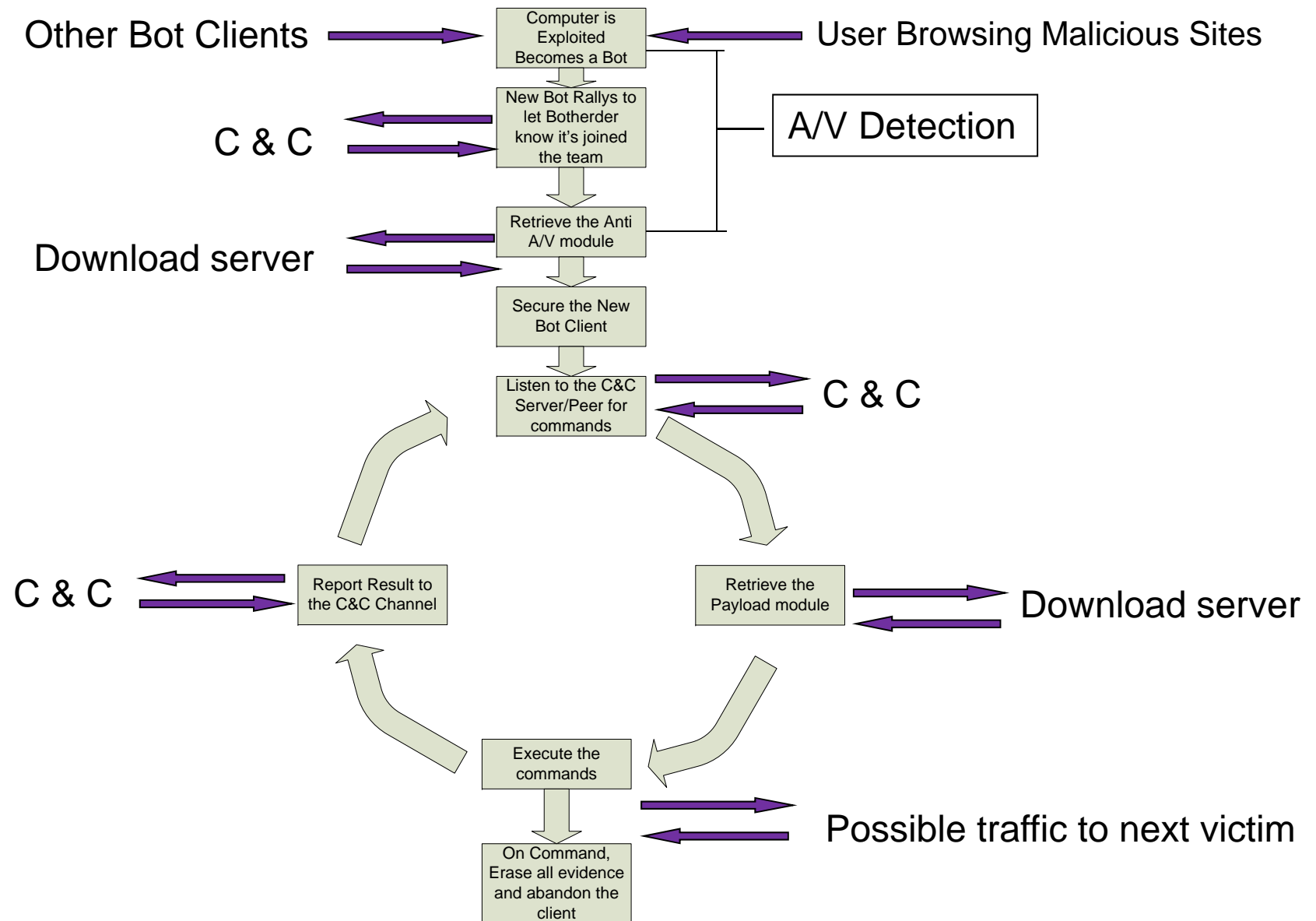# INFO 310

Fall 2016

Week 8 – Lecture 2

HOUSEKEEPING

- Attendance

Botnets

- A collection of computers infected with autonomous malware that can be controlled remotely, all without the knowledge of the users / owners of those computers.

- BotNet: Bot + Net(work)
  - Bot: A compromised system running malware designed to 'phone home' and receive / carry out instructions
  - Network: A collection of bots under the control of a single individual or entity (bot herder, bot master)

- Bot: Originally from *roBOT*, a program that performs a repetitive function such as searching for information, or admin tasks in IRC channels
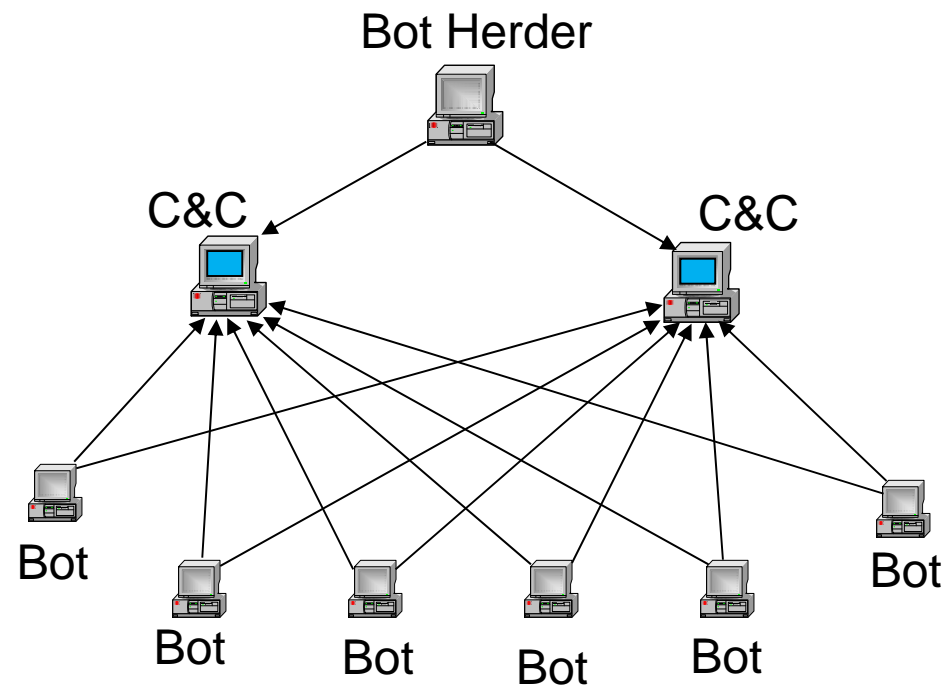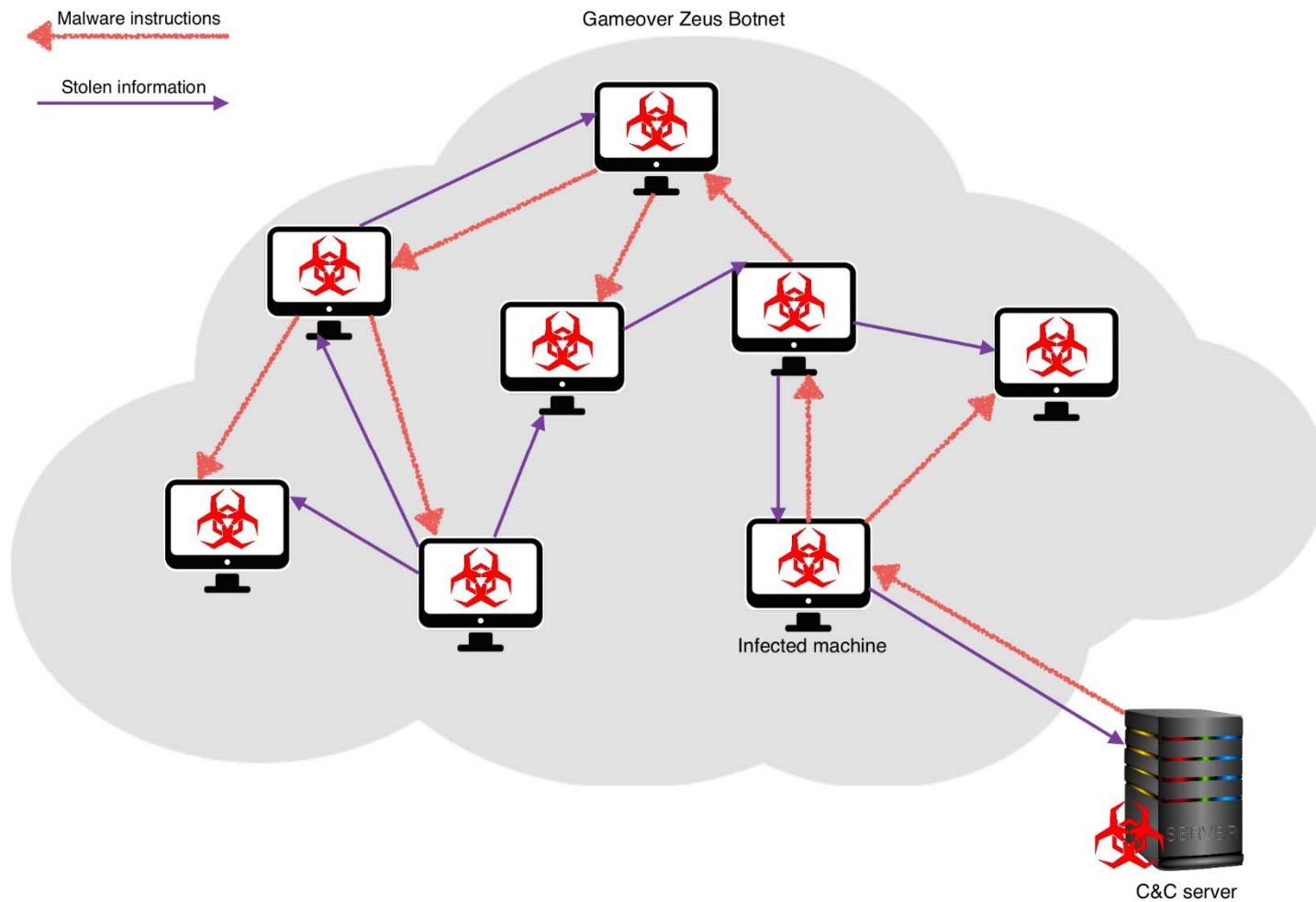
High-Level Lifecycle

Other Bot Clients → Computer is Exploited Becomes a Bot ← User Browsing Malicious Sites

New Bot Rallys to let Botherder know it's joined the team

C & C

A/V Detection

Retrieve the Anti A/V module

Download server

Secure the New Bot Client

Listen to the C&C Server/Peer for commands

C & C

Retrieve the Payload module → Download server

Report Result to the C&C Channel

C & C

Execute the commands → Possible traffic to next victim

On Command, Erase all evidence and abandon the client

Types of Botnets

- Star
- Multi-server
- Hierarchical
- Random p2p

Basic (Multi-Server) Botnet

Bot Herder

C&C

C&C

Bot

Bot

Bot

Bot

Bot

Bot

p2p Botnet (Zeus)

Malware instructions
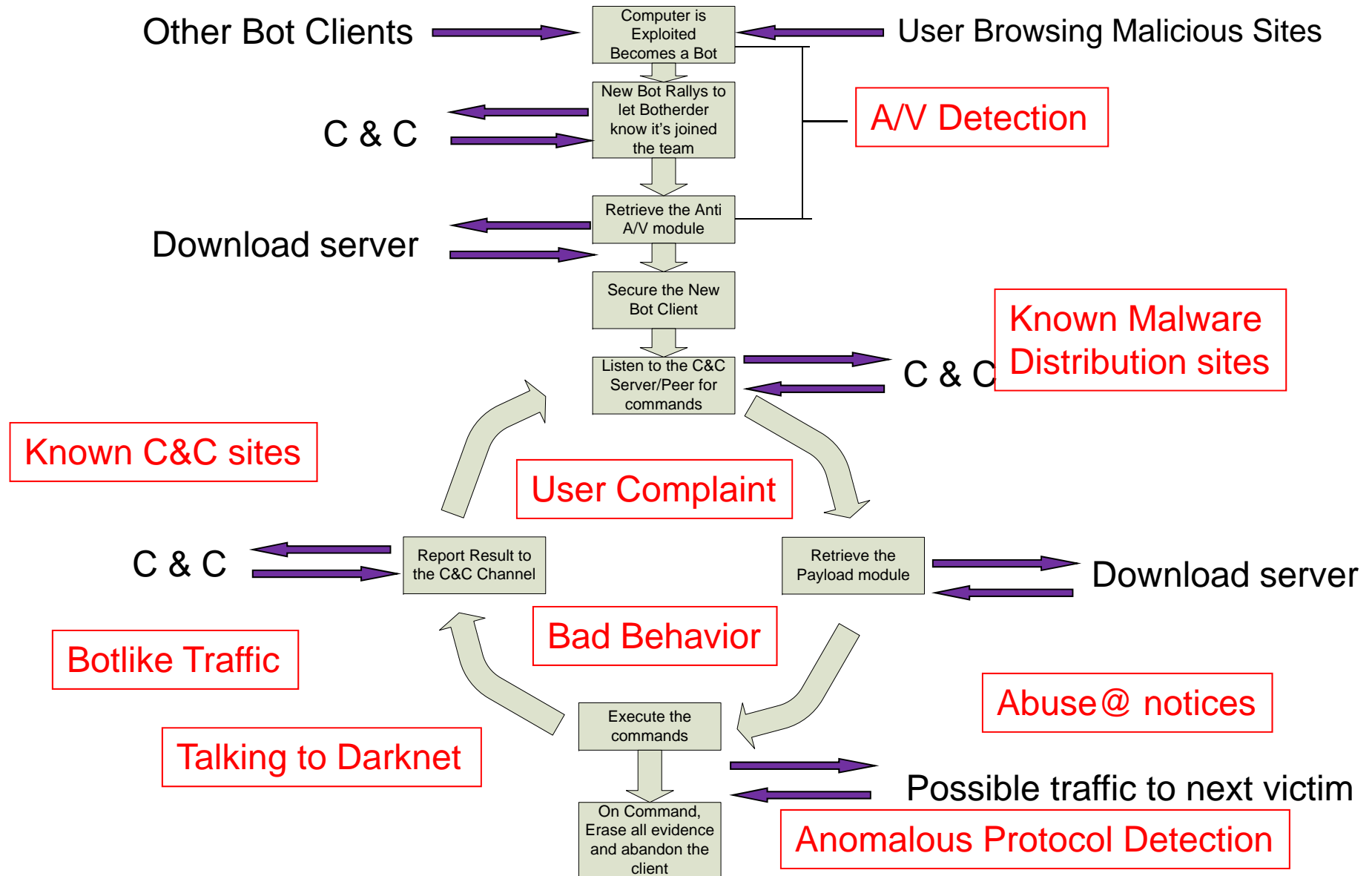
Stolen information

Gameover Zeus Botnet

Infected machine

C&C server

Botnet Purposes

- Spam
- DDoS
- Phishing
- Click Fraud
- Scanning
- Blackmail
- Hosting pirated content (old skool)
- …

Potential Detection

Other Bot Clients → **Computer is Exploited Becomes a Bot** ← User Browsing Malicious Sites

New Bot Rallys to let Botherder know it's joined the team

C & C →

A/V Detection

Retrieve the Anti A/V module

Download server →

Secure the New Bot Client

Listen to the C&C Server/Peer for commands → C & C

Known Malware Distribution sites

Known C&C sites

User Complaint

C & C ← **Report Result to the C&C Channel** → ← **Retrieve the Payload module** → Download server

Bad Behavior

Botlike Traffic

Abuse@ notices

Talking to Darknet

Execute the commands

On Command, Erase all evidence and abandon the client → Possible traffic to next victim

Anomalous Protocol Detection

(break)

Mobile Device Security (&Privacy)

The Big Players

SMARTPHONE MARKET SHARE

Android to Retain Big Lead in Maturing Smartphone Market
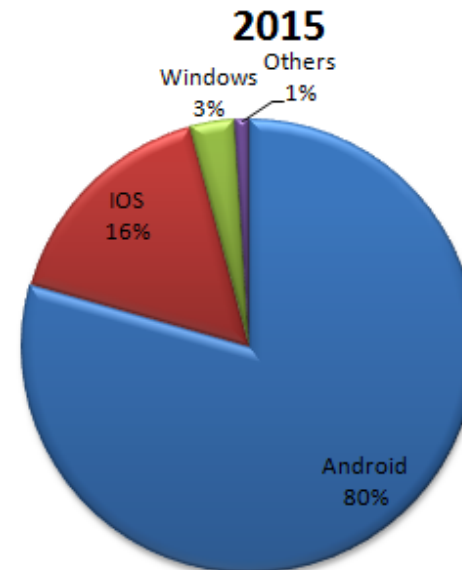
Worldwide smartphone market share, by OS
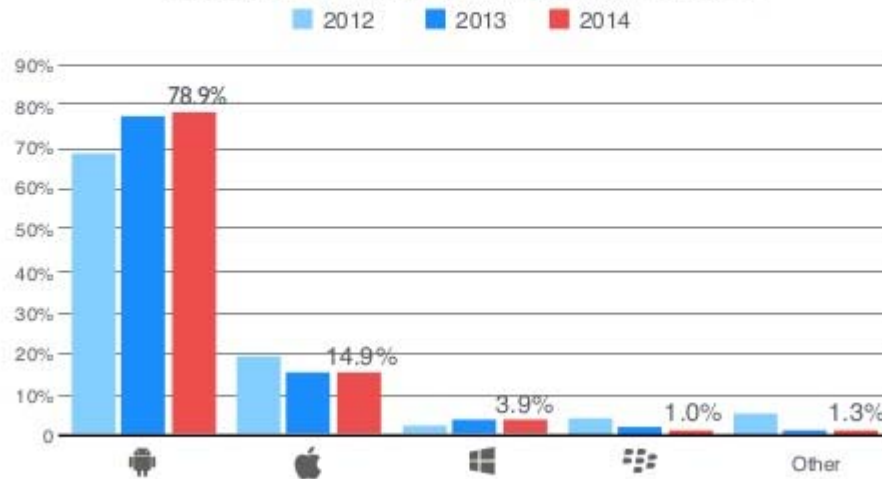
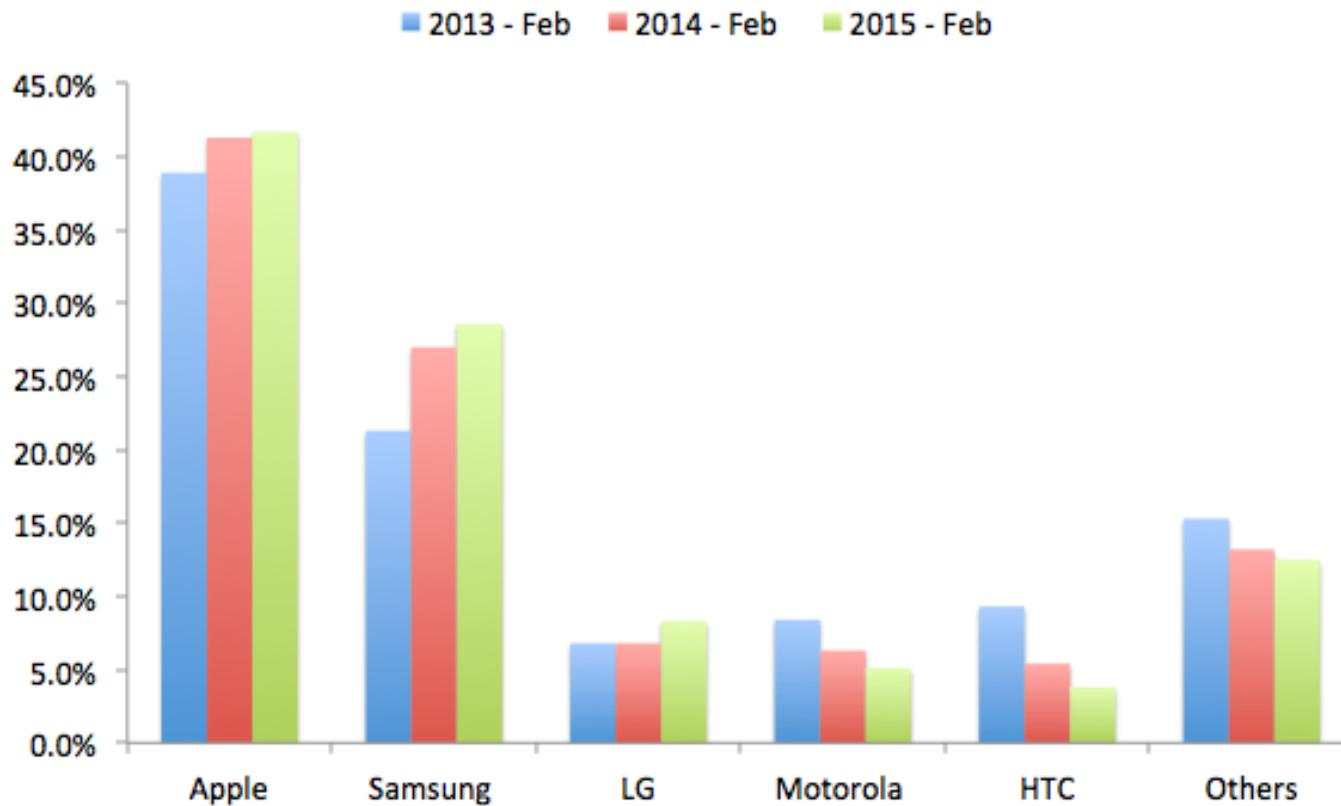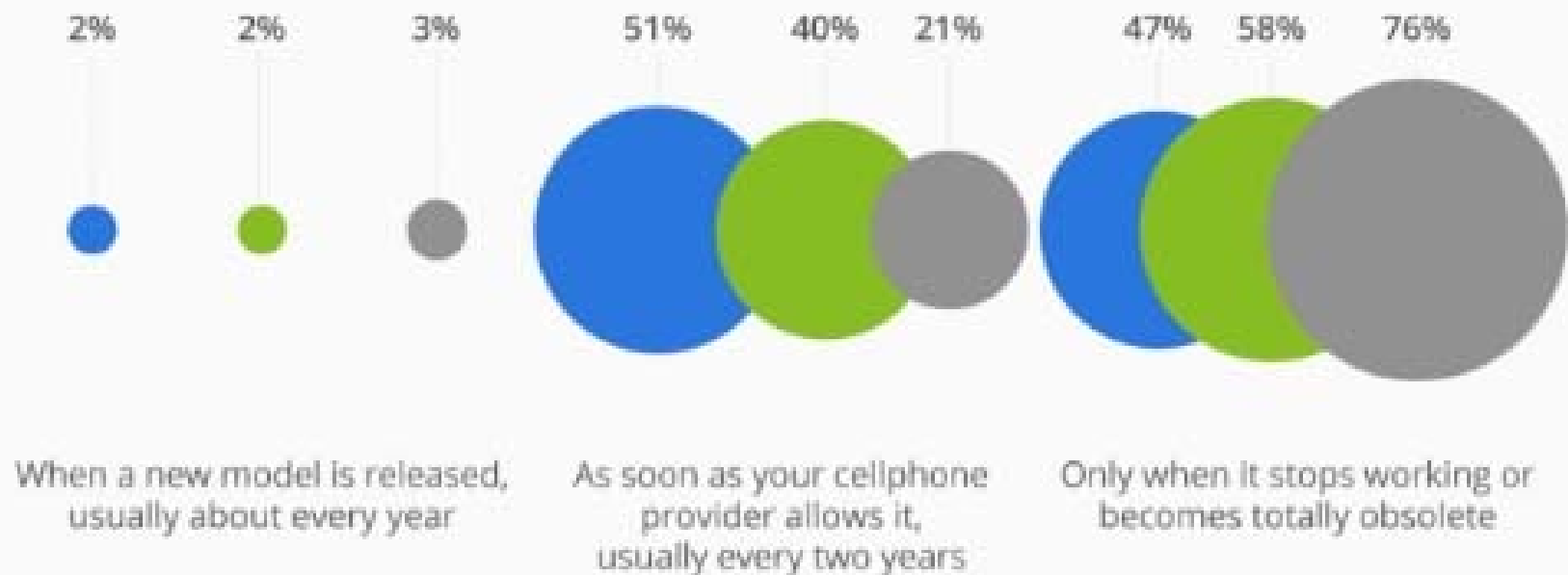# Global Operating System Market Share 2015

Device Manufacturer
US Market Share

How Often Do Americans Upgrade Their Smartphones?

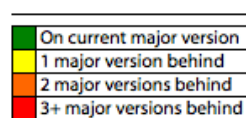Frequency of upgrading a smartphone by type of smartphone user in 2015

iPhone   Android   Other

2%   2%   3%   51%   40%   21%   47%   58%   76%

When a new model is released,
usually about every year

As soon as your cellphone
provider allows it,
usually every two years

Only when it stops working or
becomes totally obsolete

ANDROID & IPHONE UPDATE HISTORY

Includes every iPhone & Android model released in the US before July 2010.

Data as of the end of October 2011.

KEY

- 🟩 On current major version
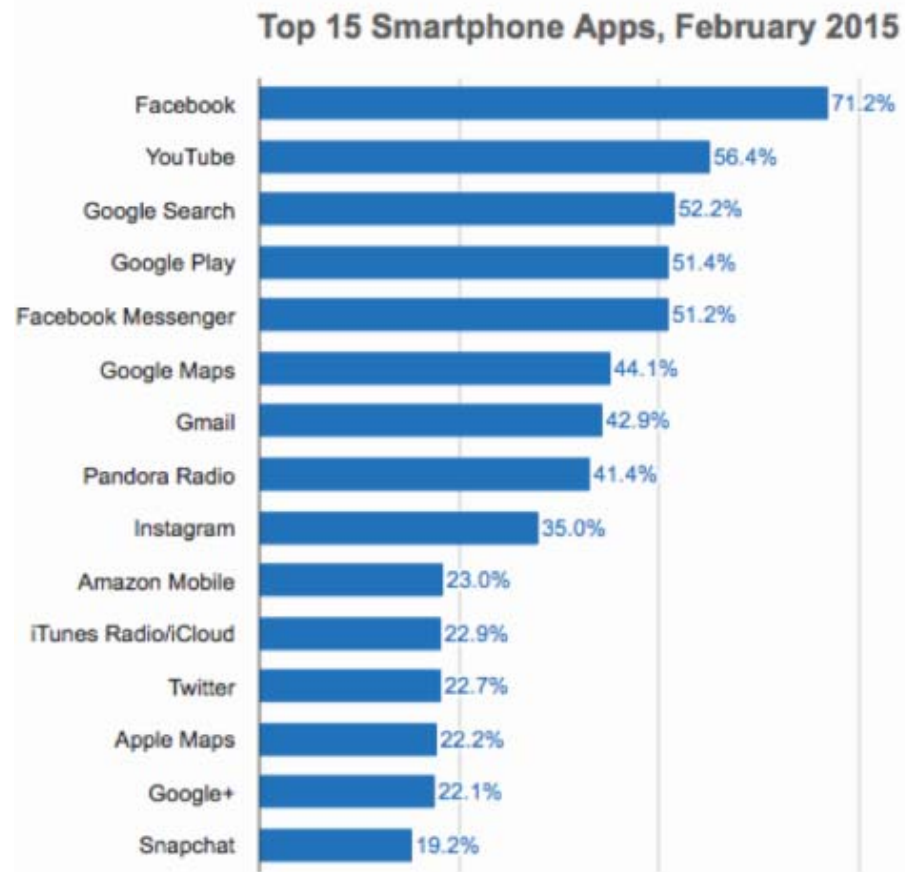- 🟨 1 major version behind
- 🟧 2 major versions behind
- 🟥 3+ major versions behind

☐ Actively for sale
╌╌ Getting support updates

Prices are with 2 year contract

iPhone	1st Year After Release	2nd Year After Release	3rd Year After Release
Apple iPhone 6/29/07 AT&T $499			
Apple iPhone 3G 7/11/08 AT&T $199			
Apple iPhone 3GS 6/19/09 AT&T $199			*Still sold & possibly updated*
Apple iPhone 4 6/21/10 AT&T $199		*Still sold & possibly updated*	

2008 Android	1st Year After Release	2nd Year After Release	3rd Year After Release
HTC G1 10/22/08 T-Mobile $180			

2009 Android	1st Year After Release	2nd Year After Release	3rd Year After Release
HTC MyTouch 3G 8/5/09 T-Mobile $200			
HTC Hero 10/11/09 Sprint $180*			
Samsung Moment 11/1/09 Sprint $180*			
Motorola Cliq 11/2/09 T-Mobile $200			
Motorola Droid 11/6/09 Verizon $200*			
HTC Droid Eris 11/6/09 Verizon $100*			
Samsung Behold II 11/18/09 T-Mobile $230			

2010 Q1&2 Android	1st Year After Release	2nd Year After Release	3rd Year After Release
HTC Nexus One 1/5/10 T-Mobile $180			
Motorola Devour 2/25/10 Verizon $150			
Motorola Backflip 3/7/10 AT&T $100*			
Motorola Cliq XT 3/17/10 T-Mobile $130			
HTC Droid Incredible 4/29/10 Verizon $200*		*Possibly still being updated*	
LG Ally 5/20/10 Verizon $100*			
HTC MyTouch 3G Slide 6/2/10 T-Mobile $180*		*Still being sold*	
HTC Evo 4G 6/4/10 Sprint $200*		*Possibly still being updated*	
Garmin Garminfone 6/9/10 T-Mobile $200*			
HTC Aria 6/20/10 AT&T $130*			

* After $100 mail-in rebate ($50 on MyTouch 3G Slide & Garminfone)

Apps, Apps, & More Apps

Top 15 Smartphone Apps, February 2015

App	%
Facebook	71.2%
YouTube	56.4%
Google Search	52.2%
Google Play	51.4%
Facebook Messenger	51.2%
Google Maps	44.1%
Gmail	42.9%
Pandora Radio	41.4%
Instagram	35.0%
Amazon Mobile	23.0%
iTunes Radio/iCloud	22.9%
Twitter	22.7%
Apple Maps	22.2%
Google+	22.1%
Snapchat	19.2%

February 2014

Top 15 Apps	% Reach
Smartphone App Audience	100.0%
Facebook (Mobile App)	75.7%
Google Play (Mobile App)	52.1%
Google Search (Mobile App)	49.8%
YouTube (Mobile App)	48.4%
Pandora Radio (Mobile App)	45.0%
Apple App Suite (Mobile App)	44.8%
Gmail (Mobile App)	42.9%
Google Maps (Mobile App)	41.3%
Yahoo Stocks (Mobile App)	29.5%
Instagram (Mobile App)	28.1%
Yahoo Weather Widget (Mobile App)	26.3%
Apple Maps (Mobile App)	24.9%
Facebook Messenger (Mobile App)	24.1%
Twitter (Mobile App)	22.7%
The Weather Channel (Mobile App)	21.0%

Not so anonymous...
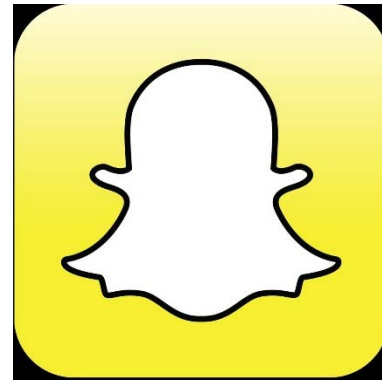
There are options!

Potential Issues

- GPS / Location services

- Malicious Apps

- Jailbreaking / Rooting

- No more OS updates but phone still under contract

- Apps with too much access

- Questionable mobile network operators

- Supply chain poisoning

- ....

(this page intentionally left blank)

Quiz II – "Study Guide"

- Define Computer Virus, Trojan Horse, Worm and their specific differences

- Define malware, including examples (both types and names)

- Describe malware delivery mechanisms

- Describe AV software, and, at a (very) high level, how it works

Quiz II – "Study Guide" cont'd

- Define Bot & Botnet
- Describe Botnet components & lifecycle
- Describe different types of botnets
- Describe what botnets are used for
- Describe methods for detecting botnet activity

Quiz II – "Study Guide" cont'd

- Mobile Device Security
  - Ability to discuss device lifecycle compared to availability of OS updates
  - Ability to describe how to check mobile device OS version number, and where to search for vulnerabilities
  - The App Store ecosystem
  - Potential privacy issues around location services
  - App permission pitfalls
  - International travel with smartphones – concerns, risks

Quiz II – "Study Guide" cont'd

- Citizenfour (2014) – Documentary
  - Who are the main characters, what are their roles?
  - What are Ed Snowden's main claims?
  - What was Ed Snowden accused of by the US Government?