RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: BR-W01

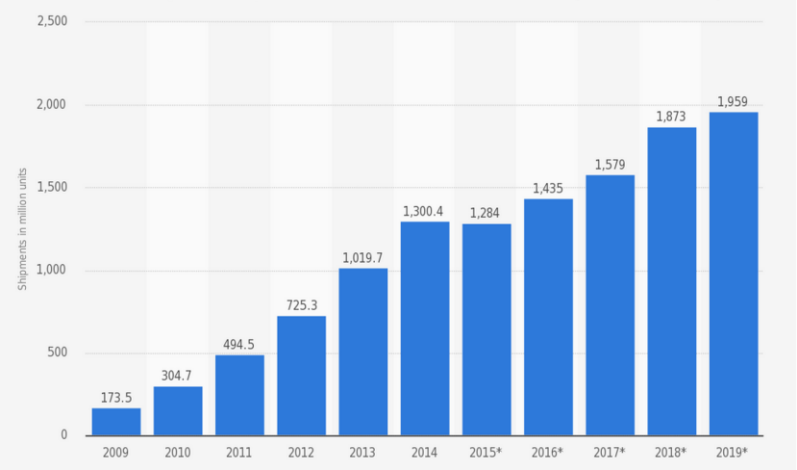
But... It's an App/Play Store Download: Research Exposes Mobile App Flaws

Andrew Hoog
CEO and Co-founder
NowSecure
@ahoog42

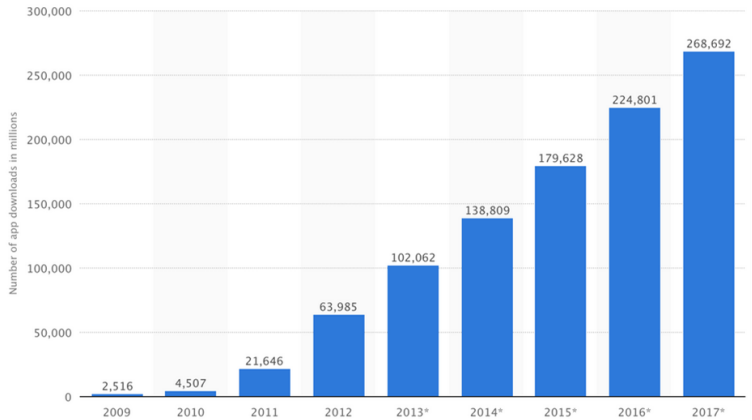
Ryan Welton
Engineer
NowSecure
@Fuzion24

Mobile is different

Global Smartphone Shipments



Mobile App Downloads



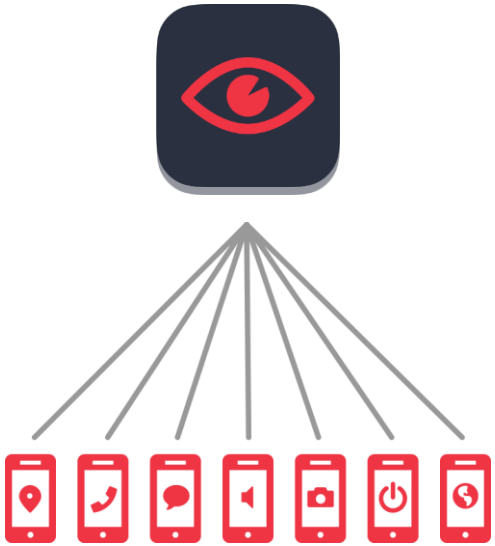
Source: http://www.statista.com/

It's vulnerable

48%

of Android apps have at least one high risk security or privacy flaw

It’s not very private



50% of Android users have an app that can do all of the following:

- Read precise location
- Read phone log
- Read sms
- Record audio
- Use camera
- Start on boot
- Connect to internet

Our research

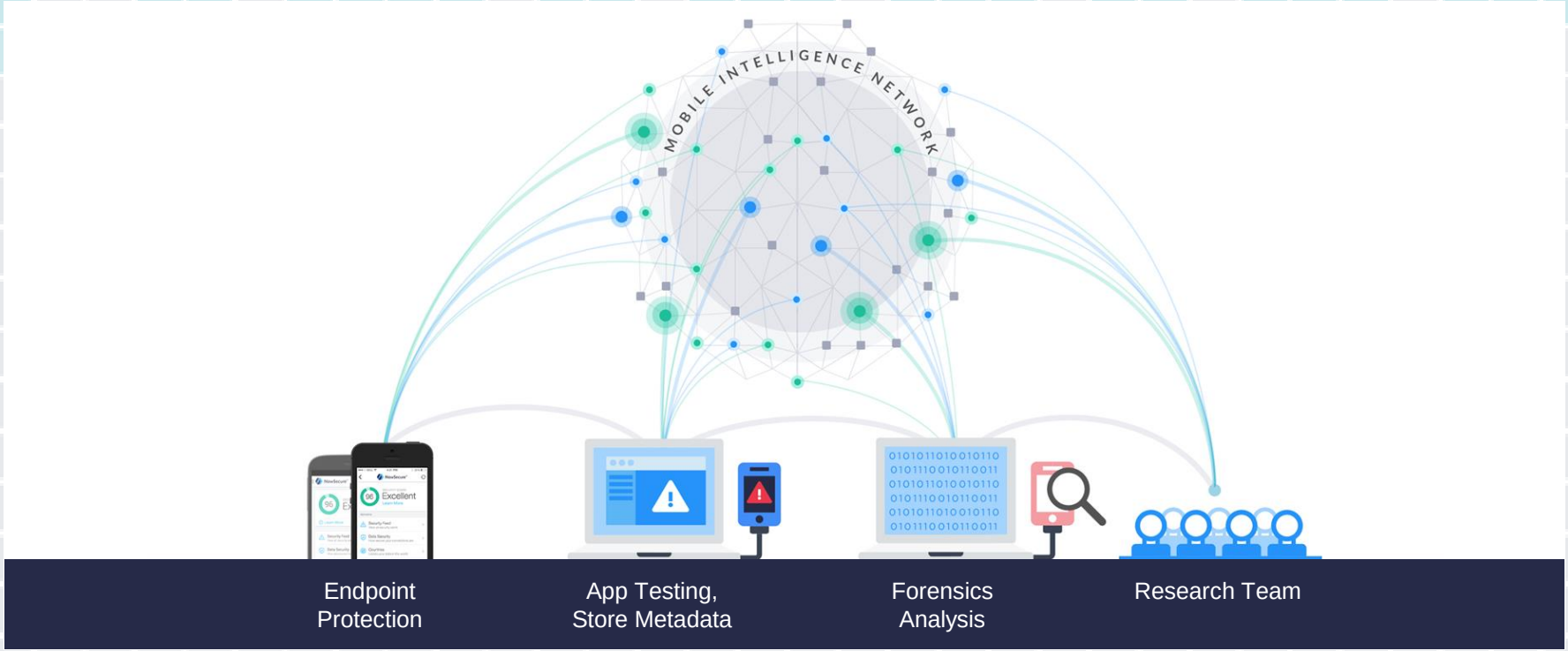
Current Tests

- Network Issues
  - Improper SSL
  - Weak Android APIs allowing file write
  - Dynamically loaded code
  - Sensitive data leakage
- Local Issues
  - Dangerous world r/w local files
  - Weak content providers- read/write files in app context

Future Work

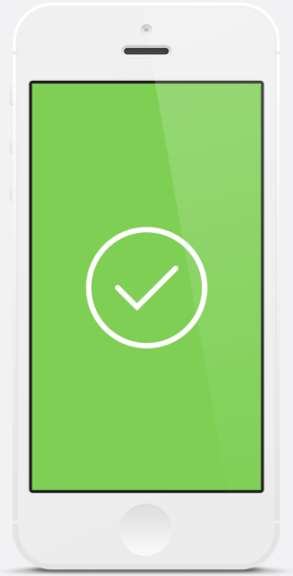
- More extensive IPC endpoint testing
- Identification of weak crypto
- More intelligent app navigation
- Forced execution flow/state

Crowdsourced data



UI automator

- Automated human app use
- High volume dynamic app testing
- Tested 62,000+ apps



Three compelling vulnerabilities

- Data leakage
- Improperly validated SSL
- Remote code execution

Data leakage

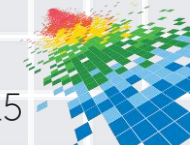
15%

of all apps leak sensitive data over the network

(plain text or encoded)

9.6%

of apps on device leak data



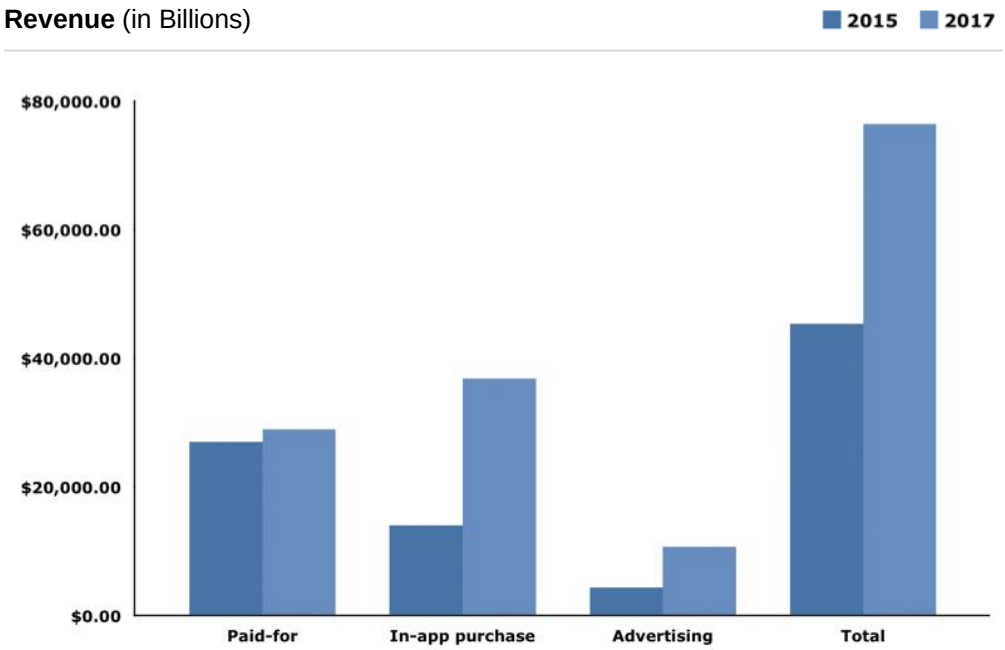
Data leakage

- **Demo #1:** Data leakage
- **Example:** ZERO Launcher
- **Popularity:** 50mil+
- **Vulnerability:** Leaks GPS coordinate to within feet and the serial number of your phone
- **Implication:** A passive network attacker can uniquely identify you and keep tabs as you move around

Apps define our lifestyle

- Mobile blurs the line between public and private
  - Individuals
  - Industries
  - Customers
  - Employees
  - Vendors
- Apps manage every aspect
- UX more important than security

And it's big money



- 180B app downloads projected in 2015
- 93% of apps free
- $45B projected revenue in 2015 with 30% CAGR
- In-app purchases and ads driving revenue growth and app download volume

Source: Gartner (September 2013)

With big flaws

CORRUPDATE

The Samsung vulnerability compromised more than

200,000,000

mobile devices

Of the 62K+ apps we tested...

36% have at least one world readable file

-

23% have at least one world writable file

-

12.3% leak IMEIs

-

5% leak MAC addresses

-

4% allow arbitrary network file writes

The 5 riskiest app categories

Games | **59%**

-

News and Magazines | **55%**

-

Photography | **54%**

-

Comics | **53%**

-

Shopping | **51%**

Gaming apps

59%

of gaming apps have at least one high-risk issue

…and 75% of mobile users have a gaming app on their device

Even the 5 least risky categories have issues

Libraries | **25%**

-

Media and video | **28%**

-

Finance | **29%**

-

Medical | **33%**

-

Health and Fitness | **36%**

Improperly validated SSL

10%

of “family” games

7%

of shopping apps

6%

of social apps

Improperly validated SSL

10%

of all apps with improperly validated SSL are finance, social, travel or shopping apps

Improperly validated SSL

- **Demo #2:** Improperly Validated SSL
- **Example:** key.me
- **Vulnerability:** Traffic intercepted includes username + password, GPS coordinates, and images of house keys
- **Implication:** the attacker can gain GPS coordinates and image of the key to your home to create a physical copy of your key

The average device has...

3 vulnerable gaming apps

6 vulnerable tool/utility apps

Of all the apps which run superuser (SU)

58%

are tools/ utilities

Financial app insecurities

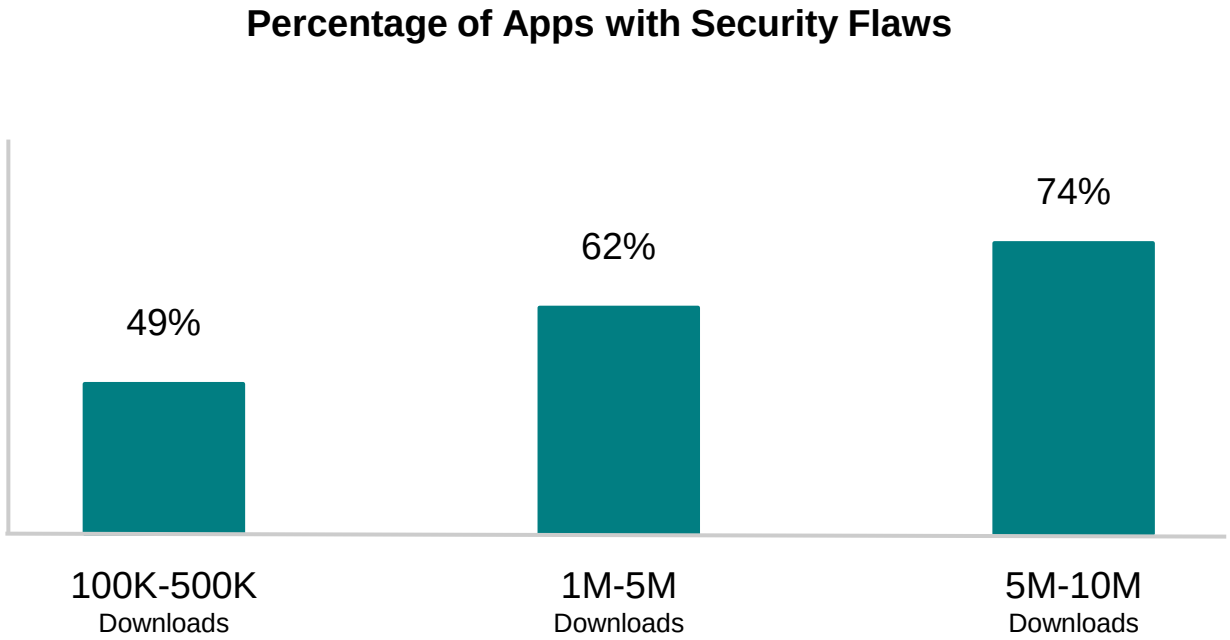
Of all finance apps...

28% had at least 1 issue

6% have sensitive data leak

1% leak superuser capabilities

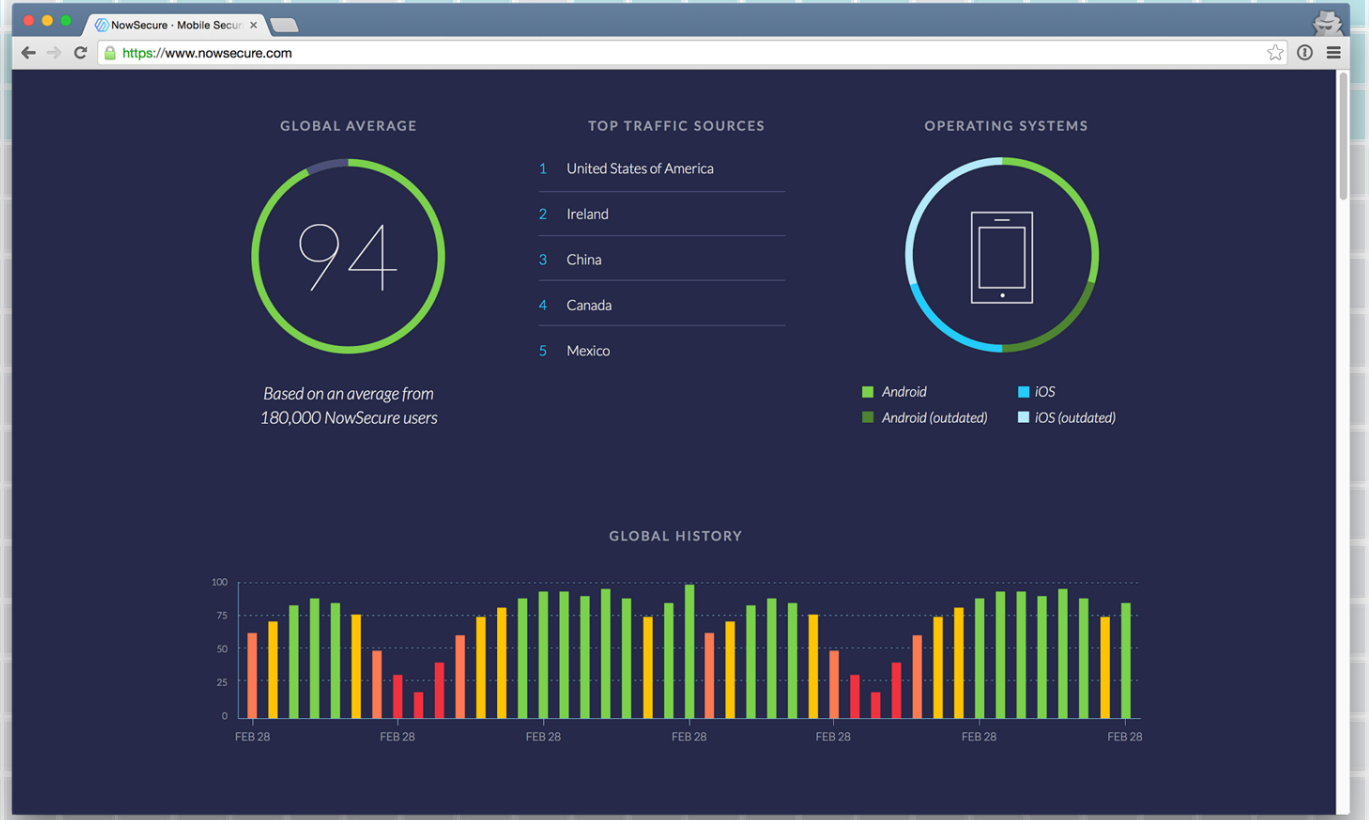
More downloads, more flaws



Remote code execution

- **Demo #3:** Remote code execution
- **Example:** SimSimi
- **Popularity:** 10 mil+
- **Vulnerability:** A network based attacker can modify traffic to gain control of the device
- **Implication:** the attacker can access the device and control it completely, including syphoning personal data (texts, pictures, emails, etc)

Mobile can be more secure.



http://www.nowsecure.com/intel/

What you can do about it

- Individual
  - Track your own device
  - Use fundamental security settings
- Enterprise
  - Develop apps with best practices
  - Test apps for security flaws
  - Invest in mobile security for employees and the entire ecosystem
- Industry
  - Advance disclosure standards
  - Remediate vulnerabilities more quickly

Applying what you have learned today

- Starting immediately...follow mobile development best practices
- Within one month...review your QA process to include not just bug fixes, but security testing
- Within six months...define and revise your budgets to ensure that you invest in the right tools, resources, processes and people

RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: BR-W01

Mobile Security.

It's different. It's possible.

Andrew Hoog
CEO and Co-founder
NowSecure
@ahoog42

Ryan Welton
Security Researcher
NowSecure
@Fuzion24