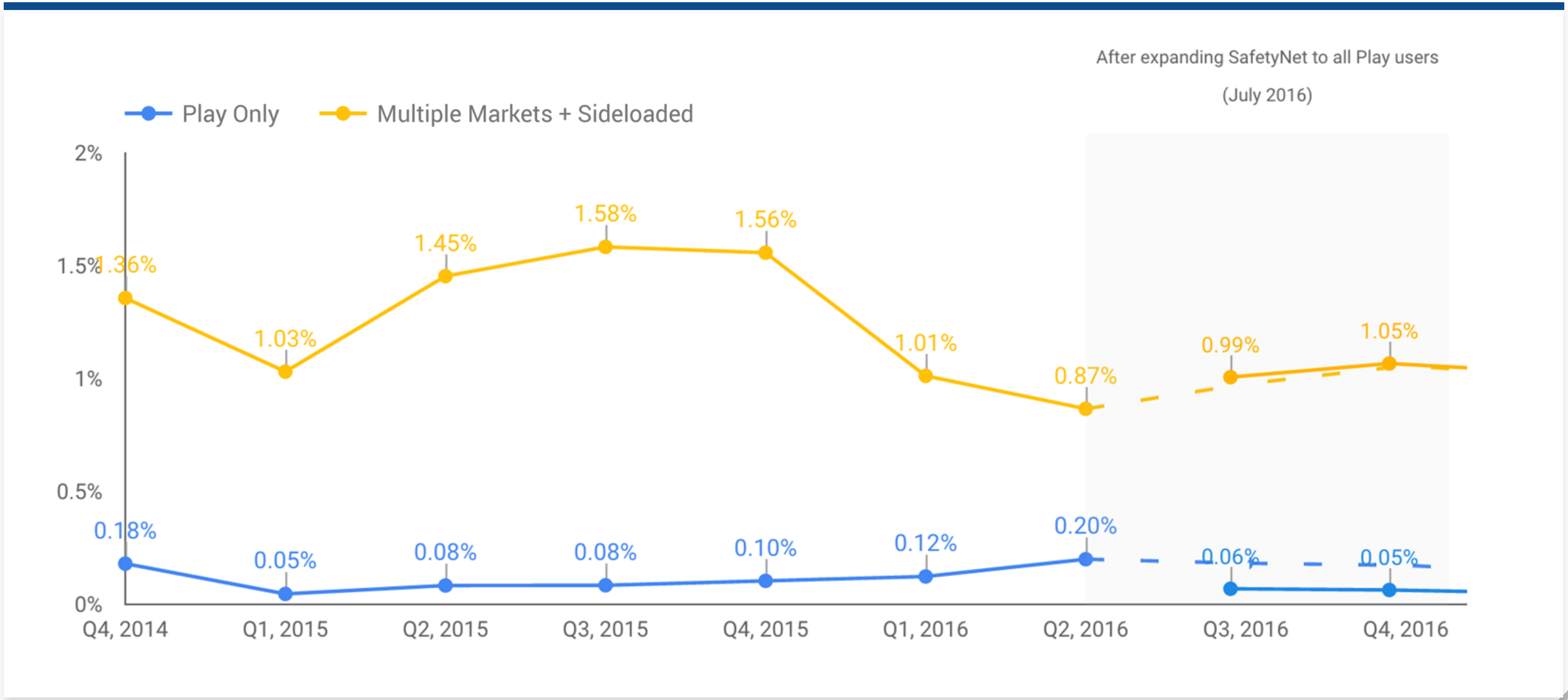
Vulnerability	Initial Claim Headline	Unique APKs	Peak exploitation after public release (per install)	Exploitation before public release (absolute)
Master Key	**99%** of devices vulnerable	1231	< 8 in a million	0
FakeID	**82%** of Android users at risk	258	<1 in a million	0
Stagefright	**95%** of devices vulnerable	N/A	None confirmed	N/A

Source: Google Safety Net Data; Masterkey data collected from 11/15/2012 to 8/15/2013 and previously published at VirusBulletin 2013. Fake ID data collected data collected from 11/15/2012 to 12/11/2014 and previously published at the RSA Conference 2015. Stagefright data current through May 2016.

Potentially Harmful Application Rates Since 2014



Potentially Harmful Application Rates Since 2014



Verify Apps API

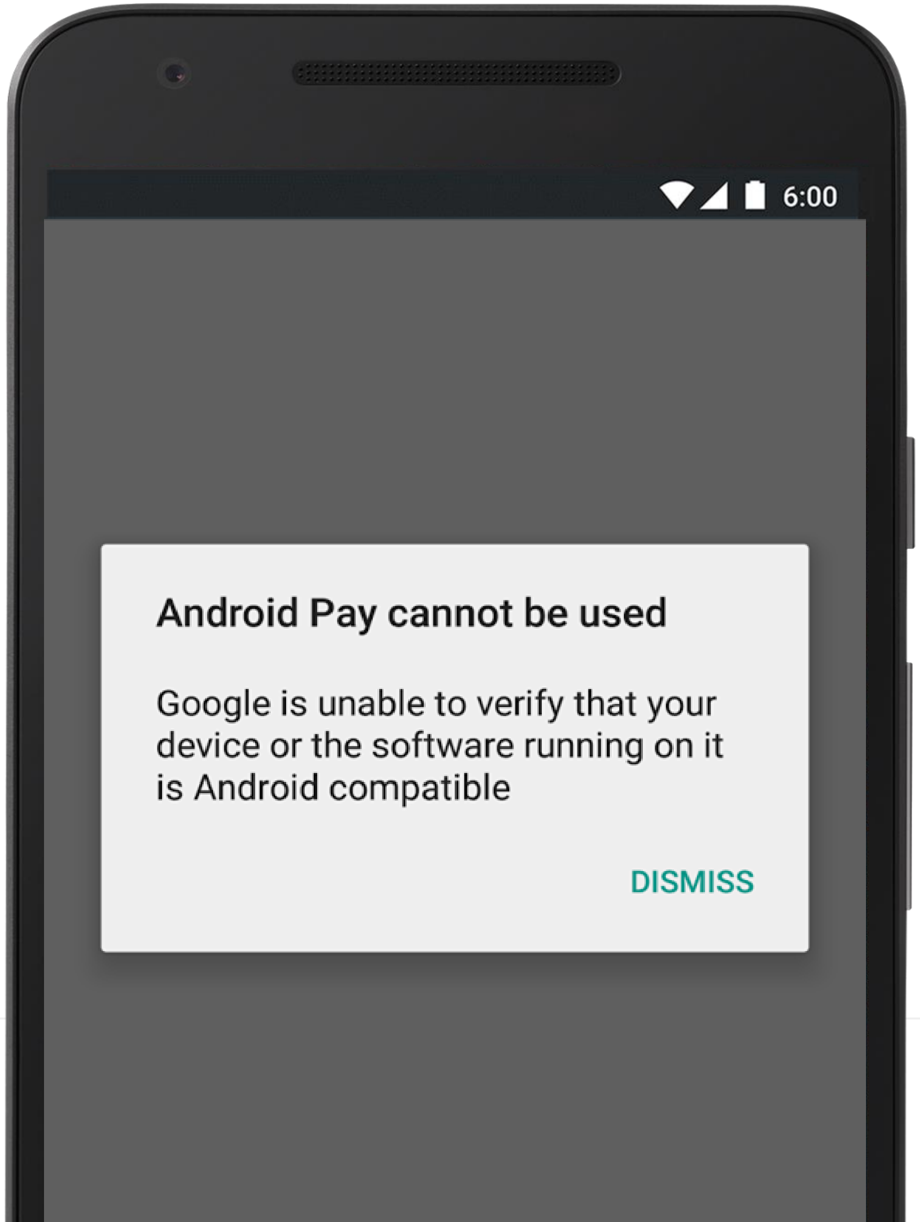
Query for the state of Verify Apps, and any harmful apps installed

isVerifyAppsEnabled()

enableVerifyApps()

listHarmfulApps()

SafetyNet Attestation



6:00

Android Pay cannot be used

Google is unable to verify that your device or the software running on it is Android compatible

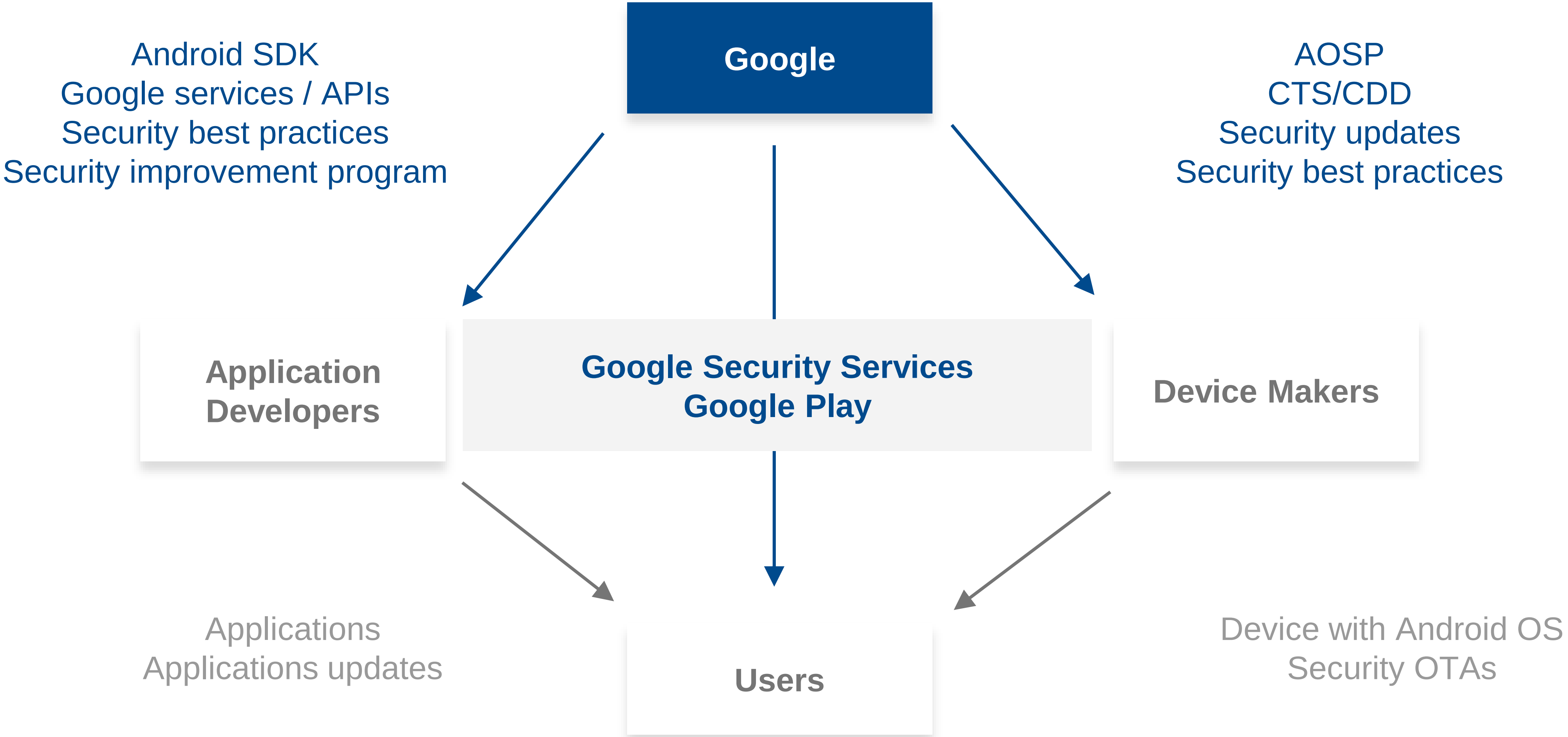
Overall…

For a device to be affected, a user must download and install a PHA that takes advantage of one of the vulnerabilities.

Using a Device Policy Controller or other lock-down systems is a very good idea for COSU devices.

Google’s role in Android ecosystem security

ZEBRA



Google

Android SDK
Google services / APIs
Security best practices
Security improvement program

AOSP
CTS/CDD
Security updates
Security best practices

Application Developers

Google Security Services
Google Play

Device Makers

Applications
Applications updates

Device with Android OS
Security OTAs

Users

https://source.android.com/security/

1

Robust Platform

2

Comprehensive Services

3

Ecosystem Updates

Android OS Offers Complete Platform Security

Application Isolation

- + Sandboxes & Permissions
- + SELinux
- + TrustZone Services
- + Seccomp
- + Isolated Process

Device Integrity

- + Hardware Root
- + Verified Boot
- + Data Encryption
- + Security Services
- + Smart Lock

Exploit Mitigation

- NX
- + ASLR
- Fortify Source
- + Updateable WebView
- + Integer Overflows
- + Hardened Media Server

Management

- + Profiles
- + Administrative APIs
- + Security Integration (VPN, etc.)

+ New or substantially changed since Android 5.0

Constant, Independent Verification

g.co/AndroidSecurityRewards

Hundreds of active researchers

1

Over $1 million paid in last 12 months

1

Robust Platform

2

Comprehensive Services

3

Ecosystem Updates

ZEBRA

SafetyNet: Complete Security Services for Android

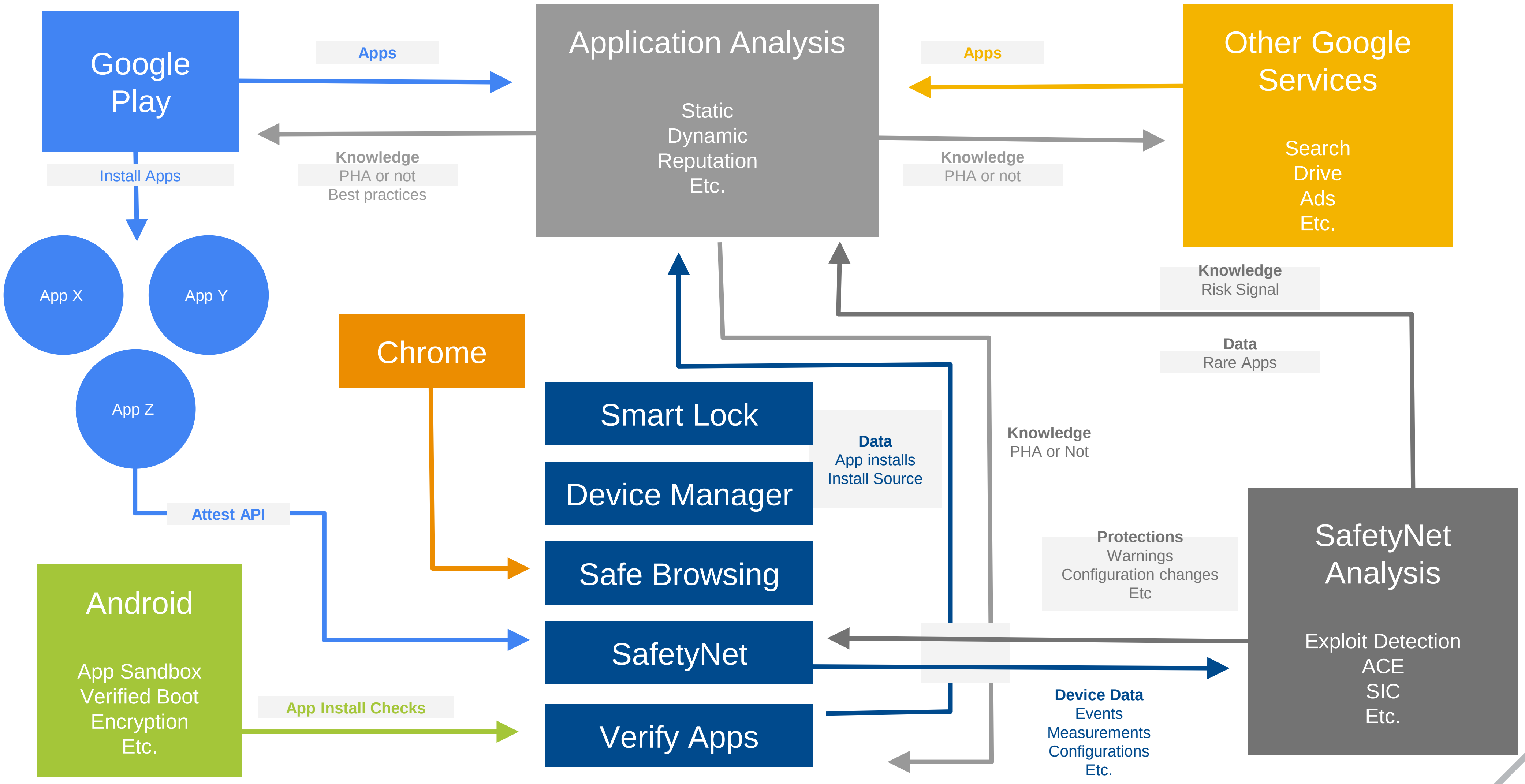
Verify Apps

Sensor Network

Android Device Manager

APIS

Architecture: Google's Safety Net for Android



ZEBRA

2 billion
devices protected

1+ billion
device scans per day

50+ billion
apps checked per day

1

Robust Platform

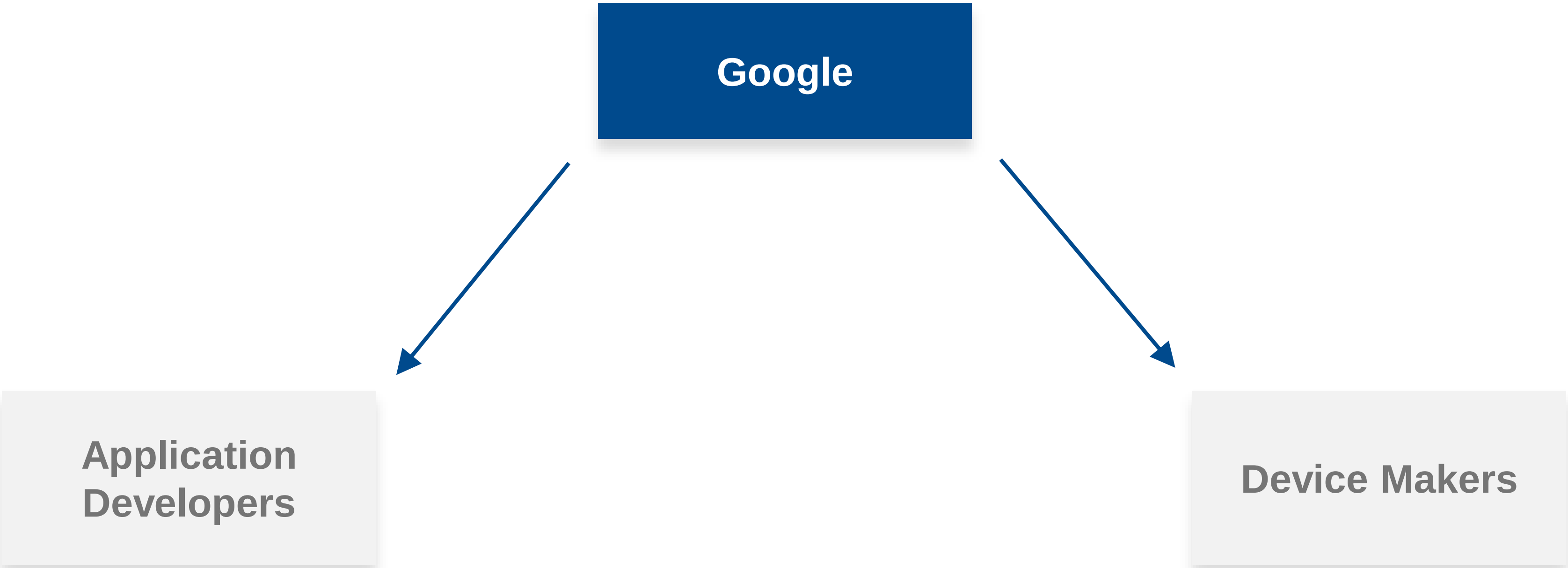
2

Comprehensive Services

3

Ecosystem Updates

Ecosystem Wide Updates

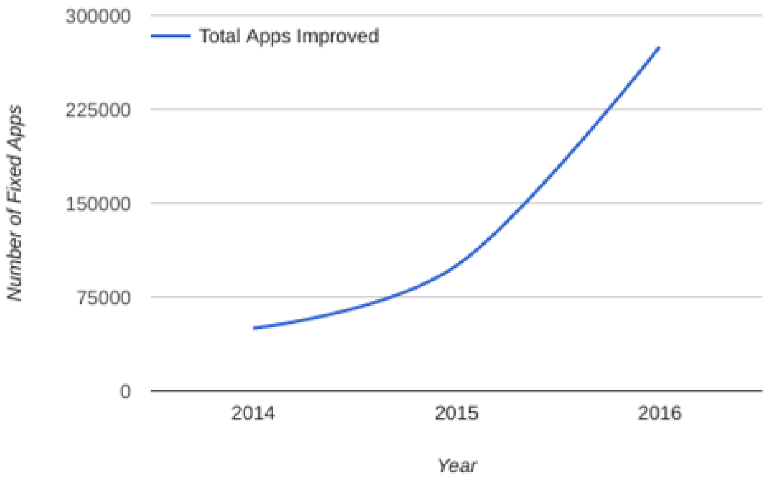


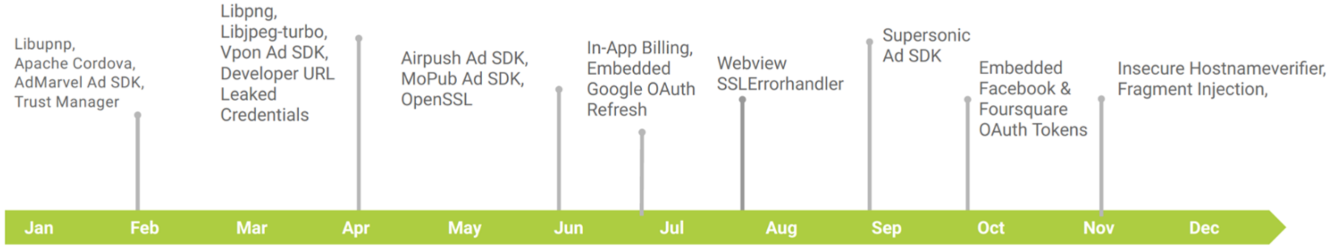
Google

Application Developers

Device Makers

Application Security Improvements





Libupnp, Apache Cordova, AdMarvel Ad SDK, Trust Manager

Libpng, Libjpeg-turbo, Vpon Ad SDK, Developer URL Leaked Credentials

Airpush Ad SDK, MoPub Ad SDK, OpenSSL

In-App Billing, Embedded Google OAuth Refresh

Webview SSLErrorhandler

Supersonic Ad SDK

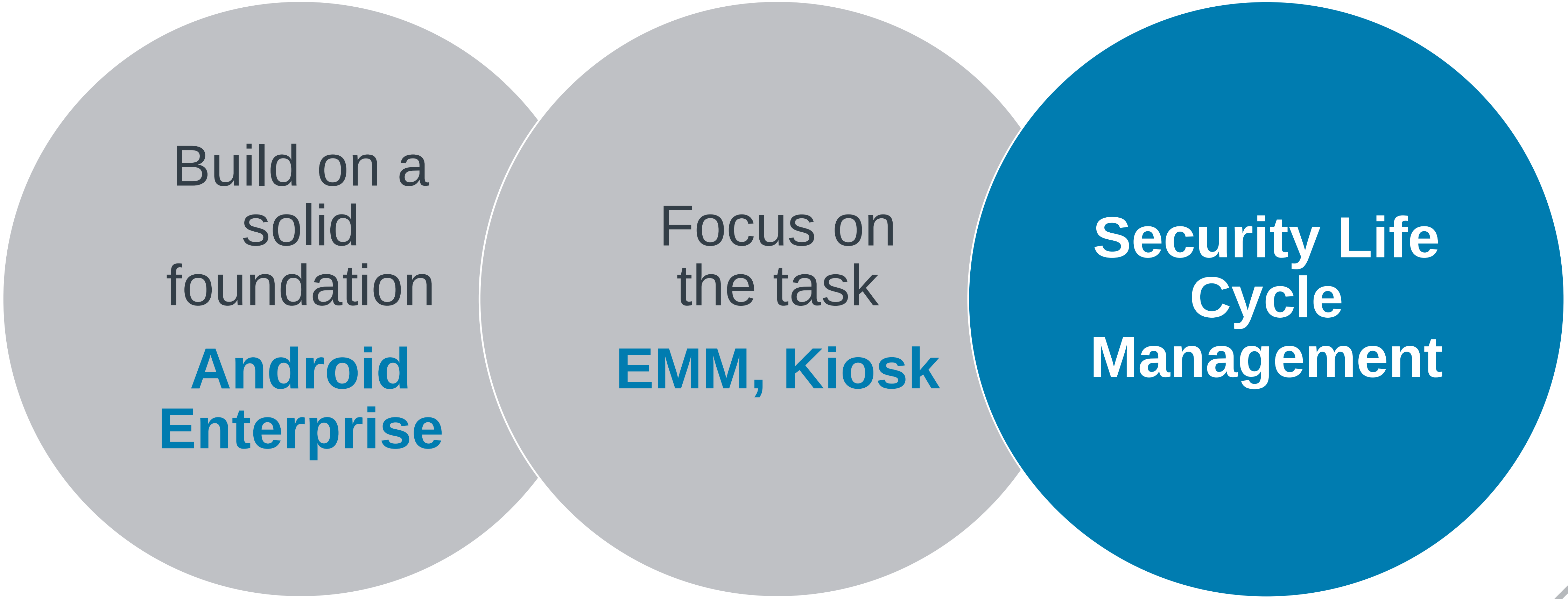
Embedded Facebook & Foursquare OAuth Tokens

Insecure Hostnameverifier, Fragment Injection,

Zebra’s role in Android devices security

ZEBRA

Zebra Security – 3 Key Paradigms



Build on a solid foundation

Android Enterprise

Focus on the task

EMM, Kiosk

Security Life Cycle Management

LIFEGUARD FOR ANDROID

Zebra Extended Life Cycle Security Support

HOW TO SECURE ENTERPRISE PLATFORMS?

1. Enterprise Demand New OS Platforms
2. Consumer Market Adoption is required
3. Successful Consumer OS Will Be Aggressively Attacked

30 Day / Quarterly Security Patch Updates

Zebra Extended Life Cycle Security Support

HOW DO I STAY SECURE MEETING MY TOTAL COST OF OWNERSHIP GOALS?

1. Consumer Operating Systems Have limited security support life
2. Enterprise Customers keep devices in services for 5yrs or more.

Security Patches 2+ Years Beyond End-of-Sale

ZEBRA

Zebra Extended Life Cycle Security Support

HOW DO I STAY SECURE DURING OS UPDATES?

1 **Consumer Operating Systems**
Have limited security support life

2 **Enterprise Customers keep**
devices in services for 5yrs or more.

Security OS Transition Period (OTP)

Zebra Extended Life Cycle Security Support

Zebra vs Consumer

		Typical Consumer	Zebra
Device Life Cycle	Device Avail for Sale	No commit, <2yrs	3, 4 or 5yrs
	Post End of Ship Service	None	Additional 3, 4 or 5yrs
	Typical Customer Device Refresh	24-29 months*	3-7yrs +
Security Life Cycle	30 Days Security Updates	Some Vendors	Yes[1]
	Security Patch Level Indication	Yes (M+)	Yes (M+)
	Update Duration from First Ship	36 months / 40 months	*60 months / 84months
	OS Transition Period	None	12 months
	Extended OS Transition Period	None	Available ($)

[1] Security Updates released every quarter during the extended life cycle

The most important defense against mobile device security threats is to ensure devices are patched against publicly known security vulnerabilities and are running the most recent operating system version. Installation of patches ensures that devices cannot be trivially targeted with well- known public exploits, but rather an attacker must invest time, resources, and risk of detection into developing more sophisticated attack methods. Running the most recent operating system ensures devices are benefiting from general security architecture improvements that provide resilience against vulnerabilities that may not yet be publicly known.

Source: USA Department of Homeland Security: Study on Mobile Device Security: link

References

- Android security bulletins: https://source.android.com/security/bulletin/index.html
- Android Security 2016 Year in Review: https://security.googleblog.com/2017/03/diverse-protections-for-diverse.html
- LifeGuard for Android: https://www.zebra.com/us/en/products/software/mobile-computers/lifeguard.html

THANK YOU

ZEBRA