CSC 574
Computer and Network Security

Alexandros Kapravelos
kapravelos@ncsu.edu

Administration

- Class website
  - https://kapravelos.com/teaching/csc574-f16
- Piazza
  - http://piazza.com/ncsu/fall2016/csc574
- Mail to instructor (for private matters)
  - kapravelos@ncsu.edu
- Recorded classes
  - https://oit.online.ncsu.edu/online/Catalog/catalogs/csc-574-001-kapravelos

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) - 40% of grade
  - Homework Assignments - 60% of grade

Topics

Basics

Web Security

Network Security

Mobile Security

You need to understand

- IP Networks
- Modern Operating Systems
- Basics of systems theory and implementation
  - E.g., file systems, distributed systems, networking, operating systems, ...

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

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 an F 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)

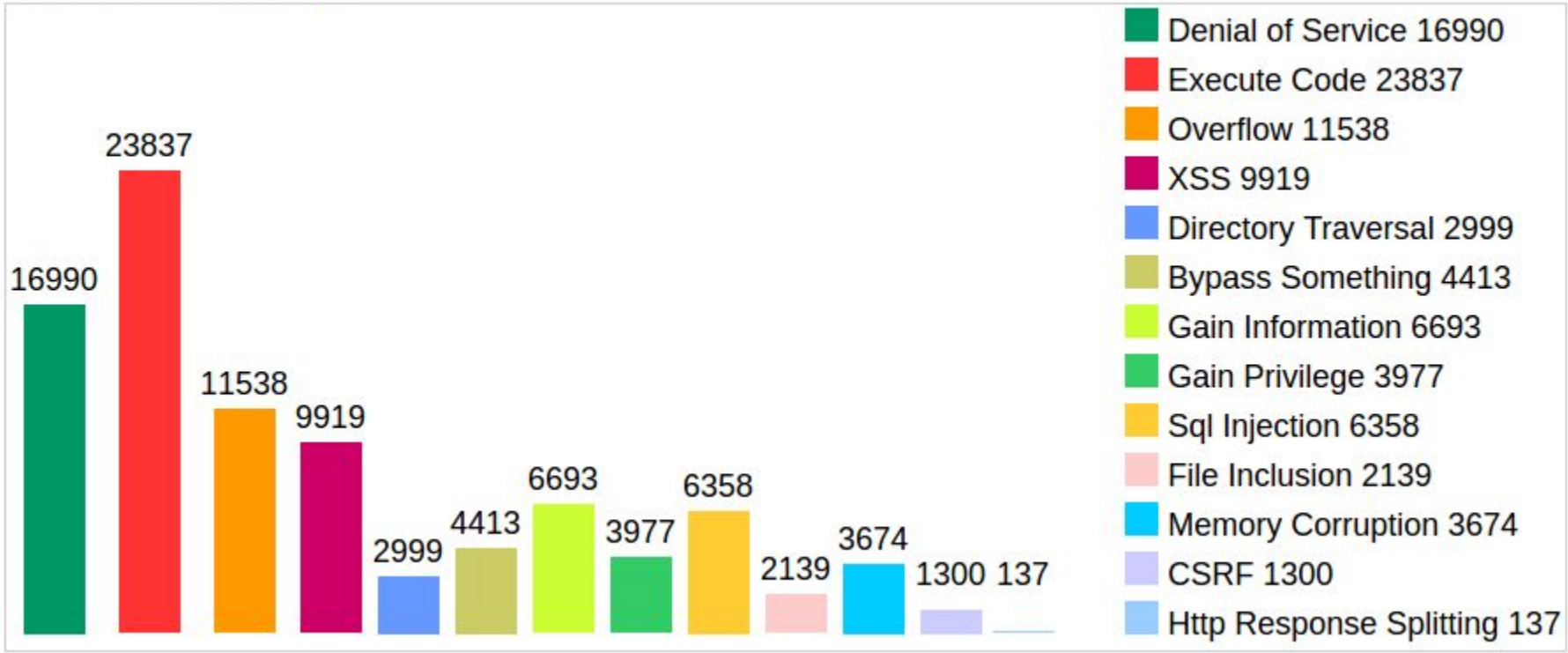
Hacking used to be cool

But now everything is done for profit!

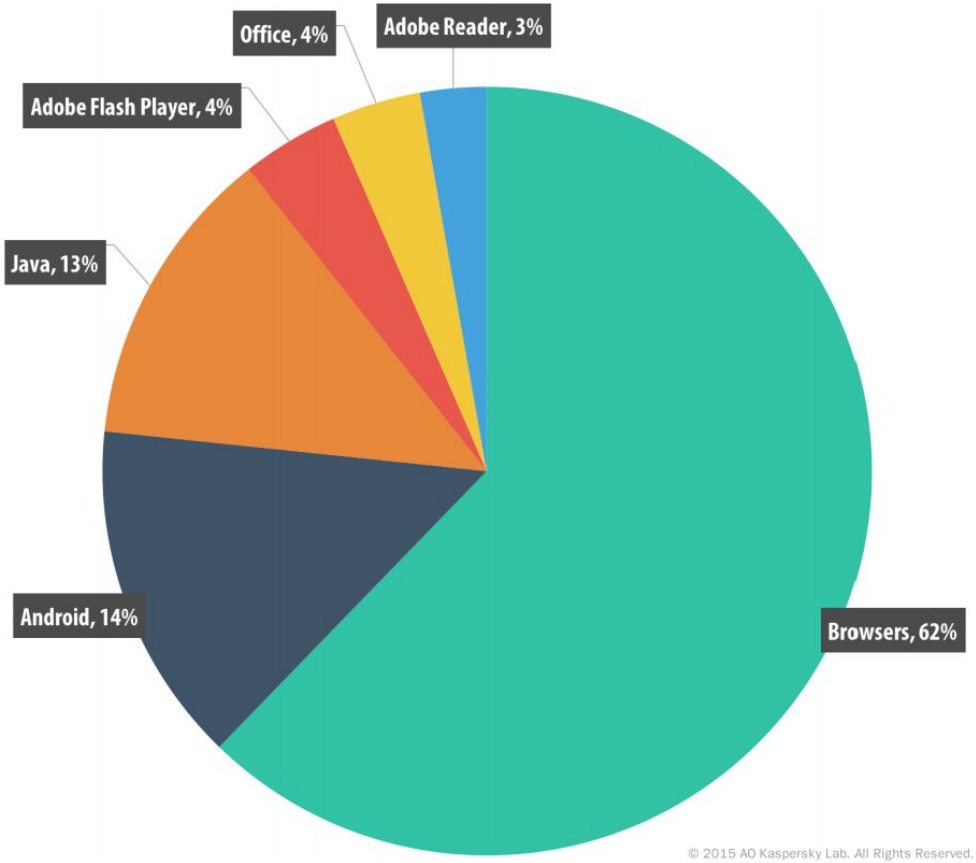
	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Mac Os X	Apple	OS	422
2	Iphone Os	Apple	OS	385
3	Flash Player	Adobe	Application	314
4	Air Sdk	Adobe	Application	246
5	AIR	Adobe	Application	246
6	Air Sdk & Compiler	Adobe	Application	246
7	Internet Explorer	Microsoft	Application	231
8	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 By Type



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



Distribution of exploits used in cyberattacks, by type of application attacked, 2015

Source: Kaspersky Security Bulletin 2015

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 on 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

Readings for Monday are up!