CISPA
Center for IT-Security, Privacy and Accountability

UNIVERSITÄT DES SAARLANDES

Android Security Lab

Kick-off Meeting (06.10.2014)

Sven Bugiel, M.Sc.

Organizational matters

- Course agenda
- Registration

Organizational matters

Course agenda

Organizational: Lab Content

- Goal: Platform security of modern mobile operating systems at the example of the open-source Android OS
  - Basics of secure architectures
  - Android's security principles and architecture
  - Modern attack vectors against smartphone operating systems
  - Selected security extensions from research
  - Implementation of security extensions
- Credits: 6 ECTS

Organizational: Lab Procedure

CISPA Center for IT-Security, Privacy and Accountability

- **First half: Lecture Period** (06.10.14 – 10.10.14)
  - Room E1.1 2.06, 09:30-16:30 **s.t.** (lunch break 12:00-14:00)
  - Morning session: Lecture-style
  - Afternoon session: Supervised Exercise
    - Tutor: Tobias Theobald

Date	09:30 – 11:30	13:30 – 16:30
06/11/2014	**Lecture**: Motivation **Lecture**: Applications and application Layer	**Lecture**: Secure architecture principles and Android security architecture
07/10/2014	**Exercise**: Basic application programming	**Exercise**: Data sharing and Android security primitives
08/10/2014	**Lecture**: Attacks on Android	**Exercise**: Data sharing and Android security primitives (cont.)
09/10/2014	**Lecture**: Selected research works	**Exercise**: Extending Android's middleware and creating a custom ROM
10/10/2014	**Exercise**: Extending Android's middleware and creating a custom ROM	Optional slot for exercises

Organizational: Lab Procedure

CISPA Center for IT-Security, Privacy and Accountability

- **First half: Supervised project** (13.10.2014 – 17.10.2014)
  - Room E1.1 2.06, 09:30-16:30 **s.t.** (lunch break 11:30-13:30)
  - Development of an exemplary Android security extension: Access control based domain isolation (private vs. business)
  - Introduction of the project: 13.10.2014, 09:30 - 10:30

Organizational: Lab Procedure

- **Second half: Project period** (20.10.2014 – 14.11.2014)
  - Teams of two students
    - No fixed classes
    - Team building and topic assignment: **Friday 17.10.2014**
    - But: Talk to your TA **(me!)** and get feedback!
      No meetings = No complaints about grade ☺
      No last minute meetings!
  - Equipment in room E1.1 2.06 can be used or private PC/laptop
    - UdS card required to get access to E1.1 2.06

Organizational: Lab Procedure

- Grade based on:
  - Final report and **code**
    - About 10 pages report + zipped code (or patch file)
    - Clearly stating for which part which team member was responsible
    - General structure of report explained in project proposals sheet
    - **Firm deadline for report: 14.11.2014 23:59**

References

- Separate PDF file with references available on the course website
- Recommended literature:
  - Karim Yaghmour. *Embedded Android: Porting, Extending, and Customizing.* O'Reilly Media. ISBN 978-1-4493-0829-2
  - Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva Fora, Stephen A. Ridley, Georg Wicherski. *Android Hacker's Handbook*. Wiley. ISBN: 978-1-118-60864-7

Online References

- http://developer.android.com
- http://source.android.com
- http://source.android.com/source/using-eclipse.html
- http://www.kandroid.org/online-pdk/guide/build_system.html
- Android tutorials by *MarakanaTech* on Youtube
- http://www.malgenomeproject.org/
- http://stackoverflow.com ☺

Organizational matters

Registration

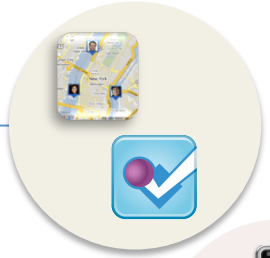
Motivation

Source: http://petapixel.com/assets/uploads/2013/3/comparison.jpg

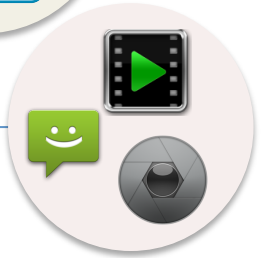
"Appification"

Online Services

Various Interfaces



Location Services

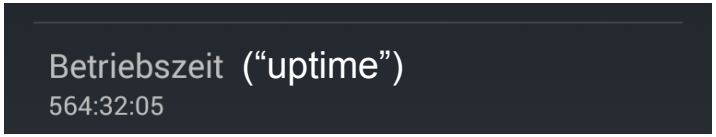


Default Features

NOMOPHOBIA

- “no-mobile-phone phobia”:
  Fear of being out of mobile phone contact
- Mobile phone users tend to be anxious when they “lose their mobile phone, run out of battery or credit, or have no network coverage”
- Stress levels induced by the average case of nomophobia to be on-par with those of "wedding day jitters" and trips to the dentists
- More than one in two nomophobes never switch off their mobile phones

http://seedcornppc.com/wp-content/uploads/2012/03/nomophobia.jpg

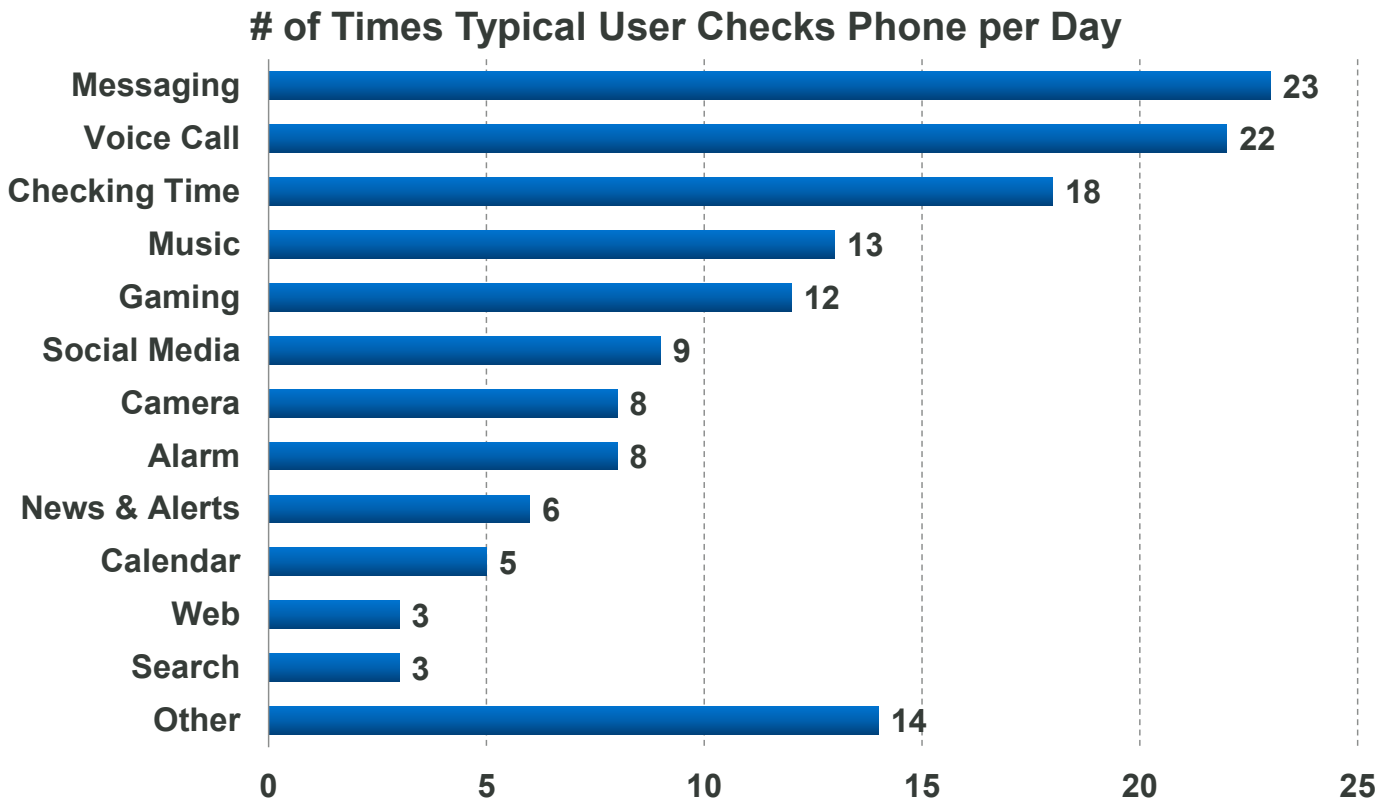


Source: Sven’s smartphone

Source: http://en.wikipedia.org/wiki/Nomophobia

CISPA Center for IT-Security, Privacy and Accountability

Mobile Users Reach to Phone ~150x a Day Could be Hands-Free with Wearables



KPCB

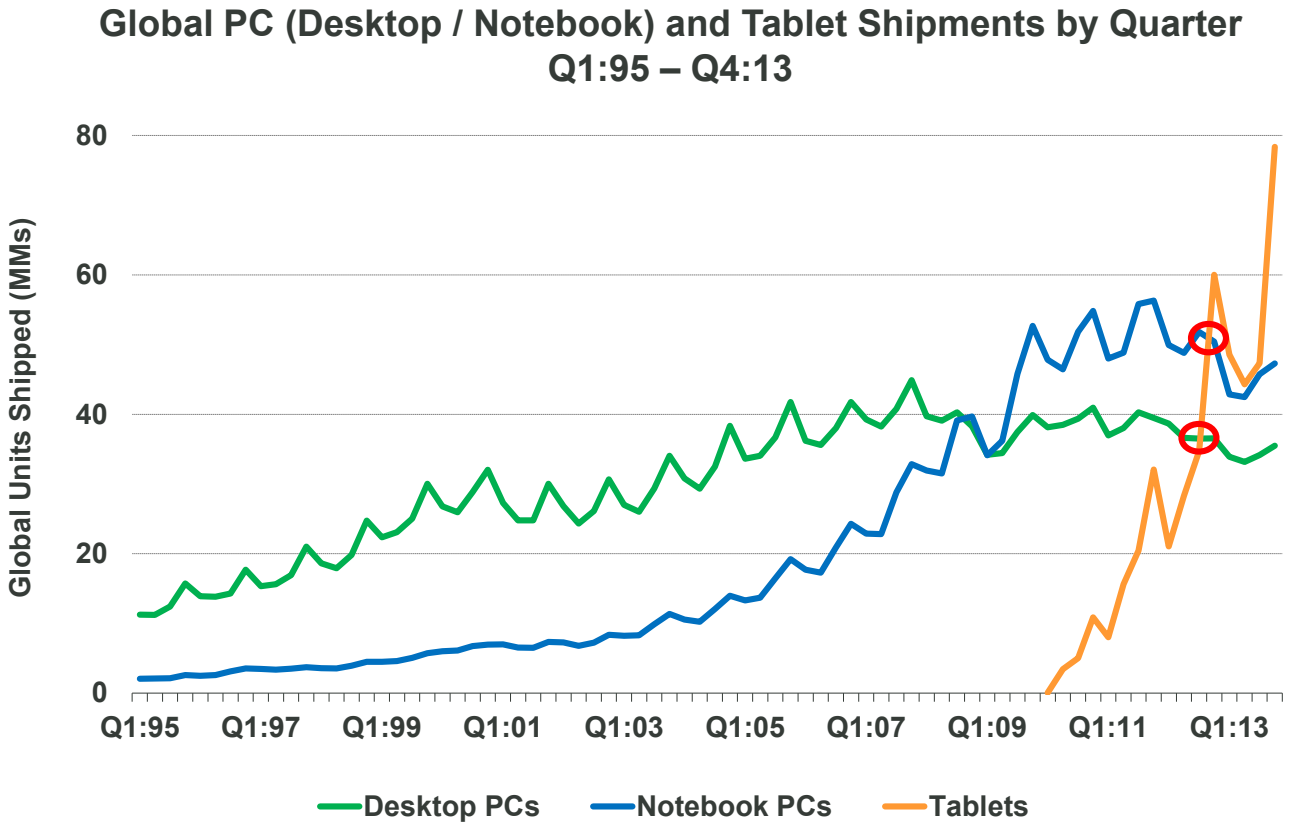
Source: TomiAhonen Almanac 2013, LINK. 'Other' includes voicemail, charging and miscellaneous activities. We cross-checked Tomi's analysis to gain context. Our references include: 1) Motorola Mobility / Google (consumers interact with their phones more than 100x per day, mid-2012); 2) Leading 3G Carrier with Operations in Europe & Asia (smartphone users interact with mobiles ~150x per day); 3) IDC (51 blended average of social sessions per smartphone user per day in USA, 3/13 excluded services like checking time, alarm and calendar events, web browsing, gaming, using camera, listening to music, searching, using maps, charging and other activities that require checking the phone) and 4) other third parties, including app providers.

52

Source: Mary Meeker. INTERNET TRENDS 2013

CISPA Center for IT-Security, Privacy and Accountability

Tablet Units = Growing Faster Than PCs Ever Did... +52%, 2013

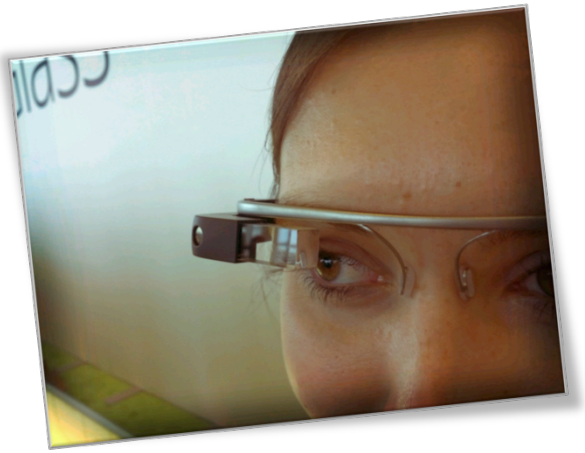


@KPCB Source: Morgan Stanley Research. Note: Notebook PCs include Netbooks.

7

Source: Mary Meeker. INTERNET TRENDS 2014

SMARTPHONE OSES IN NEW CONTEXTS



http://upload.wikimedia.org/wikipedia/commons/7/76/Google_Glass_detail.jpg

http://blog.laptopmag.com/wpress/wp-content/uploads/2013/08/SamsungSmartwatch.jpg

http://1.bp.blogspot.com/-wx6nEY5m_kM/TVWIX3vguzI/AAAAAAAAAWI/sr8-slRN9Vc/s1600/Android+in+car+auto+vehicle.jpg

Selected smartphone Operating Systems

CISPA Center for IT-Security, Privacy and Accountability

Android

iOS

Blackberry

Windows Phone

Bada

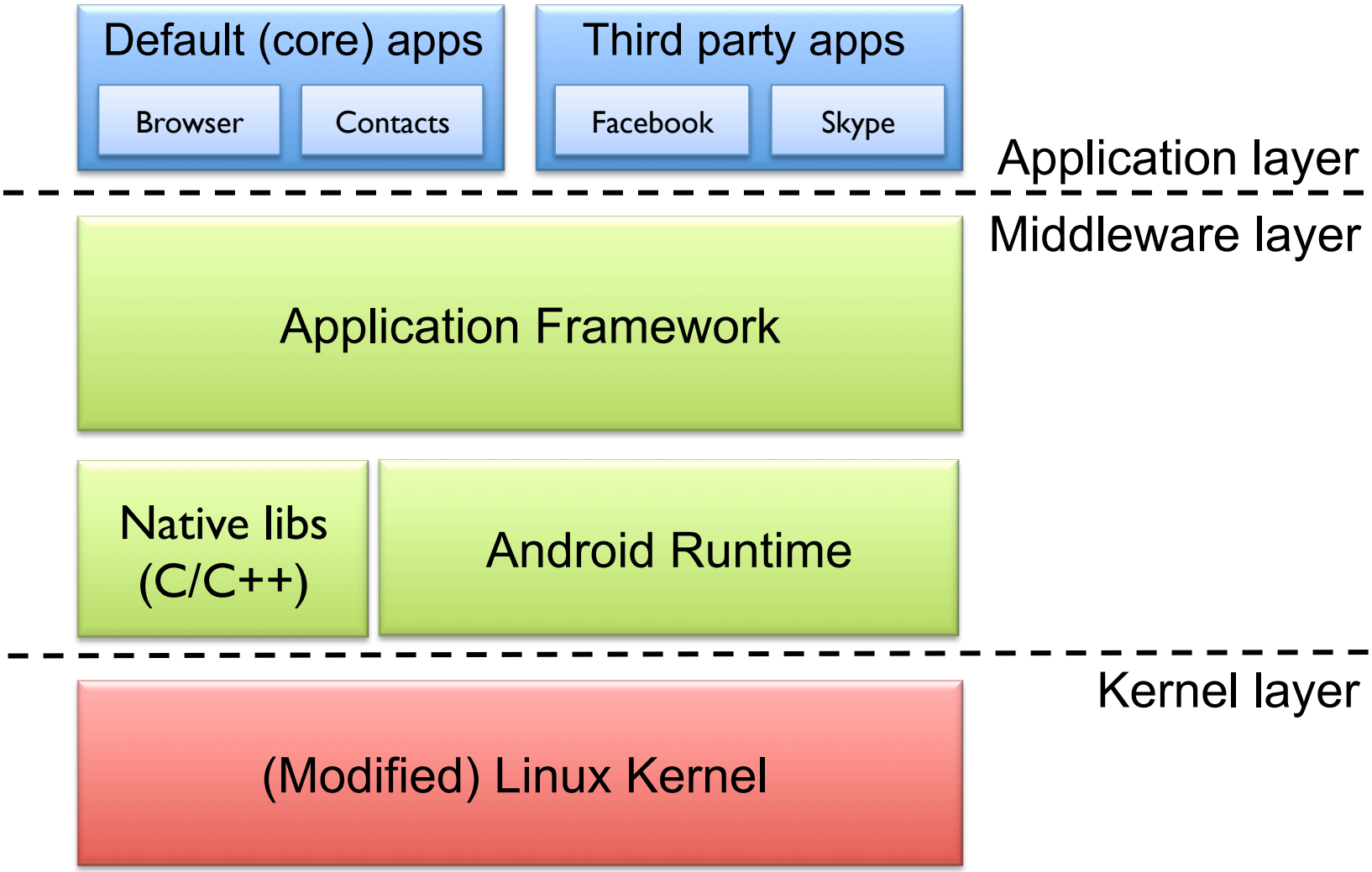
Selected smartphone Operating Systems

Android

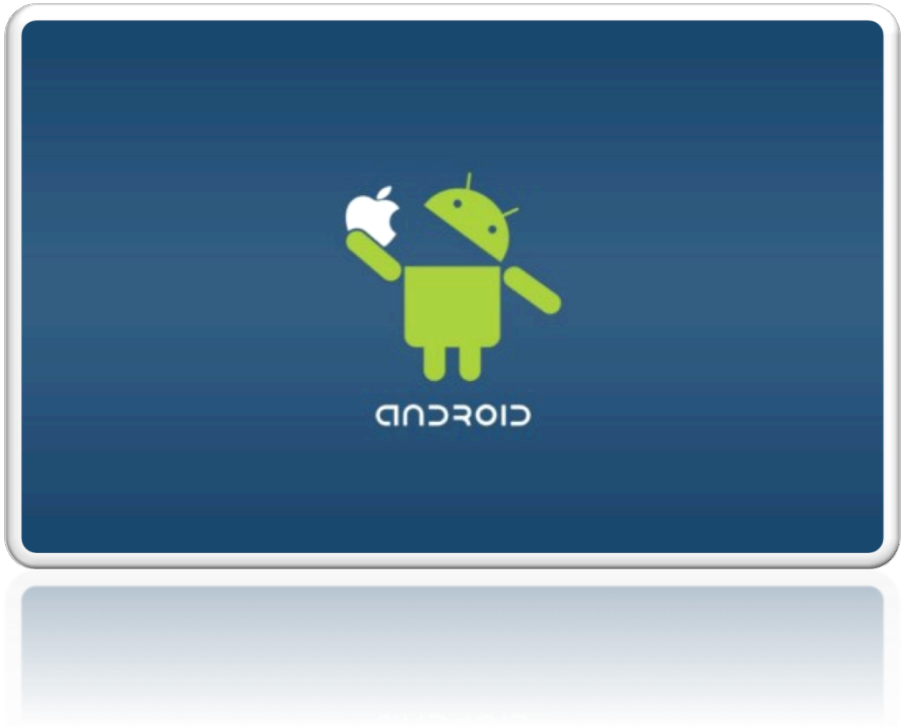
Why most research done on Android?

1. Almost completely Open Source

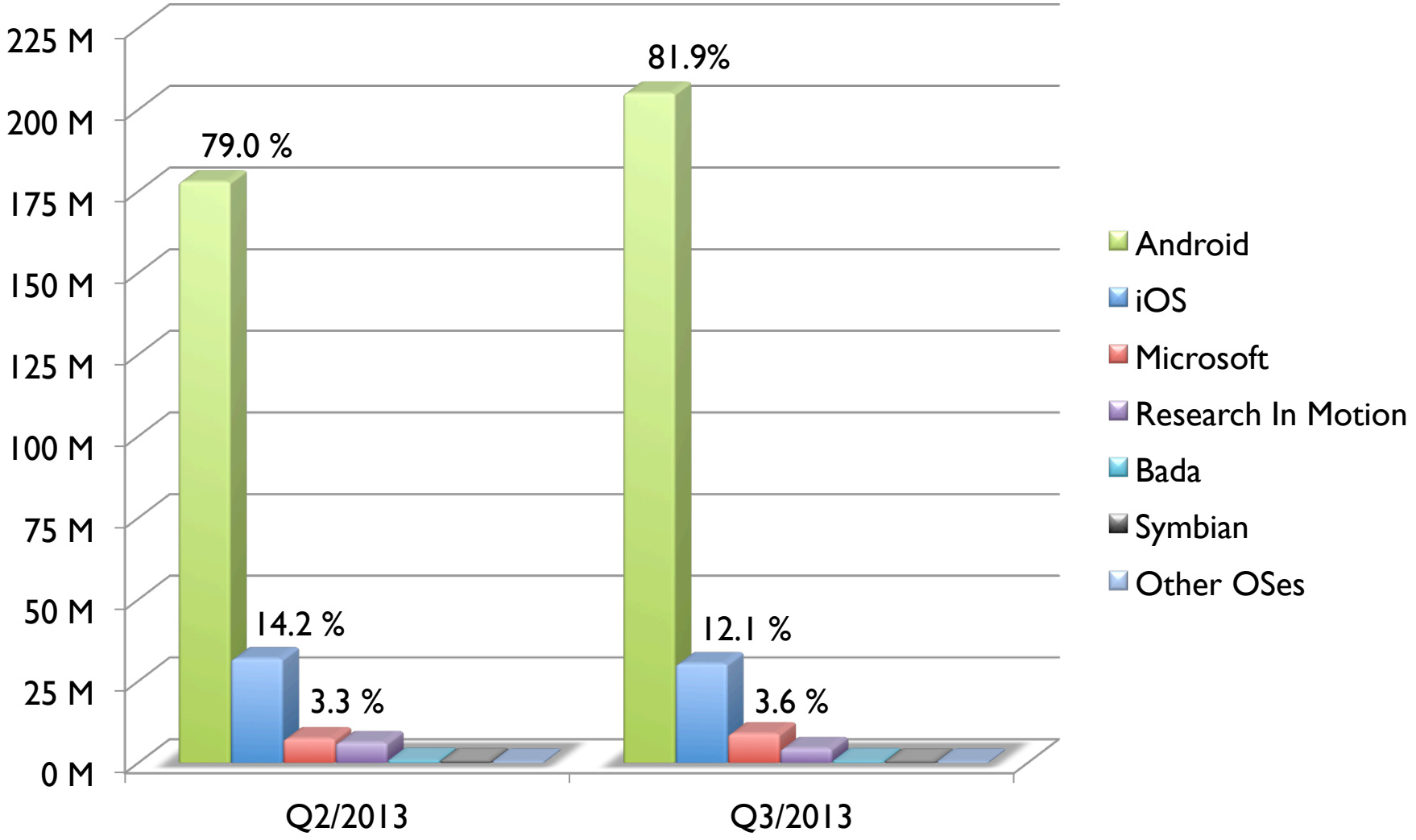
Android Software Stack



2. The Market

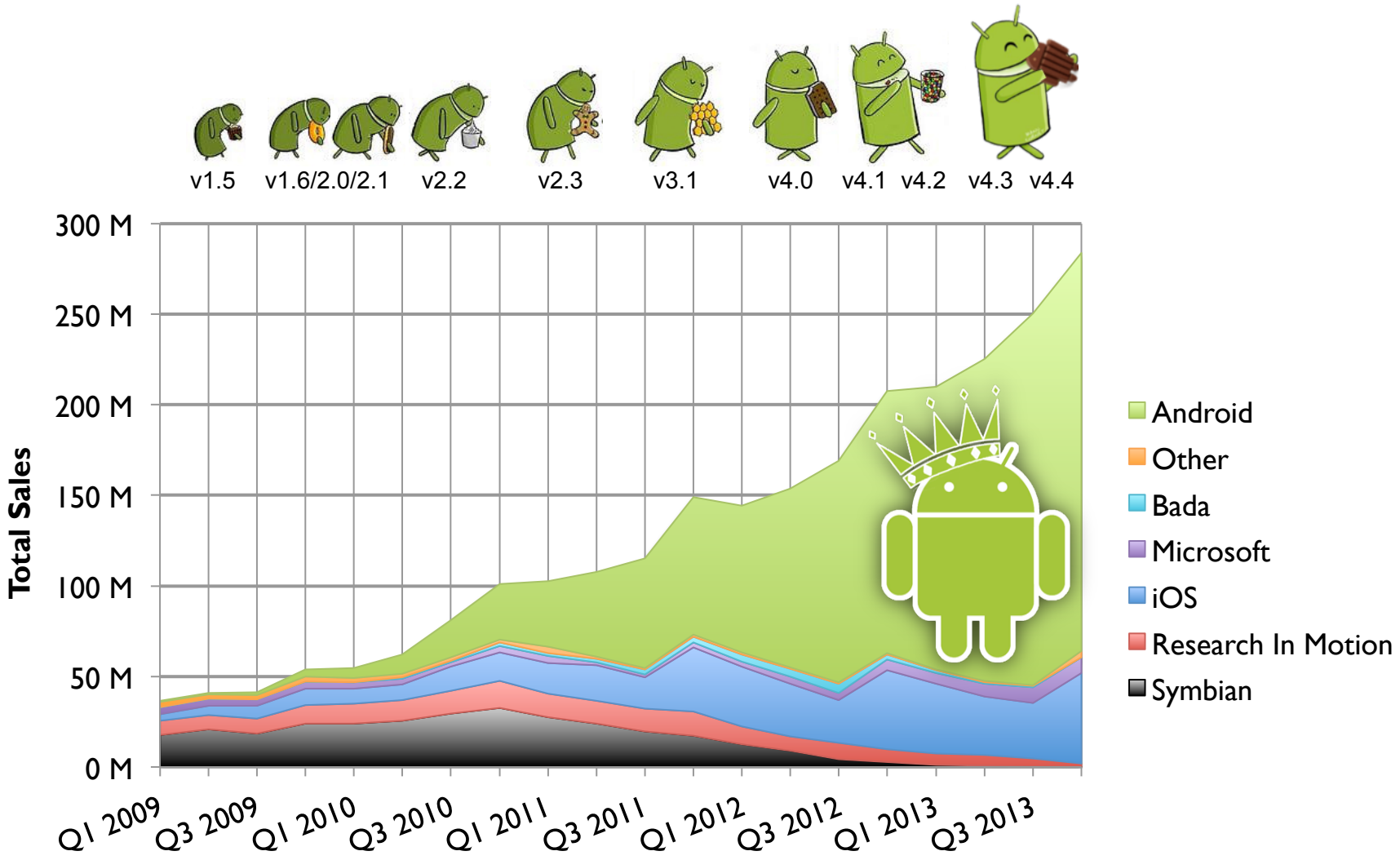


Worldwide Smartphone Sales to End Users by Operating System Sold Units and Market Share Q2/2013 and Q3/2013



Based on Gartner Statistics

Global Smartphone Market Landscape



Based on Gartner Statistics

Smartphones as Target of Attacks

SMARTPHONES: HIGH-VALUE TARGETS

We always carry them with us… most data can be captured **LIVE** …

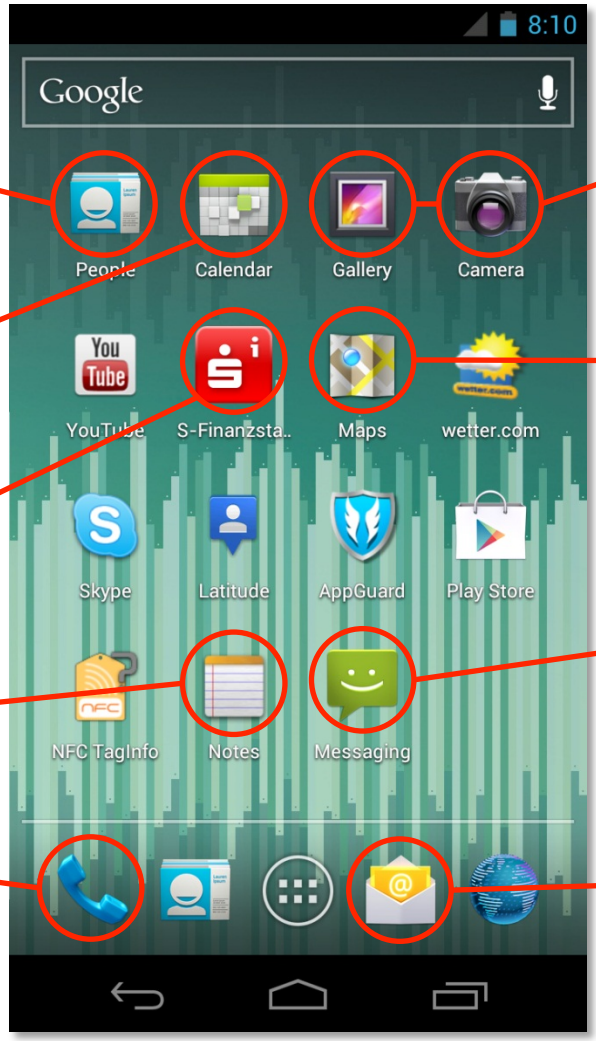
Who we know:
People, Addresses,
Phone numbers

What we do next:
Appointments
(… with whom?)

Mobile Banking
(e.g., mTAN)

Current thoughts?
ideas, memories, notes,
working documents

Premium calls



Photos, videos
(incl. sound, devices
have a mic)

GPS: Where are we,
where are we going
to, Accelerometers

Premium SMS

E-mails, chatting, Skype:
our full communication
(generally unencrypted)

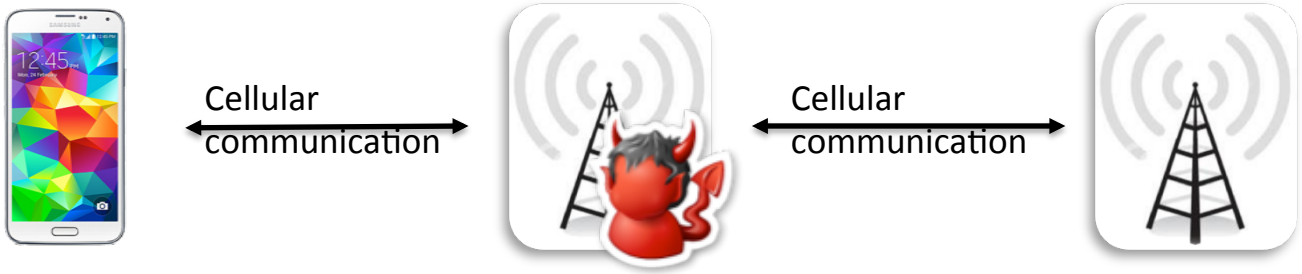
Threat Classification

Malicious Charger/Docking station [19]

- Micro-computer (e.g., BeagleBoard or Raspberry Pi) hidden in charger/docking station
- When user plugs in his iPhone, the software on the micro-computer attacks and compromises the phone's operating system and achieves root privileges
  - Demo attack against iOS: Silently replaced facebook app with a malicious version that spied on the user
- Android: USB has been shown to be a potential attack surface
  - Zero-day exploits? (e.g., error in file system driver or media manager when mounting external harddrive)

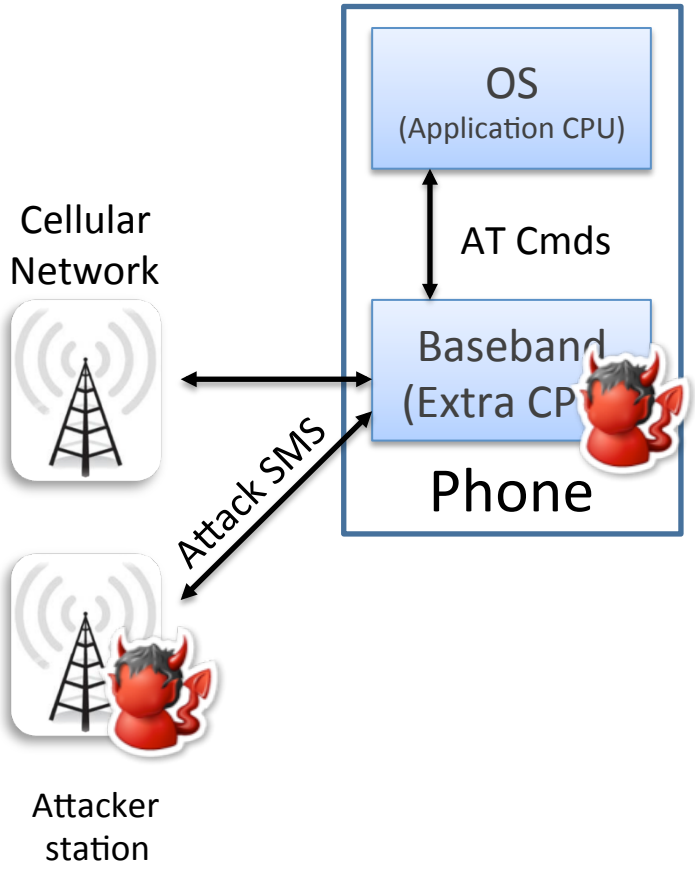
Rogue Basestation [20]

- Fake base station can be easily build
  - OpenBTS/OpenBSC software
  - Dedicated hardware ($1000) or a Motorola C123
- No mutual authentication between phone and cellular network
  - Network does not have to authenticate to phone
- Fallback to GPRS/EDGE when UMTS/HSPA unavailable
- Man-in-the-middle attacks
  - IMSI catcher, downgrade encryption, redirect/alter traffic, …



Baseband attacks [21,22]

- Baseband processor runs dedicated separate OS (e.g., OKL4)
- Baseband OS usually less hardened against software exploits
  - E.g. “software unlocks” for iPhone’s network locks
- Fuzzing the baseband with specially crafted SMS from a rogue basestation revealed software vulnerabilities
  - Compromise the baseband OS



Threat Classification

CISPA Center for IT-Security, Privacy and Accountability

Software exploits

- iPhone rooting:
  Dedicated exploit kits
  - E.g. RedSn0w

- All modern exploits use *return-oriented programming* (code reuse) techniques to circumvent defenses such *Data Execution Prevention (DEP)* or *W^X* (write-xor-execute)

Exkursion: Concept of ROP

- "Classical" attack prevented by DEP

Code

Data

I'm the most lovely and non-harmful program you can imagine. I embody functionality like document analysis of different types. I'm not bad in any way.

Attacker

Exkursion: Concept of ROP

- "Classical" attack prevented by DEP

Code

Data

I'm the most lovely and non-harmful program you can imagine. I embody functionality like

This program now executes an exploit

not bad in any way.

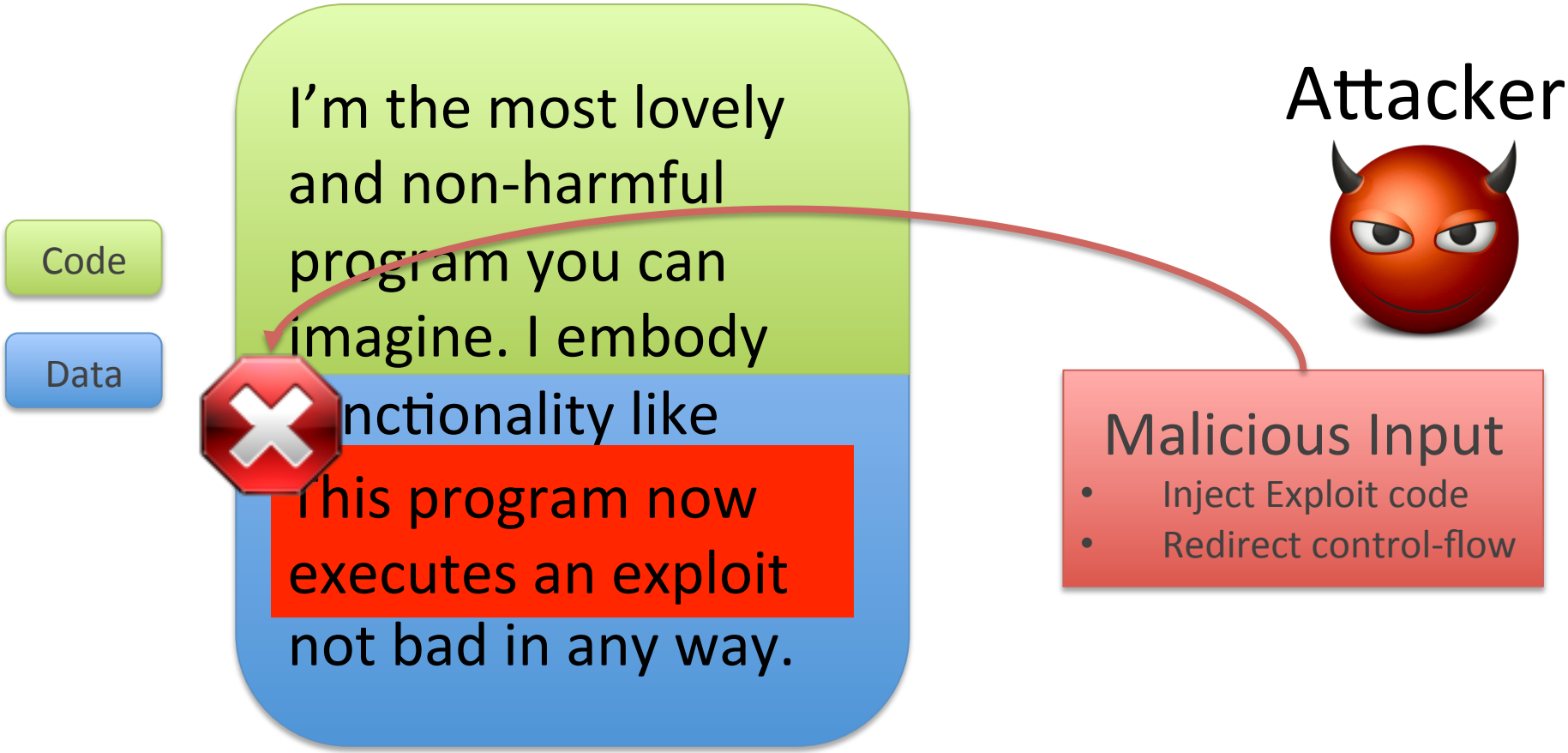
Attacker

Malicious Input

- Inject Exploit code
- Redirect control-flow

Exkursion: Concept of ROP

- "Classical" attack with DEP



Exkursion: Concept of ROP

- Code reuse attack: No need to “execute data”

Code

Data

I’m the most ~~lovely~~ and ~~non-~~ harmful program you can imagine. I embody functionality like document analysis of different types. I’m not bad in any way.

Attacker

Malicious Input

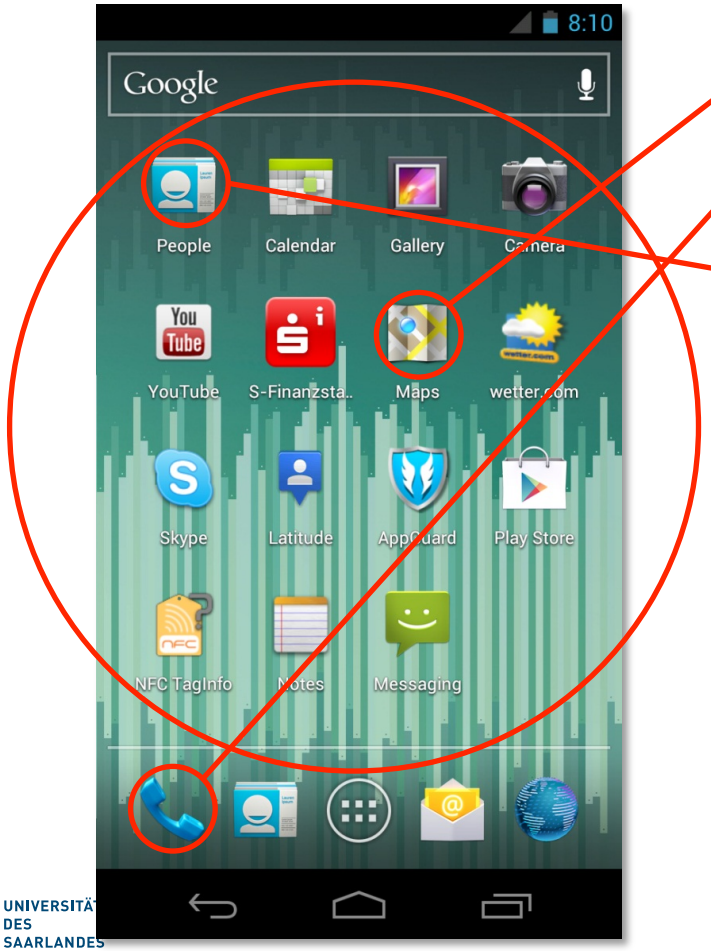
- Inject addresses in known code (Must be known)
- Redirect control-flow to jump to each of those addresses

Threat Classification

Some Statistics and Examples

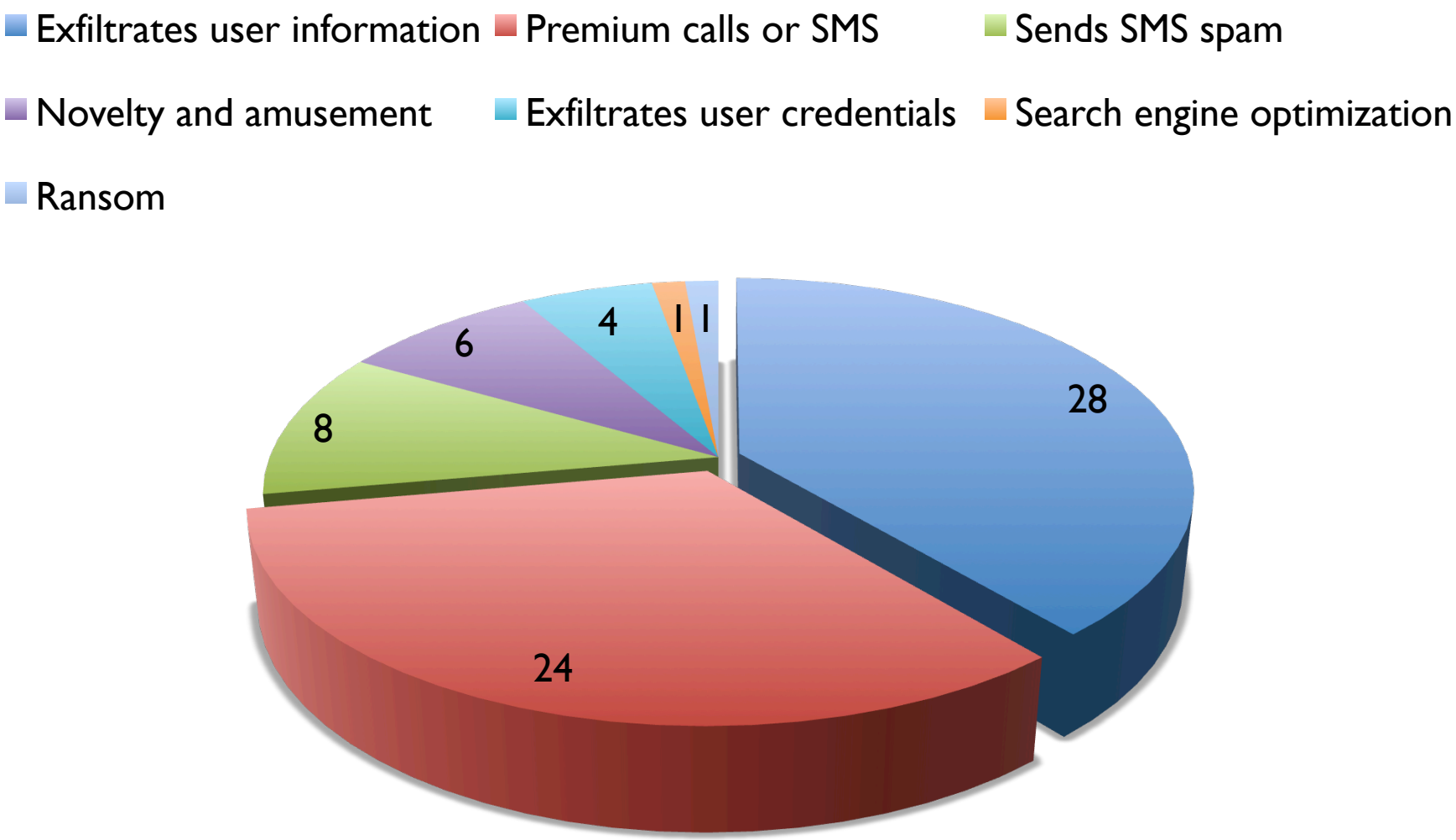
Danger of Advertisement Libraries [12]

- 52.1% of 100,000 apps hosted at Google Play and third-party stores include at least one advertisement library
- For the apps that include an ad library,



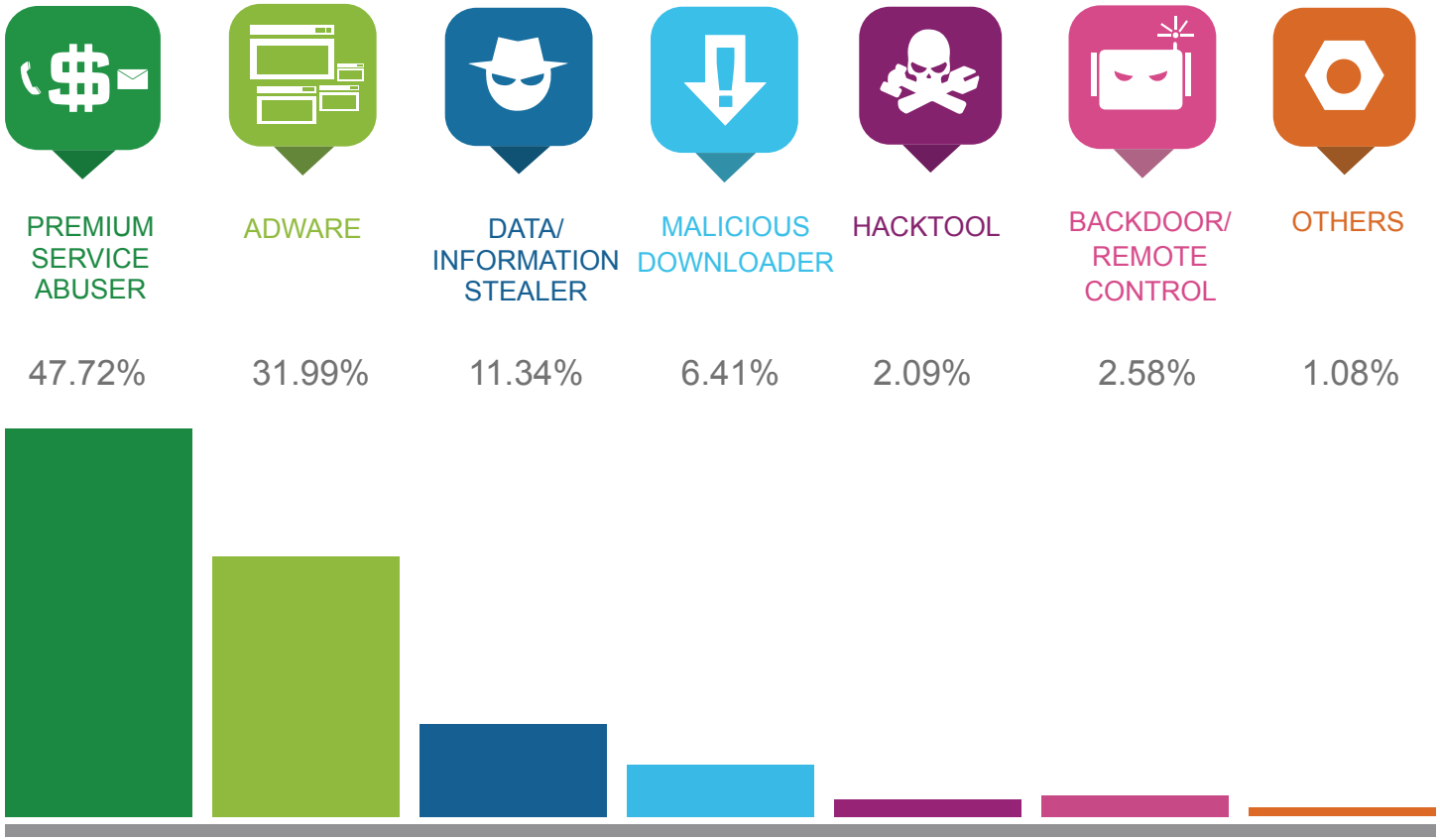
- 79.41% access location data,
- 33.62% read phone information,
- 4.98% read contacts/call logs, and
- 0.78% read installed packages
- Some: Hidden update functionality

Classification of Android Malware [9]



Classification of Android Malware (Industrial Stats)

CISPA Center for IT-Security, Privacy and Accountability



GRAY ZONE

- WhatsApp messaging app
  - Uploads the entire address book and stores it on the servers
  - Creating fake contacts to enumerate range of phone numbers allows you to detect which numbers belong to real WhatsApp users (no mutual authentication required between users)
  - Several incidents with insufficient security of the communication between the app and the servers
- Tinder dating app
  - Revealed exact user location and allowed stalking of members
- Facebook app
  - Requests permission to read SMS messages for authentication purposes (automatically detect SMS with confirmation code for two-factor authentication)

Motivation

- Mobile security a very active research area
  - Feature-rich smartphones and “appification” have induced security research on various (new) aspects
- Android’s open-source nature has made Android very attractive to security researchers
- Android’s market share has made Android the #1 target for malware authors and makes improved security & privacy mechanisms imperative