CSC 405
Computer Security

Alexandros Kapravelos
akaprav@ncsu.edu

Why take a course in computer security?

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 - 2015

	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 - 2017

	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 product - 2018

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	908
2	Android	Google	OS	597
3	Ubuntu Linux	Canonical	OS	478
4	Enterprise Linux Server	Redhat	OS	387
5	Enterprise Linux Workstation	Redhat	OS	370
6	Enterprise Linux Desktop	Redhat	OS	362
7	Firefox	Mozilla	Application	333
8	Acrobat Reader Dc	Adobe	Application	286
9	Acrobat Dc	Adobe	Application	286
10	Windows 10	Microsoft	OS	254

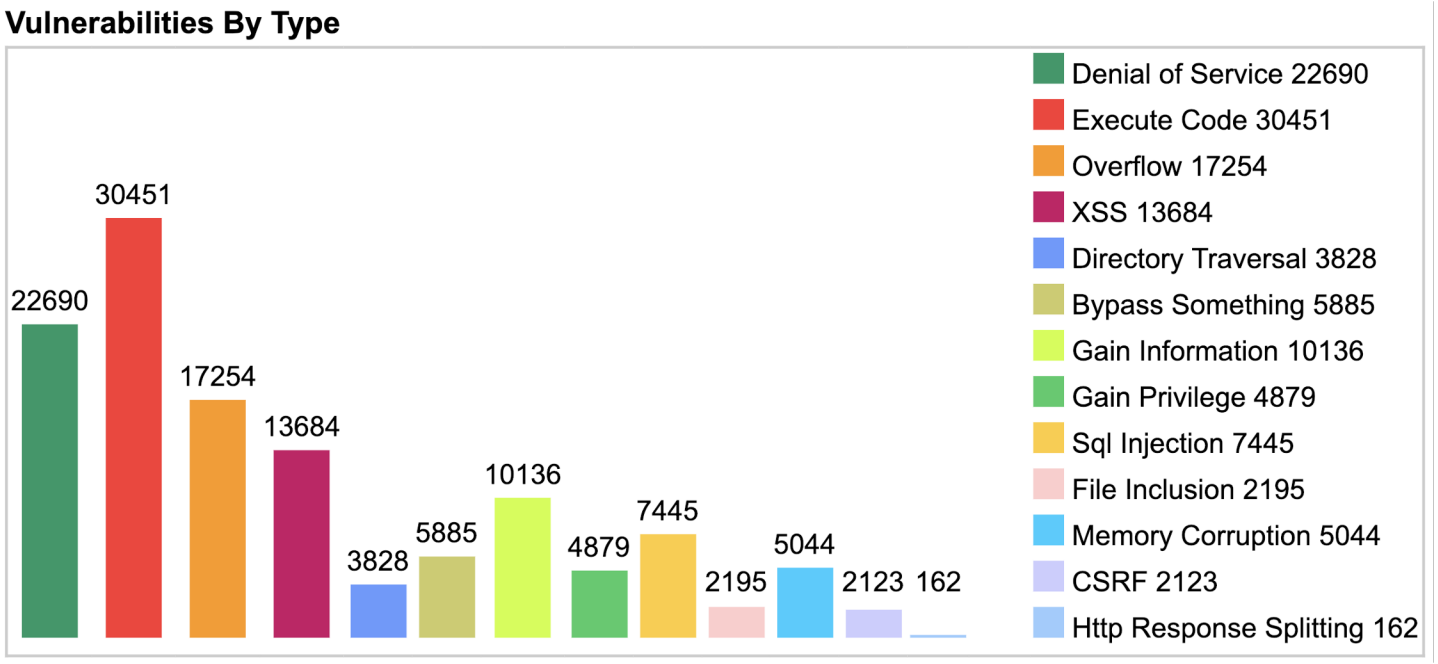
Source: https://www.cvedetails.com/top-50-products.php?year=2018

Vulnerabilities per product - 2019

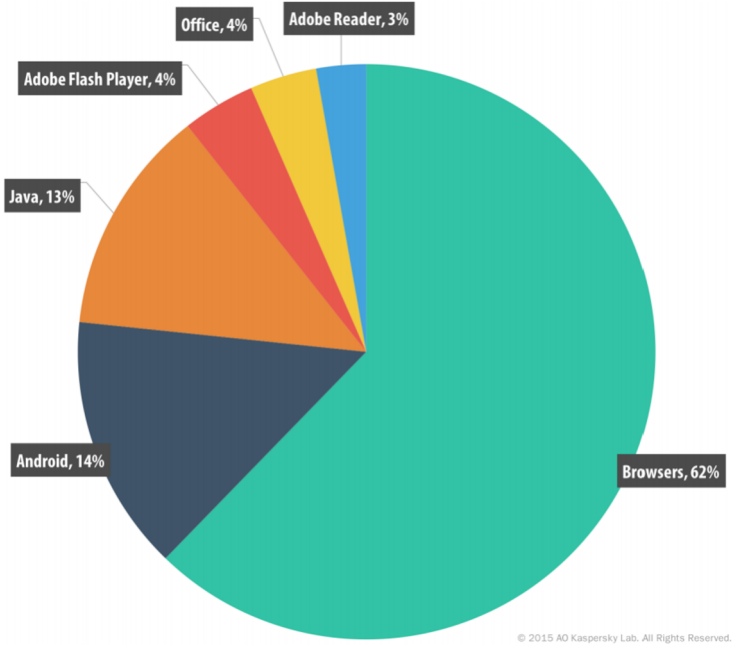
	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	414
2	Debian Linux	Debian	OS	360
3	Windows Server 2016	Microsoft	OS	357
4	Windows 10	Microsoft	OS	357
5	Windows Server 2019	Microsoft	OS	351
6	Acrobat Reader Dc	Adobe	Application	342
7	Acrobat Dc	Adobe	Application	342
8	Cpanel	Cpanel	Application	321
9	Windows 7	Microsoft	OS	250
10	Windows Server 2008	Microsoft	OS	248

Source: https://www.cvedetails.com/top-50-products.php?year=2019

Vulnerabilities per type - 1999-2018

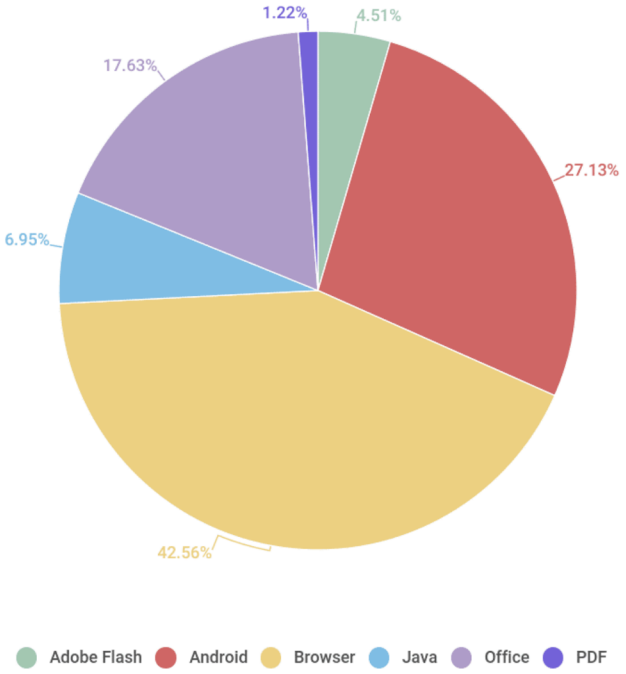


Distribution of exploits per application 2015



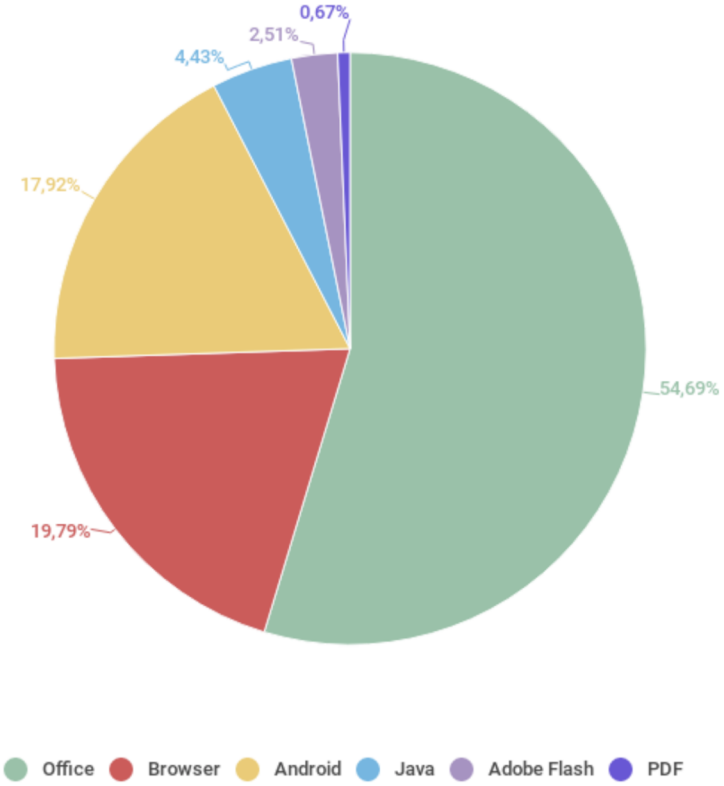
Source: Kaspersky Security Bulletin 2015

Distribution of exploits per application 2017



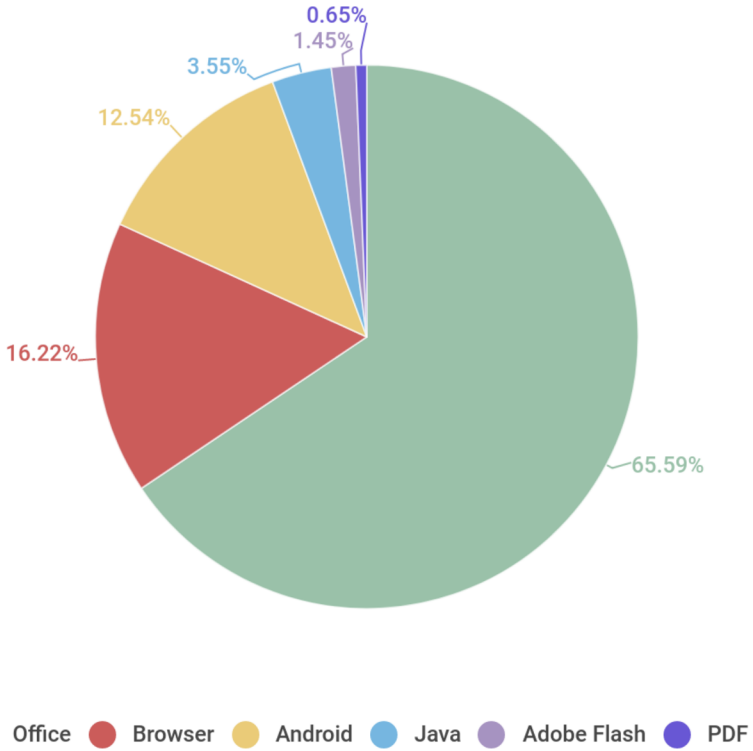
Source: Kaspersky Security Bulletin 2017

Distribution of exploits per application 2018



Source: Kaspersky Security Bulletin 2018

Distribution of exploits per application 2019



Source: Kaspersky Security Bulletin 2019

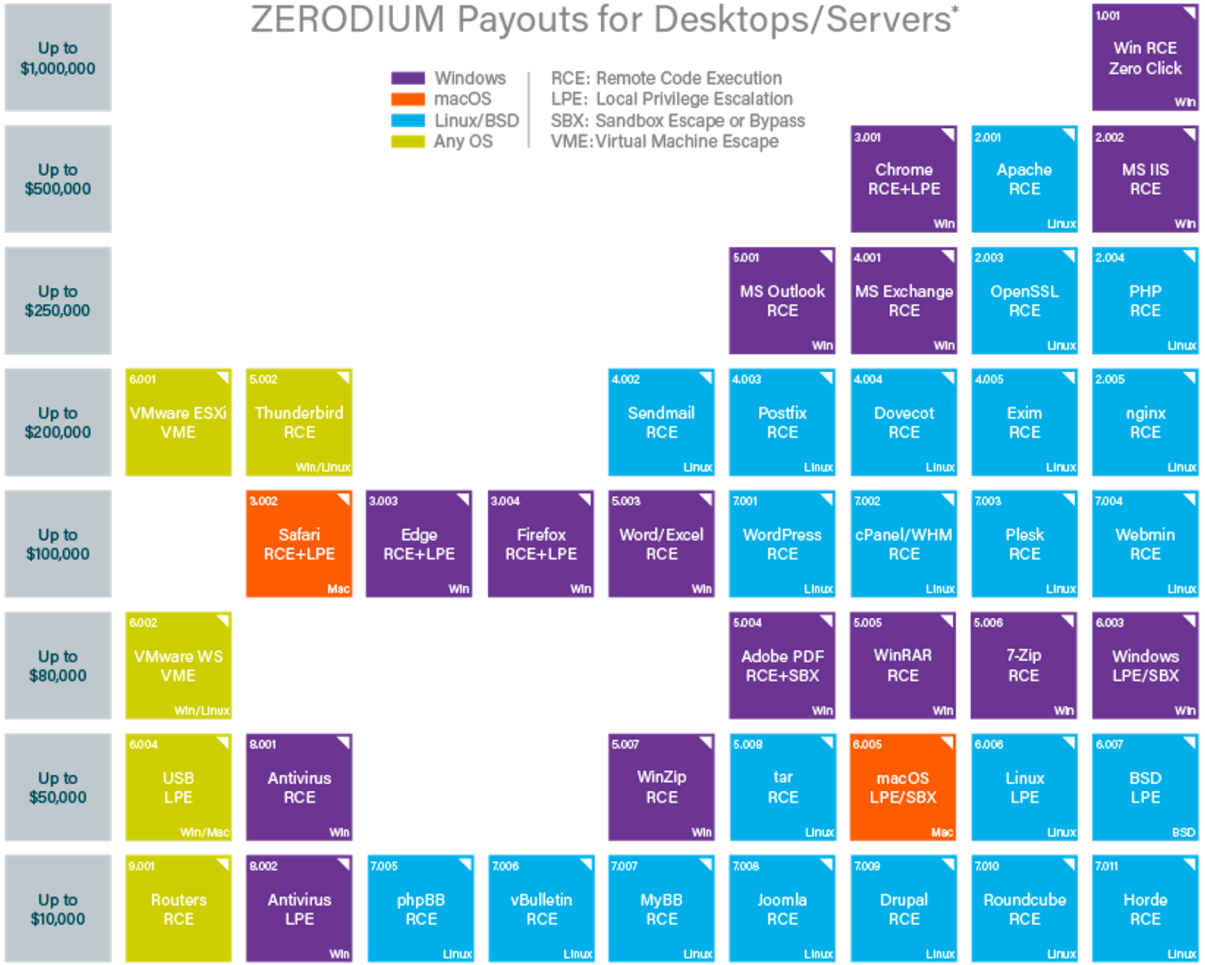
Bug bounty programs

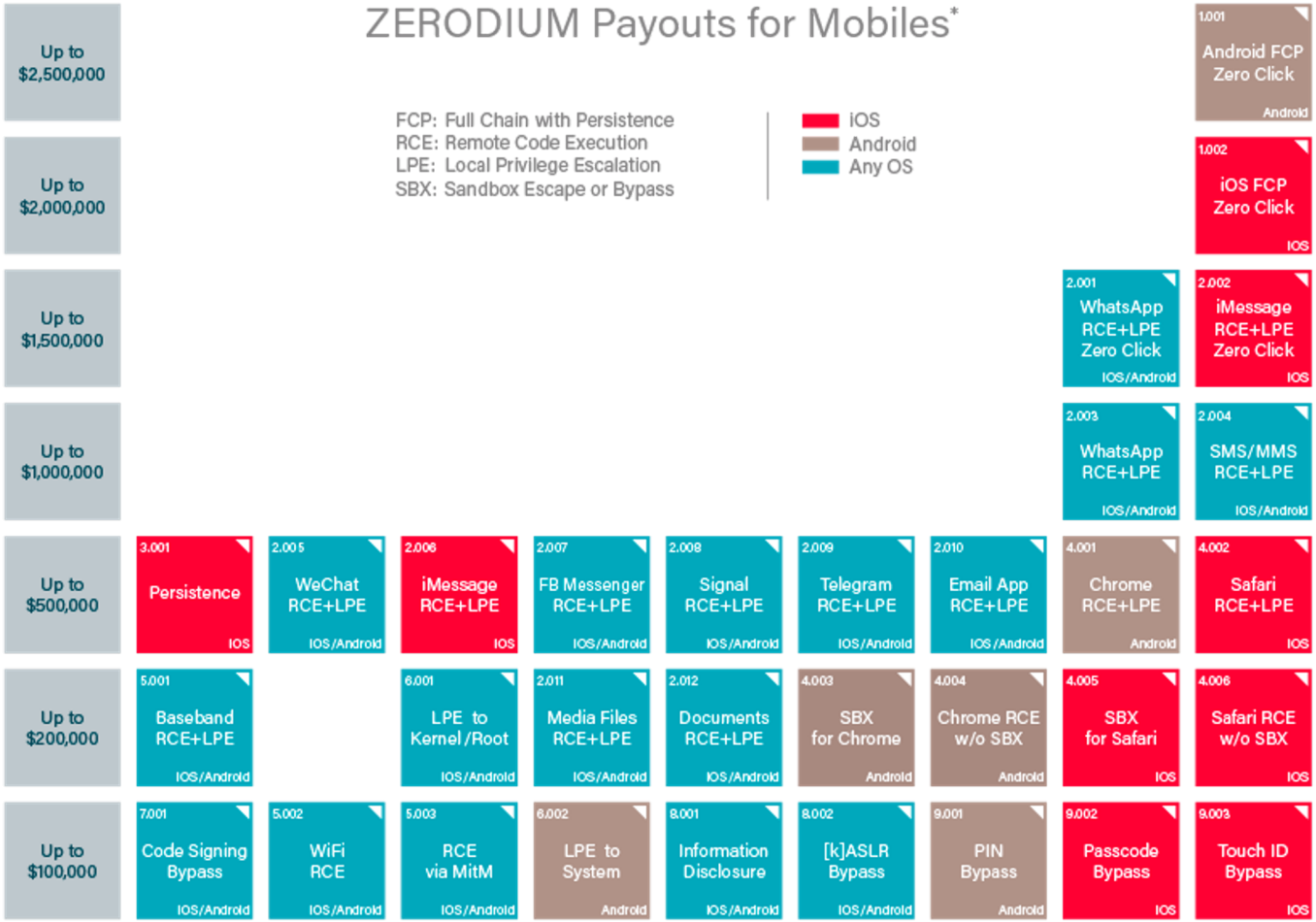
- Companies will pay you money to report vulnerabilities
- Certain conditions and rules per program
  - No Denial-of-service attacks
  - Spam
  - … (depends on the program)

Black market for exploits

Last iOS exploit was sold for

1 million dollars


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $1,000,000
1.001 Win RCE Zero Click Win
Up to $500,000
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $250,000
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $200,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
4.002 Sendmail RCE Linux
4.003 Postfix RCE Linux
4.004 Dovecot RCE Linux
4.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $100,000
3.002 Safari RCE+LPE Mac
3.003 Edge RCE+LPE Win
3.004 Firefox RCE+LPE Win
5.003 Word/Excel RCE Win
7.001 WordPress RCE Linux
7.002 cPanel/WHM RCE Linux
7.003 Plesk RCE Linux
7.004 Webmin RCE Linux
Up to $80,000
6.002 VMware WS VME Win/Linux
5.004 Adobe PDF RCE+SBX Win
5.005 WinRAR RCE Win
5.006 7-Zip RCE Win
6.003 Windows LPE/SBX Win
Up to $50,000
6.004 USB LPE Win/Mac
8.001 Antivirus RCE Win
5.007 WinZip RCE Win
5.008 tar RCE Linux
6.005 macOS LPE/SBX Mac
6.006 Linux LPE Linux
6.007 BSD LPE BSD
Up to $10,000
9.001 Routers RCE
8.002 Antivirus LPE Win
7.005 phpBB RCE Linux
7.006 vBulletin RCE Linux
7.007 MyBB RCE Linux
7.008 Joomla RCE Linux
7.009 Drupal RCE Linux
7.010 Roundcube RCE Linux
7.011 Horde RCE Linux
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/01 © zerodium.com



** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

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

Next class

Refresh your assembly skills!