RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

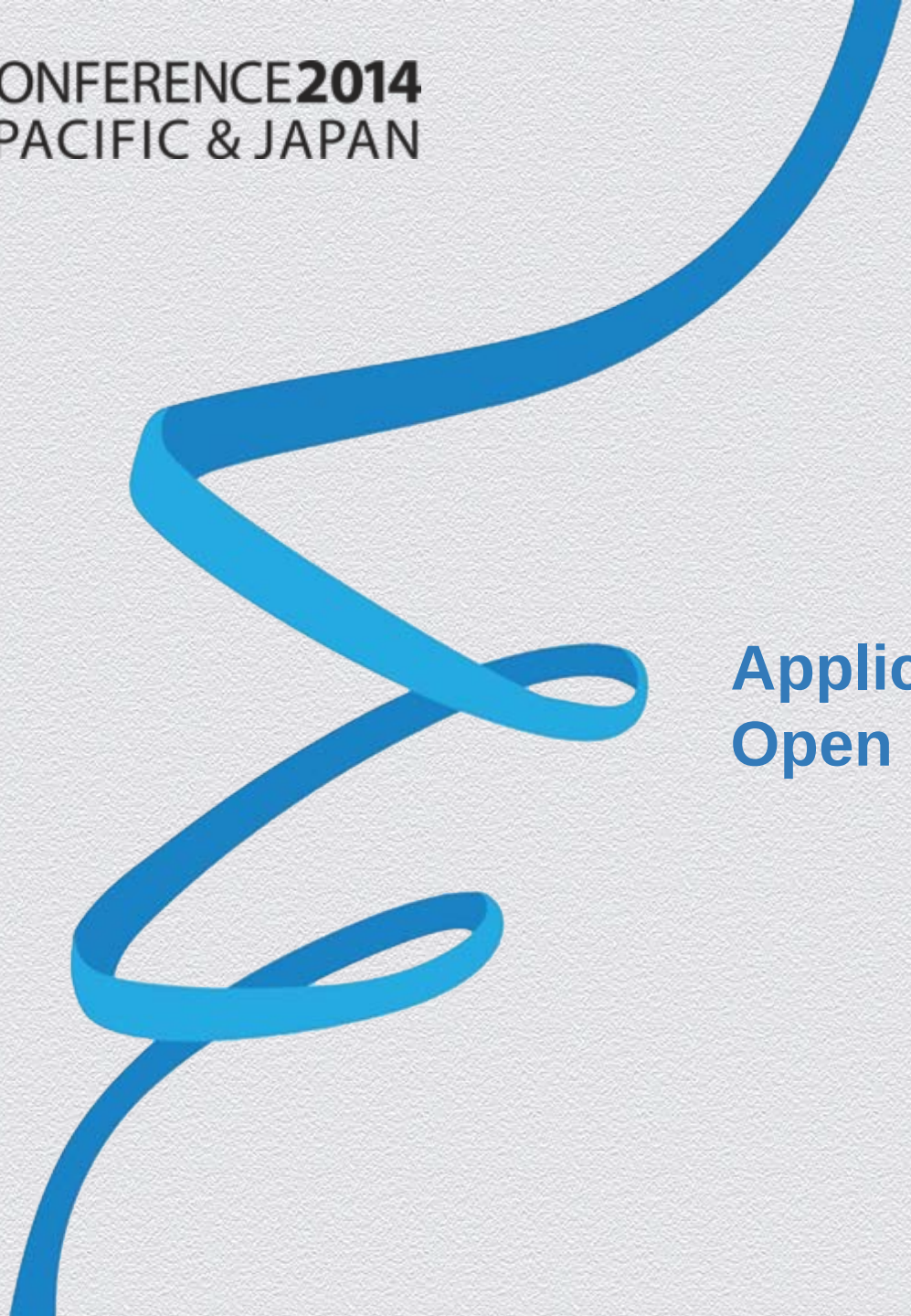
Third Party Components in Applications: Understanding Application Security

SESSION ID: MBS-W08

Olli Jarva

Chief Security Specialist, APAC
Codenomicon, Singapore
@ollijarva

#RSAC



Applications and Open Source

Open Source Components in Mobile Software

- 80-90% of mobile software consists of re-used libraries
- Most – open source
- Some – overlapping
- 26-96% of mobile software has known vulnerabilities (depending on platform and developers)
- Closed source – also subject to vulnerabilities

Open Source Components

- No need to re-invent the wheel
- Affordable
- In theory, multiple developers means better quality
- Can be combined to create brilliant things
- End products, inherit vulnerabilities and licensing issues

Open Sources Vulnerable

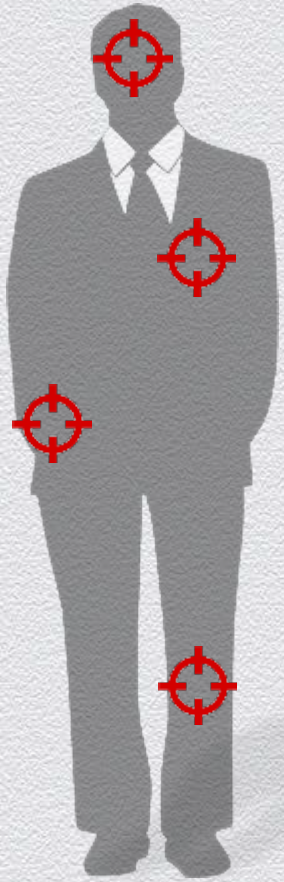
- Middleware libraries
- Common Unix-daemons
- Embeddable services
- Utility libraries
- Encryption libraries
- Kernels

And more...

Vulnerabilities are Everywhere

Where do the vulnerabilities come from?

- Immature / Malfunction processes
  - Operating systems, Applications, Anti-{malware/virus/spam} not up-to-date
  - Users fall victim to social engineering
  - Poor or incorrect configurations
- Poorly implemented software
  - Unknown (and known) vulnerabilities
  - Logic errors in implementation
  - Poor software design and architecture



What is the Impact of These Vulnerabilities?

- Software = Bugs
- Some vulnerabilities act intentionally or unintentionally
  - Leak information
  - Behave maliciously
  - Do other nasty things behind the scenes that user is not aware of
- BYOD policies can reveal a larger issue
- How do we counter this situation?

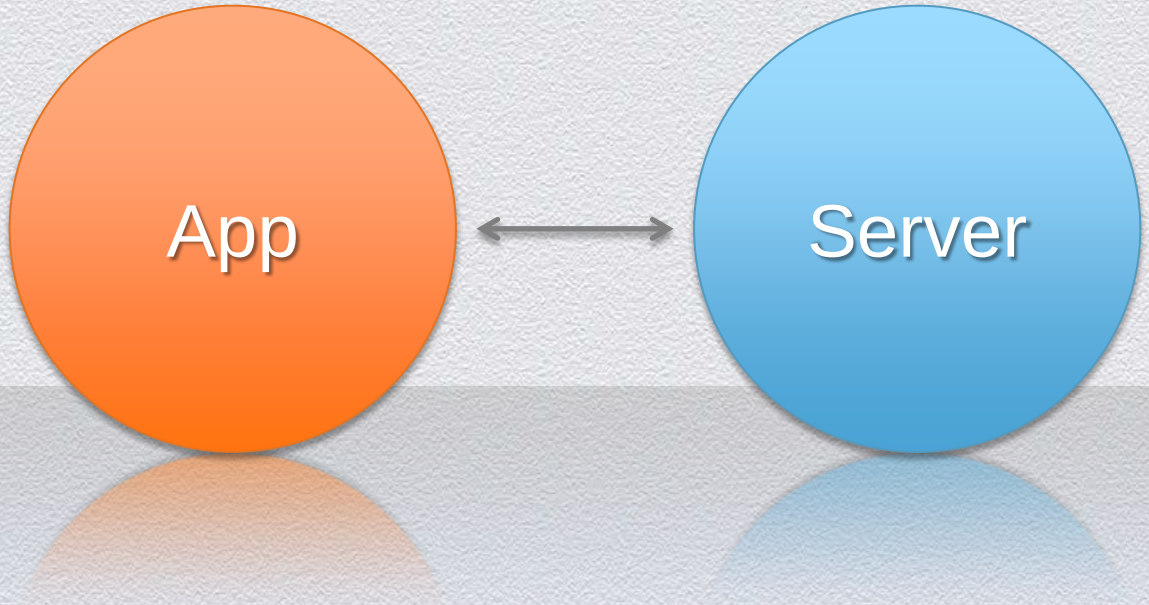
Who is in Charge?

- End users
- Policy-makers and their enforcers
- Developers
- *Combination of all above*

How Do We Make Sure We Know What the Applications are Doing…

- …Consequently, how do you choose what to use?
- Issues are invisible to the users – this all happens behind screens
- Are there any platform issues related to choosing what we have at use?
- Testing?

Example of a Good Application Behavior



Example of Bad Application Behavior

Application sends…

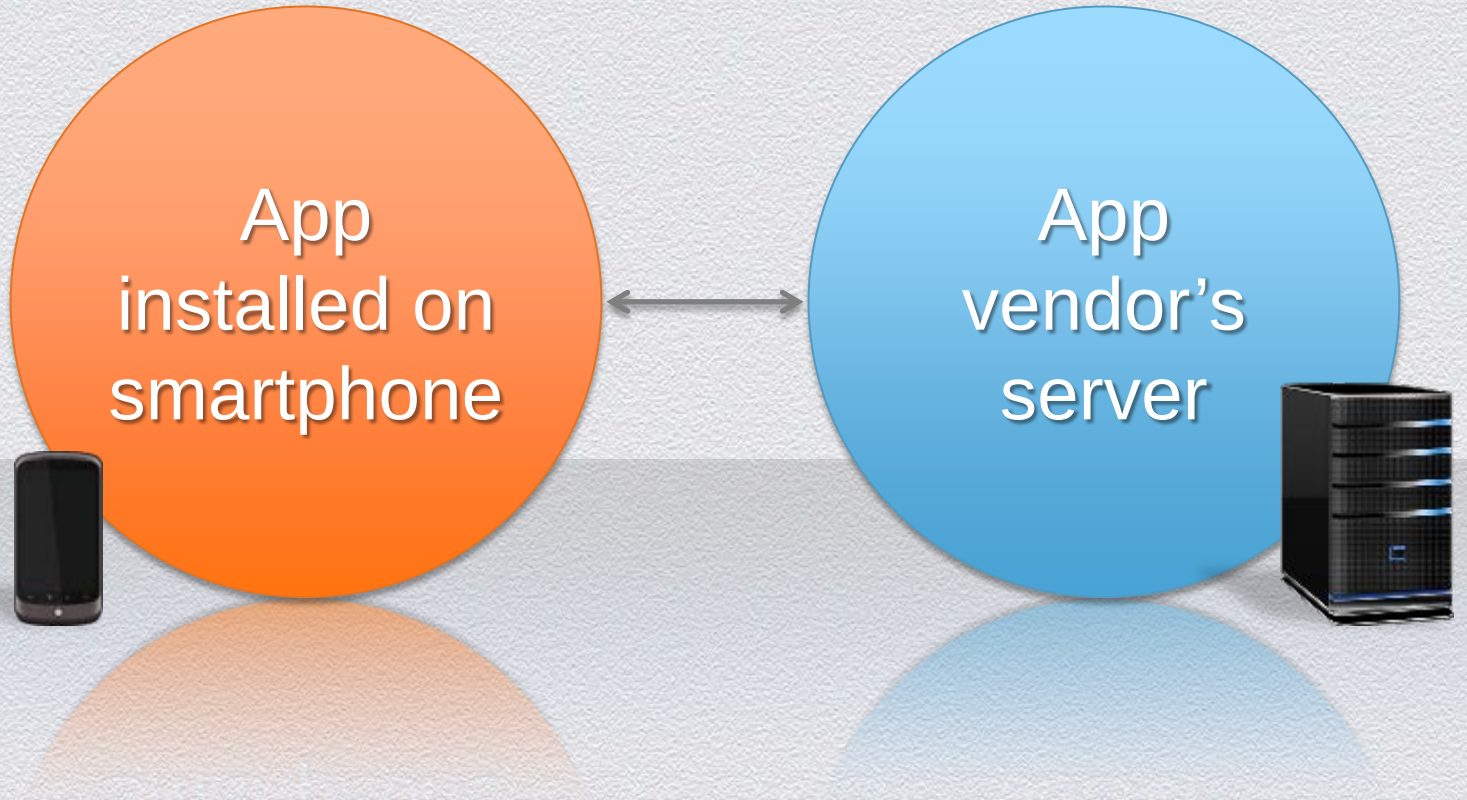
- Irrelevant information
- Too sensitive information
- To server, and also…
- Third, fourth and fifth parties

Applications and Vulnerabilities

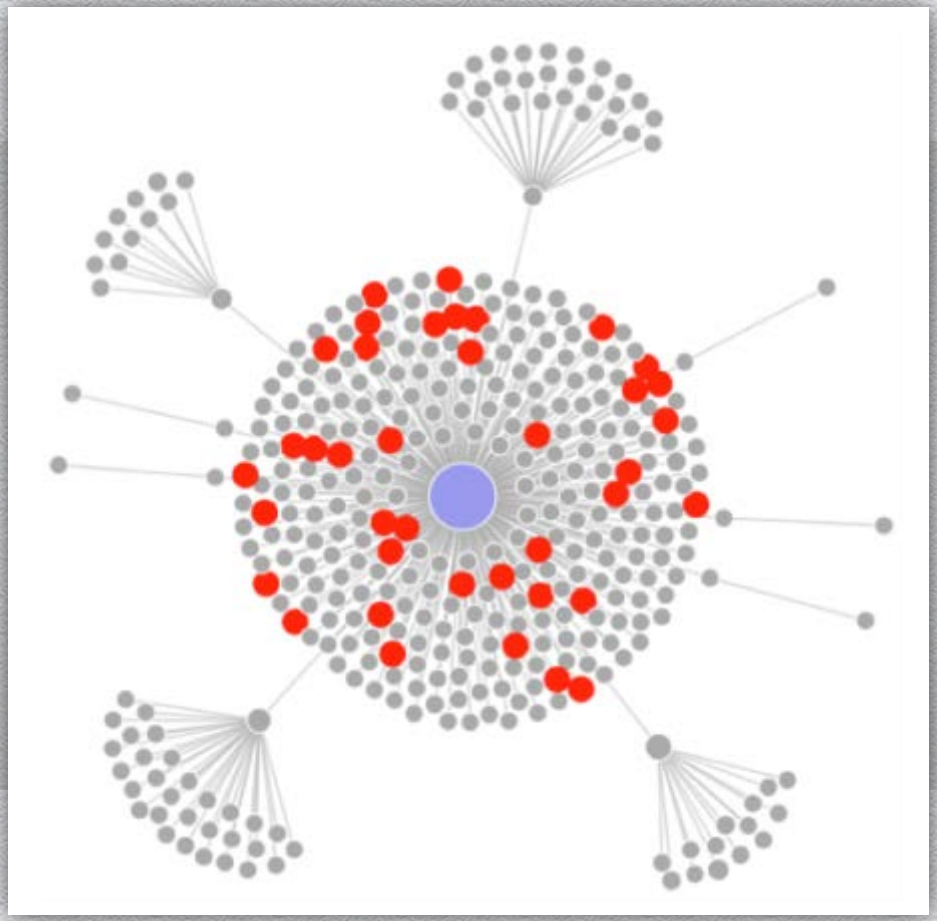
What Makes Applications Vulnerable

- Many Mobile Applications use Open Source libraries
  - 80-90% of mobile software consists of re-used libraries
- Commonly used libraries:
  - OpenSSL
  - Image handling (PNG, TIFF and so on)
  - Curl
  - Freetype
  - Zlib
- Many Mobile Applications connect to Ad networks
- May be stack issues

Communication in a Perfect World



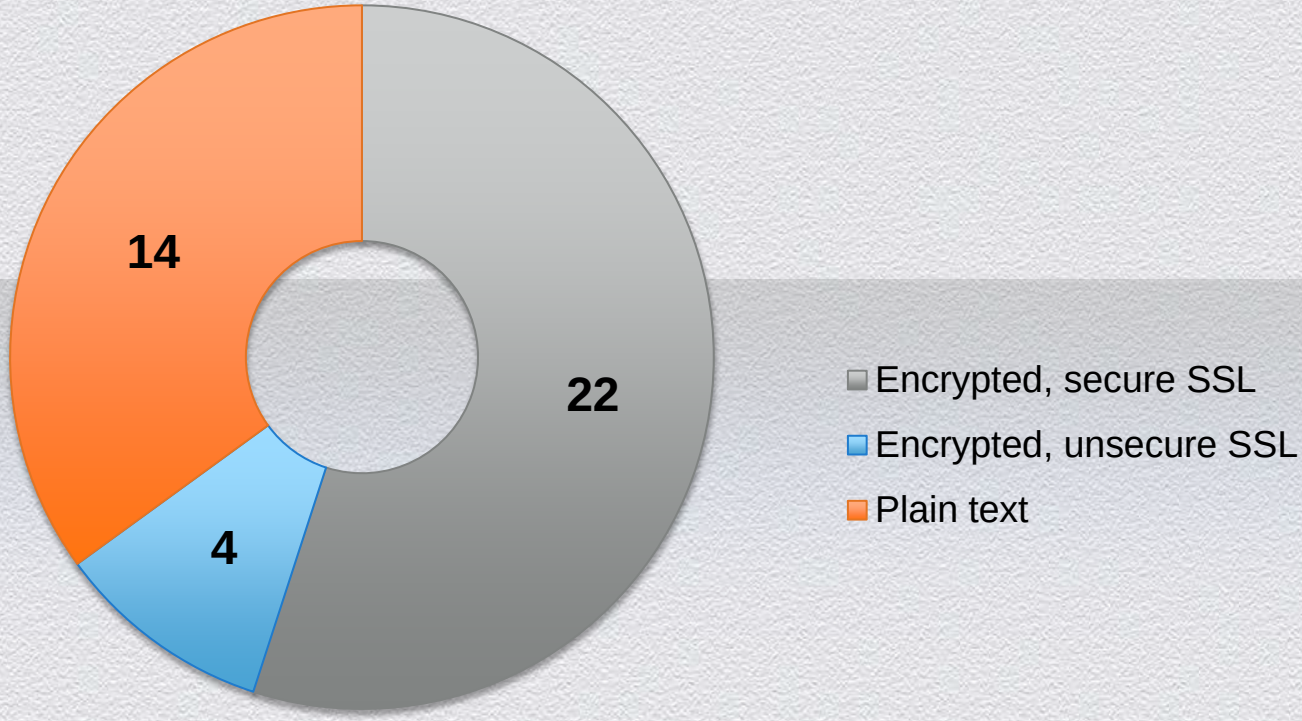
The Reality is Something Else



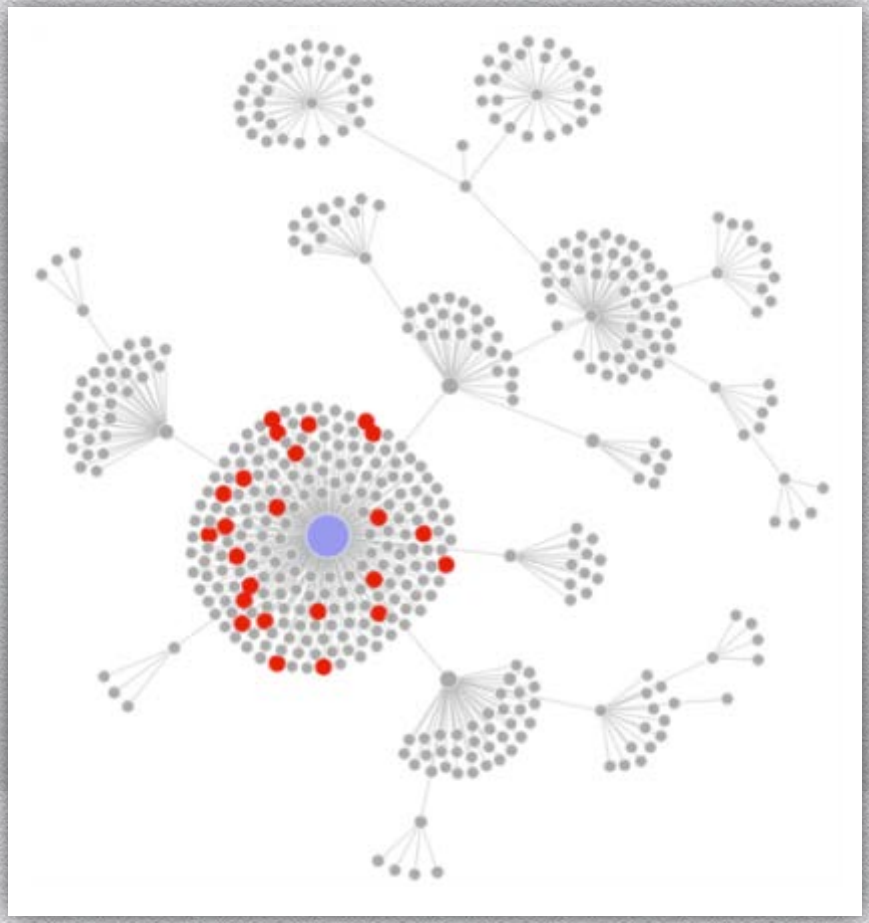
Private information is being shared to outsiders (IMEI, Android ID, Contacts, etc.)

Private Information

How Private Information is sent



And it Just Gets Better



When Problems Surface…

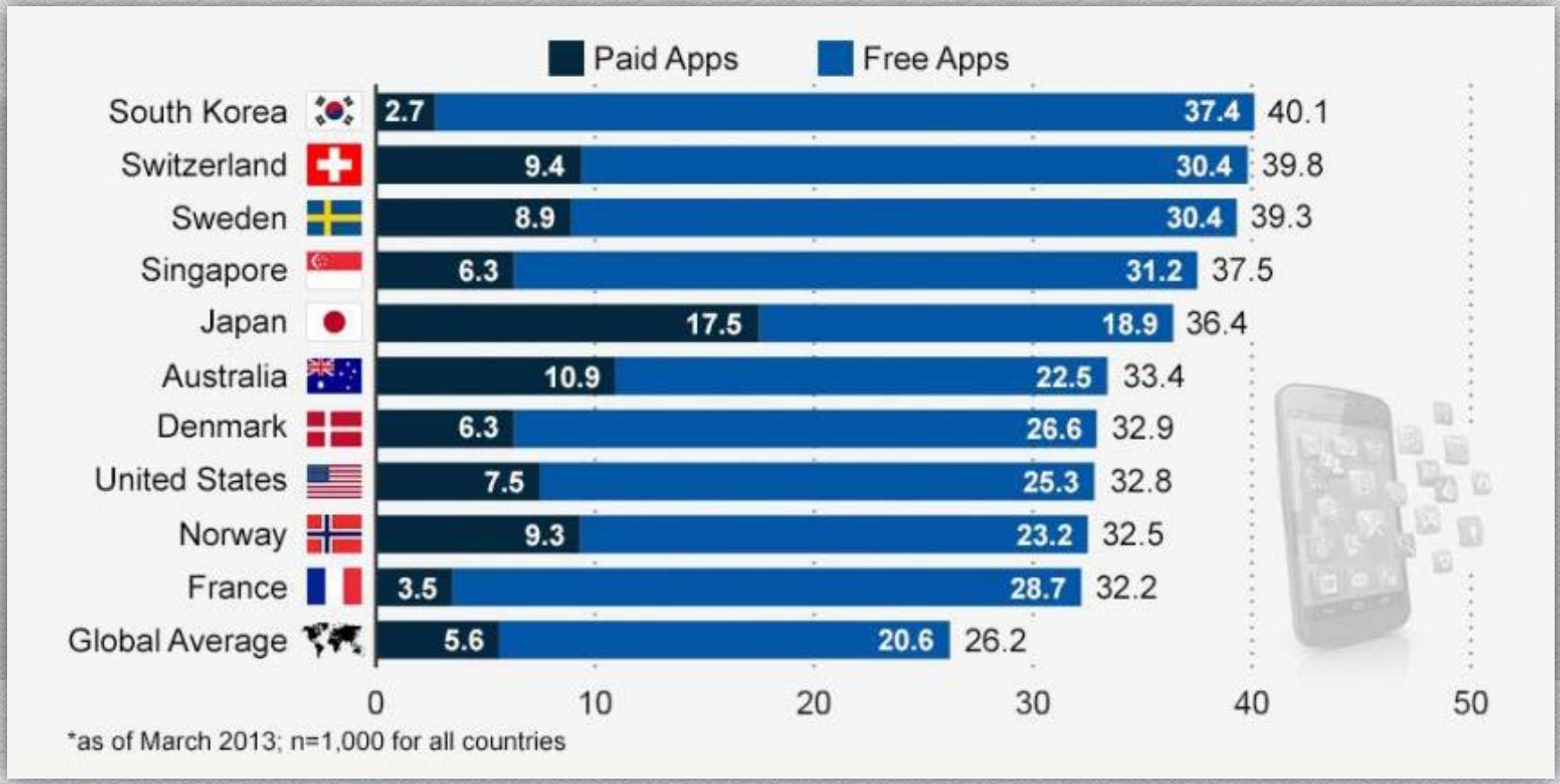
- Consider possible issues when we use Applications in BYOD environments
- New issues:
  - Privacy
    - What others are knowing about our daily life, our behavior of doing things?
  - Security
    - What might be the impact of Malicious user utilizing vulnerability in end users device, exposing company secrets?
  - Confidentiality
    - How are we limiting the access or places for certain types of information?
  - Availability
    - Is there a possibility that our availability might be compromised by Malicious application?

Where Do We Stand Now?

Today's Landscape

- Top 50 android apps and their behavior
- How many Applications are connecting to Ad Networks?
  - Sharing your private information without user awareness?
    - Location
    - Contacts
    - IMEI code
    - Android ID
- How many endpoints do the applications have?
- What private information is being shared?

Application Downloads
(Singapore Above Average, ~37 Apps)

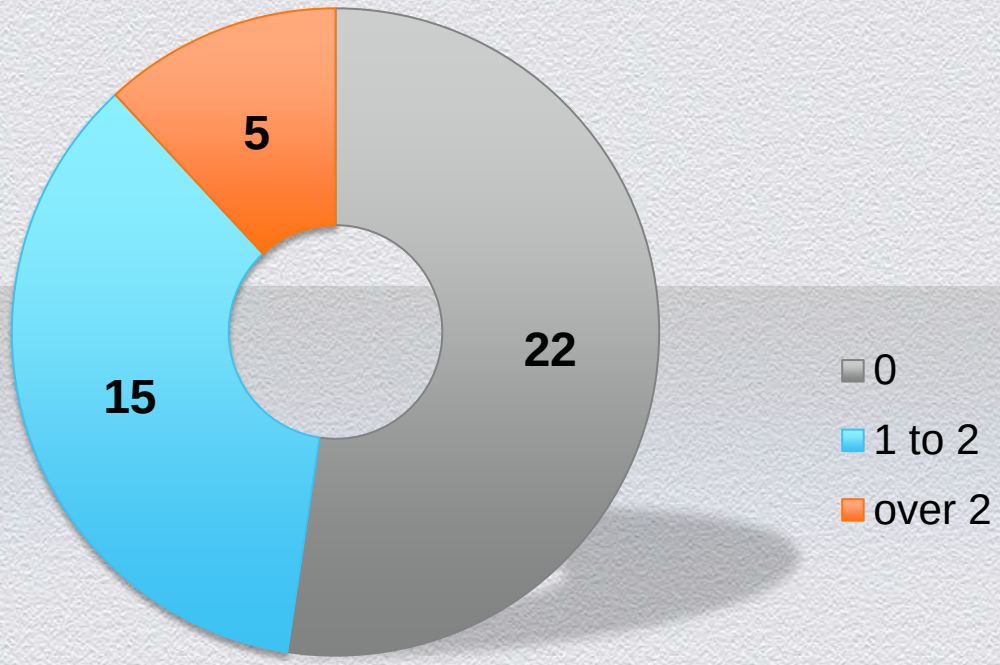


Source: Mashable

The Issue is Privacy – Ad Networks

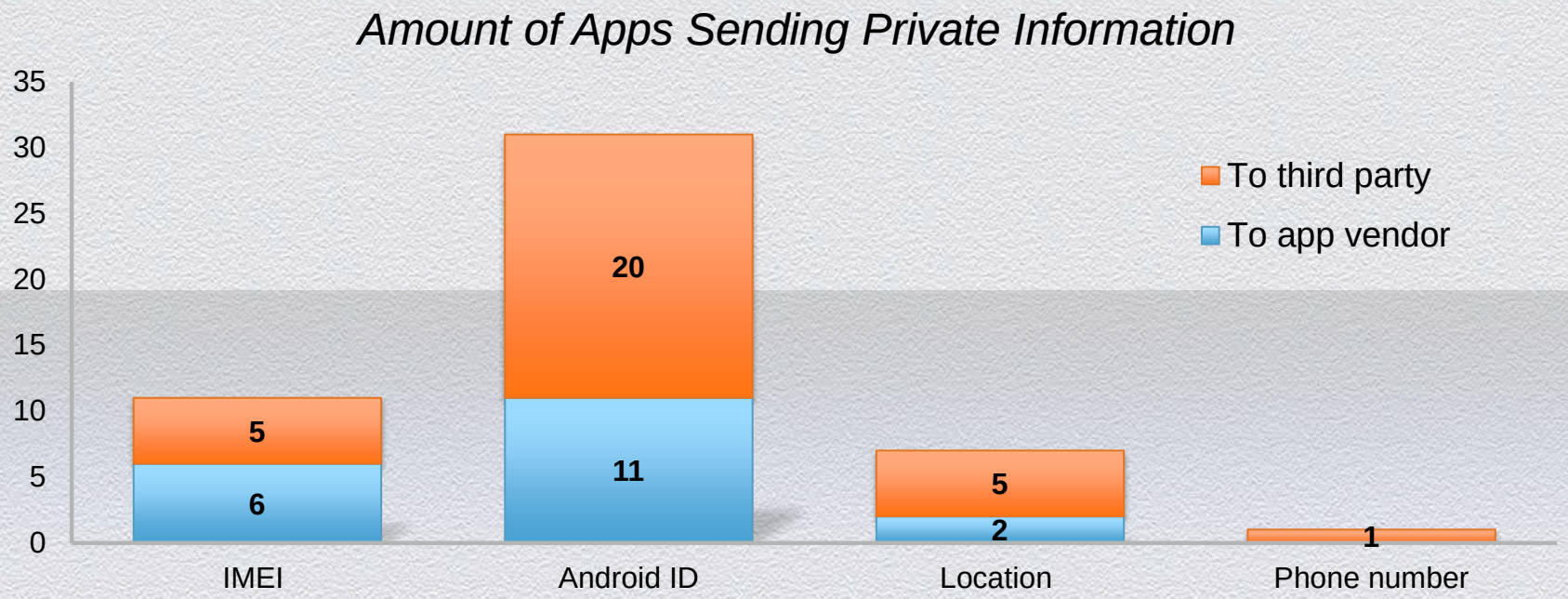
Ad Network leaks – information types that should be controlled

Amount of Ad Networks



The Issue is Privacy – Mobile

Security and Integrity: Application morale and behavior of handling information is related to privacy



Five New Threats to Your Mobile Device Security

1. Mobile phishing and ransomware
2. Using an infected mobile device to infiltrate nearby devices
3. Cross-platform banking attacks
4. Cryptocurrency mining attacks
5. The enemy is us

- Home WiFi, work WiFi or Starbucks WiFi?
- Devices with vulnerabilities on these network…
- Can be exploited directly from the infected mobile device

Not Only Mobile

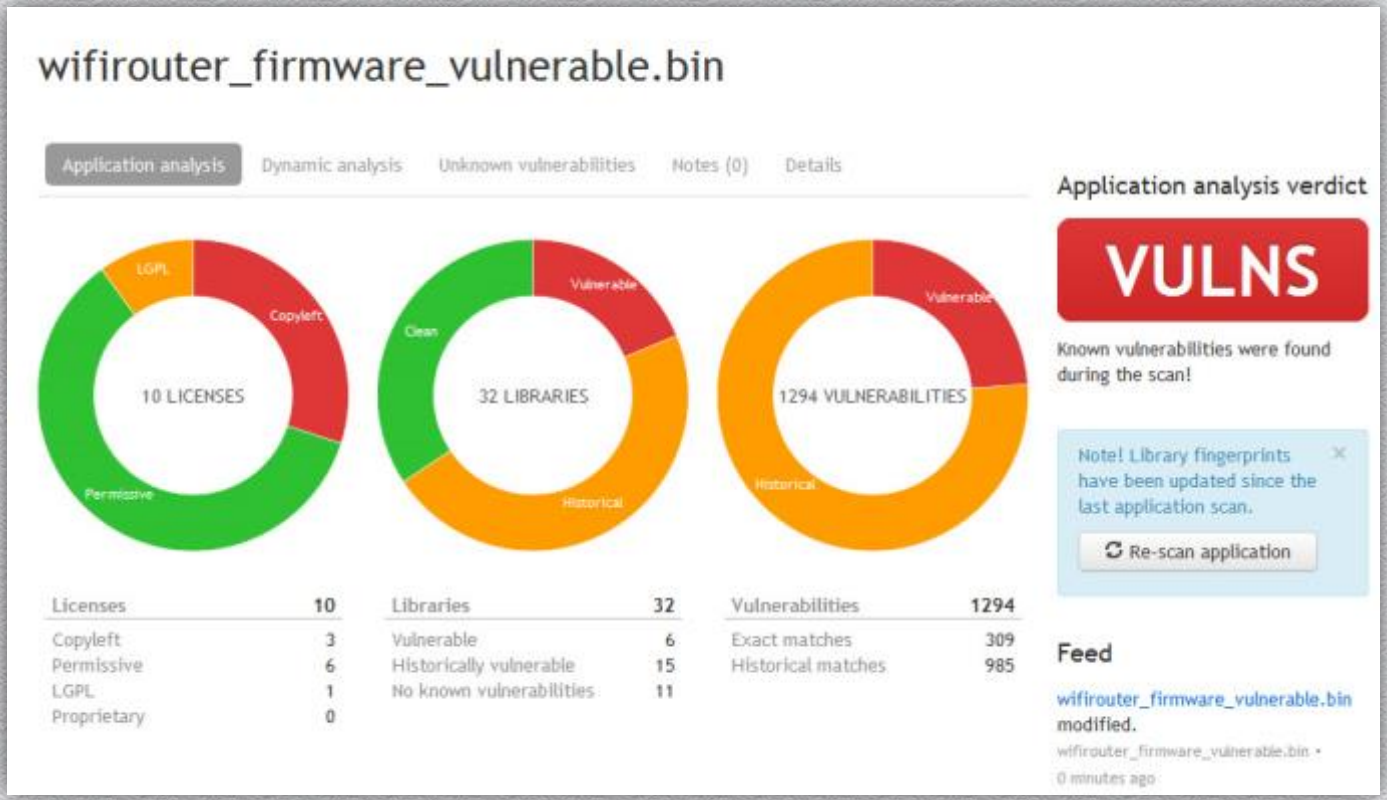
- The Internet of Things is already here
  - Printers, network-attached storage units, wifi-routers...
  - ALSO smart TVs, consoles, connected climate control systems...

Some Results: Network Printer

- Known vulnerabilities
- Copyleft license

More Results: Wireless Router

- Vulnerable libraries and restrictive licenses



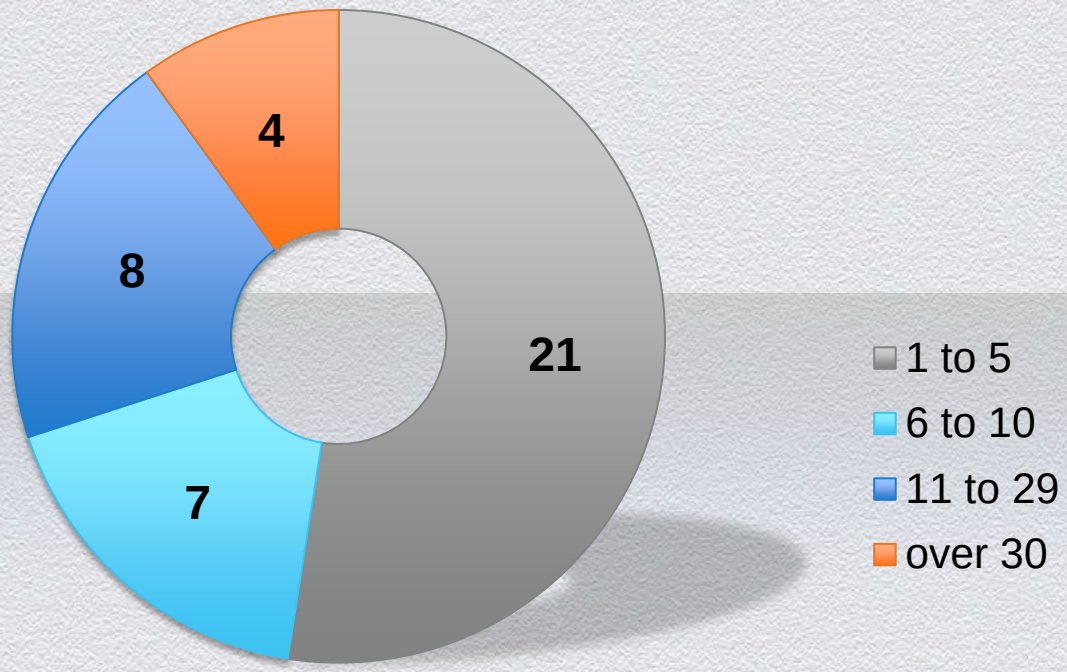
The Big Issues

- More and more devices communicating
  - Not secure enough
- Not only consumer issue – companies face similar problems
  - Smaller companies have less resources
- Unavailability, information leaks, and lost customer trust are issues
  - CEO’s problem, also the CMO’s problem and budget

The Issue is Availability – Amount of Endpoints

Compromising Availability

Without availability, privacy, integrity, confidentiality are irrelevant.
If the systems are down, what else is there?



We Can Fix This

From the Experts

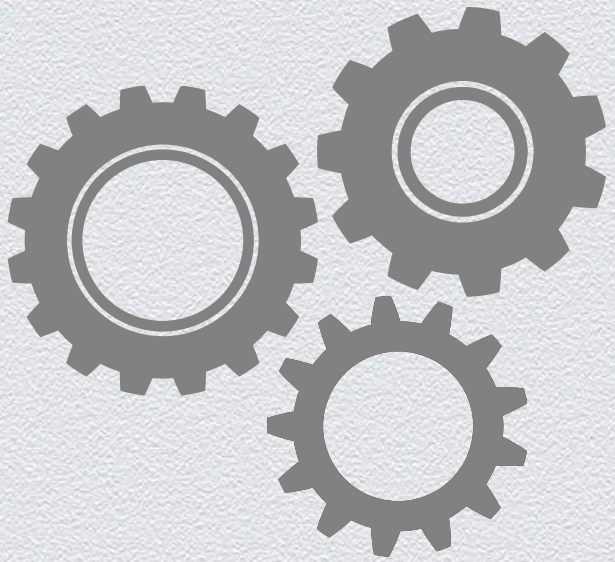
- Changes can be made, yet are temporary
  - Open Source is free, yet not foolproof
  - Community effort to make libraries safer
  - Heartbleed revealed, we can make the change quickly

Whitelisting Applications

- Challenges:
  - Enforcing white lists
  - Listing safe applications to be used
  - Maintaining the list up-to-date
  - Forcing people to consider security as a tier-one priority

Challenges in Development

- How do we make developers aware of the issue?
- Do they already know about it?
- What is the monetary impact, how do we solve it?

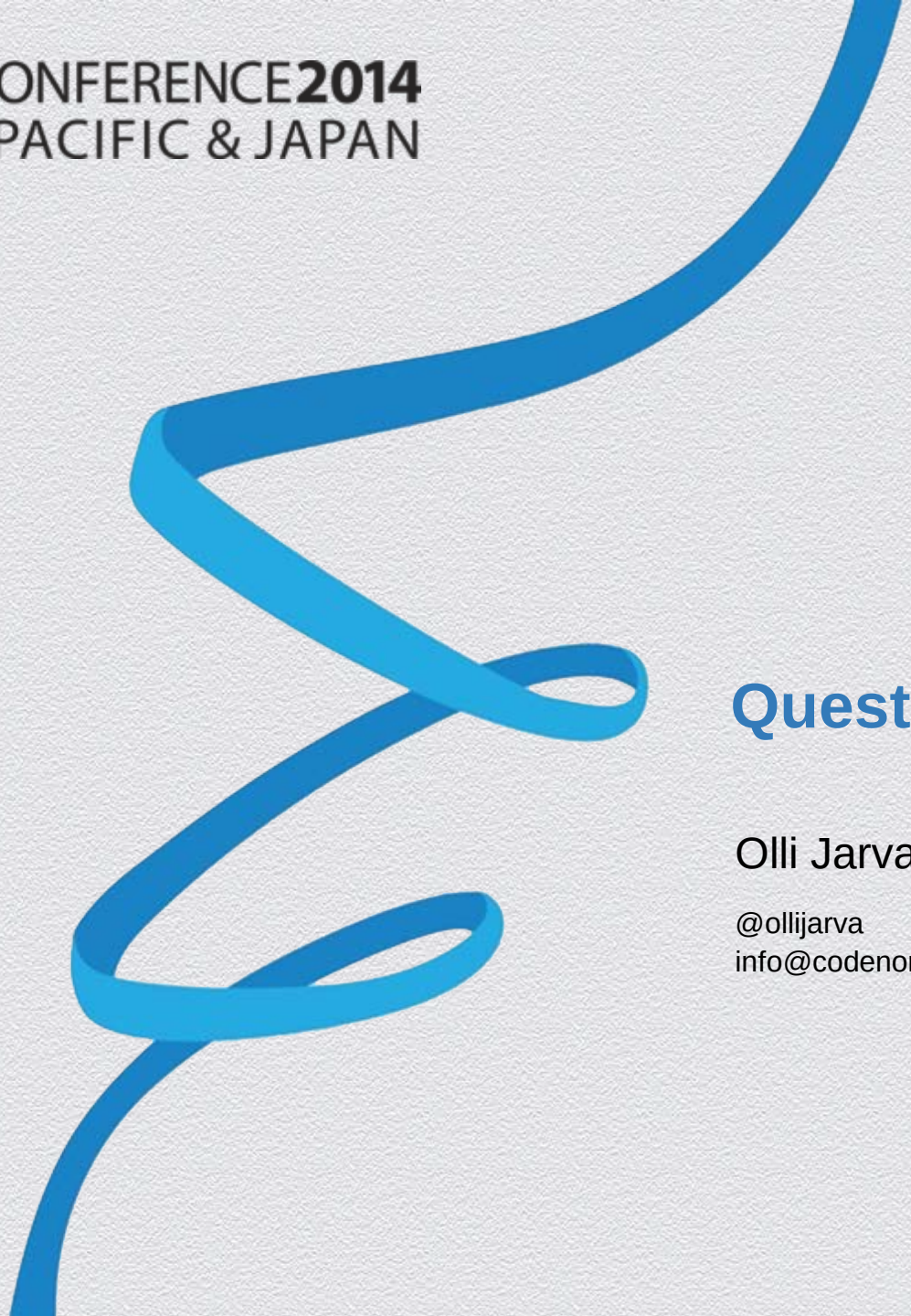


Customers' Viewpoint

- Single customer
  - Difficult as a single voice to be heard
- Demanding better and higher quality
  - Quality = higher cost
- Normally the motivating factor may not be security, until a failure occurs
  - Cheap = demand for low-end products

What's Next?

- The requirements are clear
  - Healthier, happier, and more productive
  - Perhaps…
  - Create software that is safer, reliable, "unbreakable"
  - Create software that integrates with everything



Questions

Olli Jarva

@ollijarva
info@codenomicon.com