NC STATE UNIVERSITY

CSC 405
Computer Security

Alexandros Kapravelos
akaprav@ncsu.edu

Administration

- Class website
  - https://kapravelos.com/teaching/csc405-s18/schedule/
- Piazza
  - piazza.com/ncsu/spring2018/csc405
- Mail to instructor (for private matters)
  - akaprav@ncsu.edu
- Recorded classes (if the classroom supports it)

Material

- What material will we be using?
  - Unfortunately, there is no good book on systems security
  - Use the slides that I will post on the web site
  - Related papers/readings and online material (from the syllabus)

Grading

- What are the requirements to get a grade?
  - Two exams (midterm and final) - 30% of grade
  - Homework Assignments - 60% of grade
  - Participation - 10% of grade
    - Class Participation
    - Quizzes
    - Solve one CTF challenge with the HackPack student group in a non-NCSU CTF event

Topics

Basics

Web Security

Application Security

You need to understand

- Networks and Operating Systems
- Basics of systems theory and implementation
  - E.g., file systems, distributed systems, networking, operating systems, …
- You will build stuff. I expect you to:
  - know how to code (in language of your choice*)
  - I will use mix of pseudocode, Python, Assembly, JavaScript, PHP and C
  - be(come) comfortable with Linux/UNIX

Goals

Learn how an attacker takes control of a system

Learn to defend and avoid common exploits

Learn how to architect secure systems

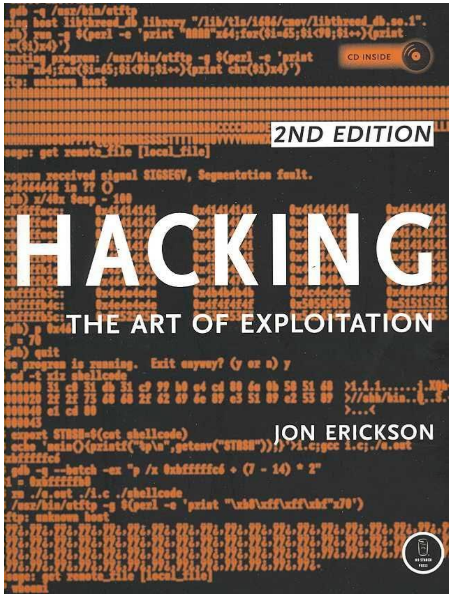
Assignments

- Individual homework assignments
- These are going to be hard!
- You are going to implement attacks and defenses

HackPack CTF

- Capture the Flag security competition
- 6 hours live hacking
- We’ll have pizzas & sodas
- **April 20th 1-7pm**
- It will count as one homework assignment
- There will be prizes for top places!

HackPack CTF prizes 2017

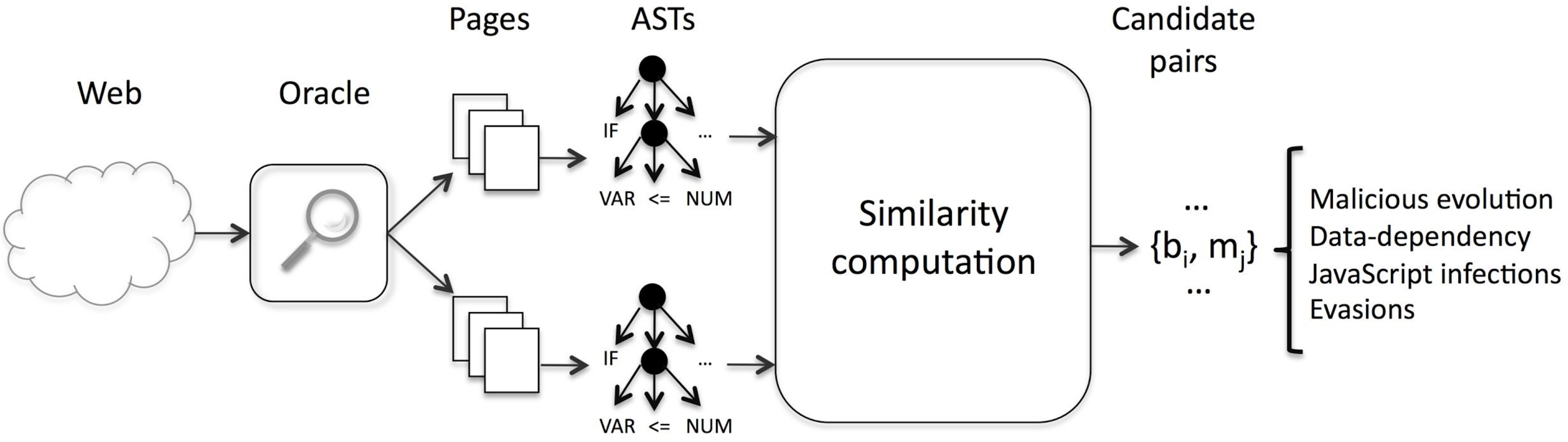


Readings

- There are a large amount of readings in this course covering various topics. These readings are intended to:
  - Support the lectures in the course (provide clarity)
  - Augment the lectures and provide a broader exposure to security topics
- **Students are required to do the reading!**
  - Some of the questions on the exams will be off the reading on topics that were not covered in class

Cheating policy

- Cheating is not allowed
- We run tools
- If you cheat you will probably get caught and get a failing grade in the course
- All academic dishonesty incidents will be reported without exception



Ethics

With great power comes great responsibility

- Topics will cover technologies whose abuse may infringe on the rights of others
- When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit written permission from the instructor.

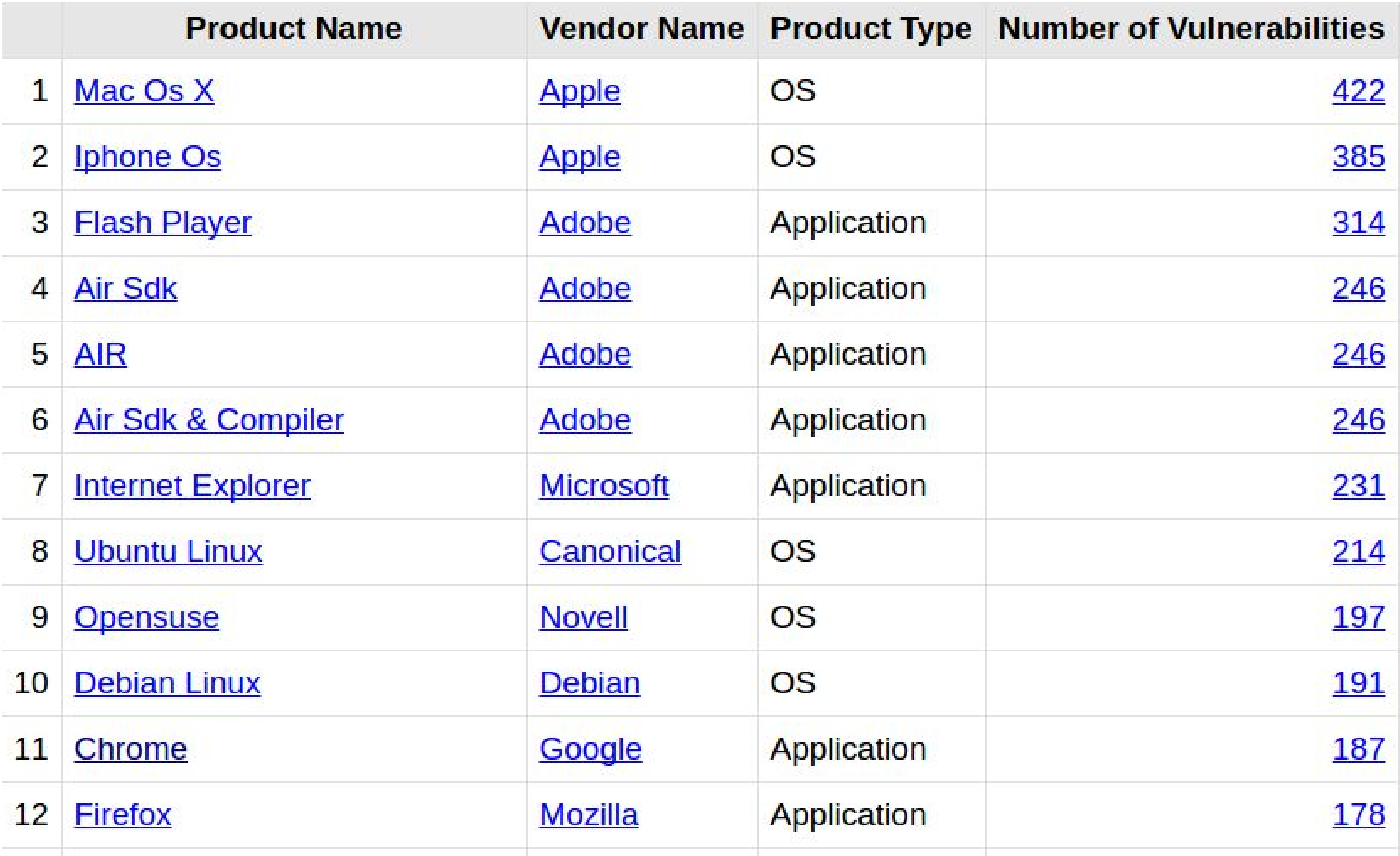
The computer security problem

- Security is everywhere (like the Matrix)
- Developers are not aware of security
(we should fix this!)
  - Buggy software
  - Legacy software
  - Social engineering
- Vulnerabilities can be very damaging (and expensive)

Hacking used to be cool

But now everything is done for profit!

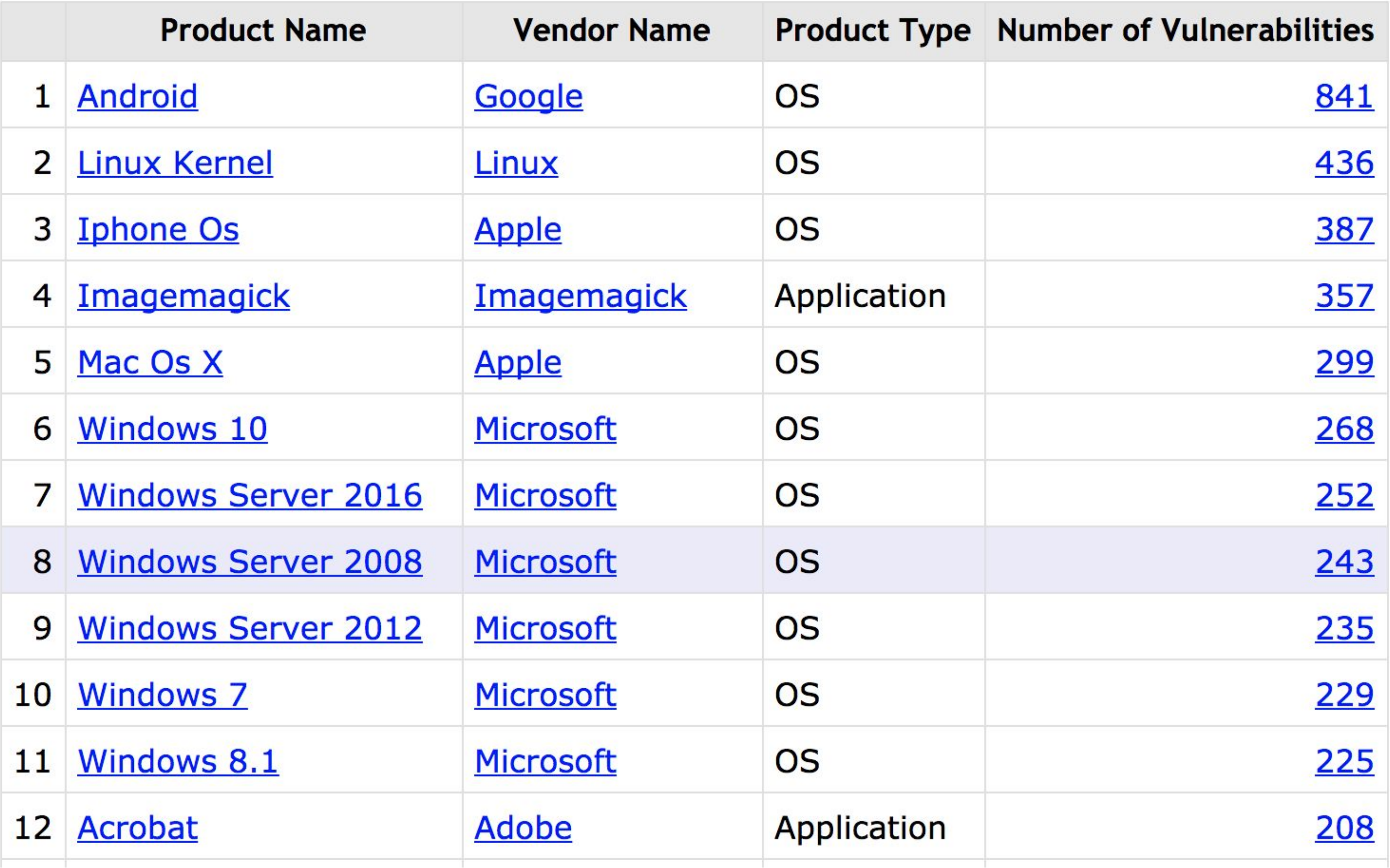
Vulnerabilities per product



	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Mac Os X	Apple	OS	422
2	Iphone Os	Apple	OS	385
3	Flash Player	Adobe	Application	314
4	Air Sdk	Adobe	Application	246
5	AIR	Adobe	Application	246
6	Air Sdk & Compiler	Adobe	Application	246
7	Internet Explorer	Microsoft	Application	231
8	Ubuntu Linux	Canonical	OS	214
9	Opensuse	Novell	OS	197
10	Debian Linux	Debian	OS	191
11	Chrome	Google	Application	187
12	Firefox	Mozilla	Application	178

Source: https://www.cvedetails.com/top-50-products.php?year=2015

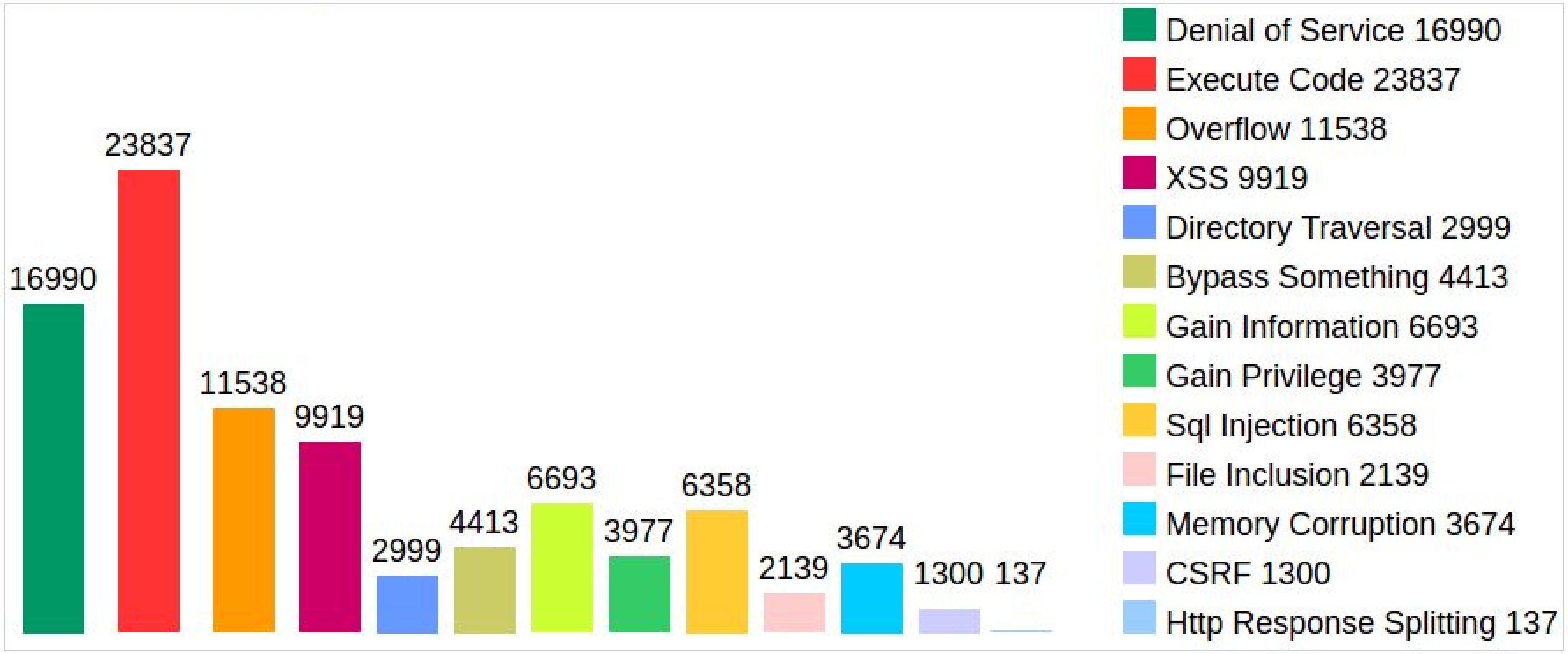
Vulnerabilities per product



	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	841
2	Linux Kernel	Linux	OS	436
3	Iphone Os	Apple	OS	387
4	Imagemagick	Imagemagick	Application	357
5	Mac Os X	Apple	OS	299
6	Windows 10	Microsoft	OS	268
7	Windows Server 2016	Microsoft	OS	252
8	Windows Server 2008	Microsoft	OS	243
9	Windows Server 2012	Microsoft	OS	235
10	Windows 7	Microsoft	OS	229
11	Windows 8.1	Microsoft	OS	225
12	Acrobat	Adobe	Application	208

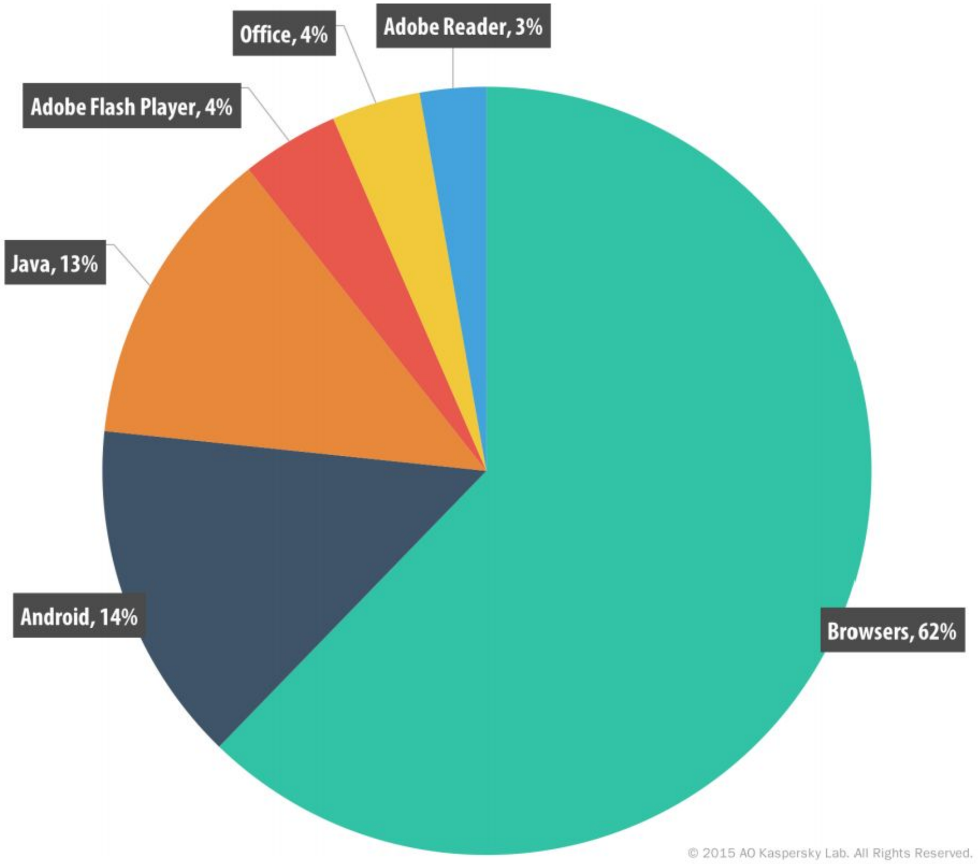
Source: https://www.cvedetails.com/top-50-products.php?year=2017

Vulnerabilities per type



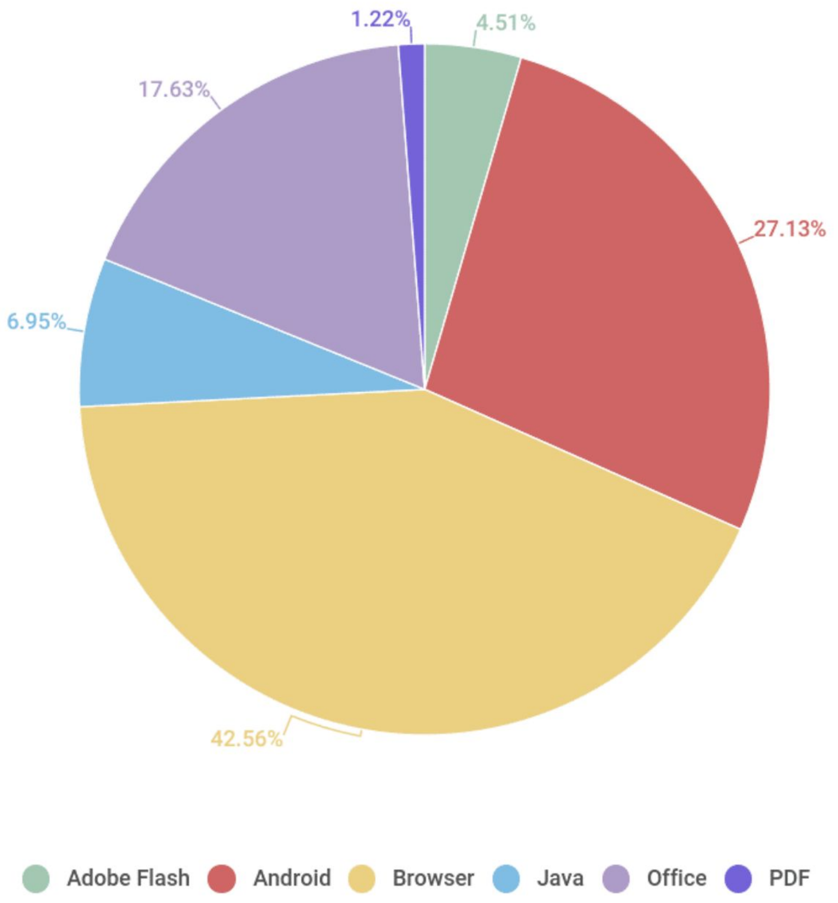
Source: https://www.cvedetails.com/vulnerabilities-by-types.php

Distribution of exploits per application



Source: Kaspersky Security Bulletin 2015

Distribution of exploits per application



Source: Kaspersky Security Bulletin 2017

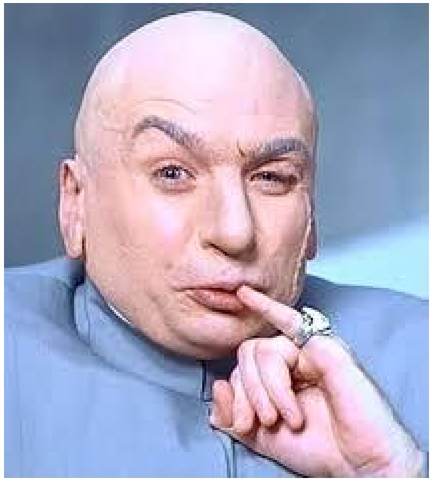
Bug bounty programs

- Companies will pay you money to report vulnerabilities
- Certain conditions and rules per program
  - No Denial-of-service attacks
  - Spam
  - … (depends on the program)

Black market for exploits

Last iOS exploit was sold for

1 million dollars



Exploits for modern software are extremely difficult to write!

Chrome exploit

- Bug 1: run Native Client from any website
- Bug 2: integer underflow bug in the GPU command decoding -> ROP chain in GPU process
- Bug 3: impersonate the renderer from the GPU in the IPC channel
- Bug 4: allowed an unprivileged renderer to trigger a navigation to one of the privileged renderers -> launch the extension manager

Source: https://blog.chromium.org/2012/05/tale-of-two-pwnies-part-1.html

Chrome exploit

- Bug 5: specify a load path for an extension
- Bug 6: failure to prompt for confirmation prior to installing an unpacked NPAPI plug-in extension

Result: install and run a custom NPAPI plugin that executes outside the sandbox at full user privilege

Your Security Zen

Meltdown and Spectre

two major security flaws in the microprocessors inside nearly all of the world’s computers (Intel, AMD, ARM)

Spectre: no easy fix, we have to redesign processors

Meltdown: 30% slow down

There are proof of concepts in the wild that can read host kernel memory from inside a KVM guest

Sources: https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html, https://meltdownattack.com/

See you on Wednesday...