Imperial College
London

CO331 – Network and Web Security

2. Vulnerabilities

Dr Sergio Maffeis
Department of Computing
Course web page: http://www.doc.ic.ac.uk/~maffeis/331

Vulnerabilities

Imperial College London

- *Vulnerabilities* are software bugs that attackers can exploit in order to compromise computers
- *Exploits* are pieces of software that take advantage of a vulnerability in order to access or infect a computer
- A *zero day* vulnerability/exploit is one that is unknown to the software vendor
- Who finds zero-days, what do they do with them, and why?
  - Vendor's employees: **fix** (it's their job)
  - Security companies: **sell, disclose** (it's part of their business model)
  - Independent security researchers: **sell, disclose** (for profit or fame)
  - Academics: **disclose** (to make the world a better place)
  - Government agents: **exploit, disclose** ("to protect and to serve")
  - Criminals: **exploit, sell** (for profit)
  - Terrorists: **exploit** (to wreck havoc)
  - Hacktivists: **exploit** (to make the world a better place, according to their idea of "better place")

Advisories

Imperial College London

- Security advisories or bulletins publicly disclose new vulnerabilities
  - Issued by vendors or security companies
  - Describe individual vulnerabilities or groups of them
    - Example: monthly Microsoft Security Bulletin
  - Important for developers, sysadmins, users
- All published vulnerabilities are classified and given a unique ID
  - Example: CVE-2014-0160 is the ID for Heartbleed
  - CVE stands for Common Vulnerabilities and Exposures (CVE)
    - Includes *exposures* (system misconfigurations)
  - Stored in the US National Vulnerability Database hosted by NIST: http://nvd.nist.gov
- There are mailing lists to report vulnerabilities
  - Full Disclosure: http://seclists.org/fulldisclosure/
- Once a vulnerability is public, proof of concept exploits may become available
  - Public database of exploits: http://www.exploit-db.com

Vulnerability reports

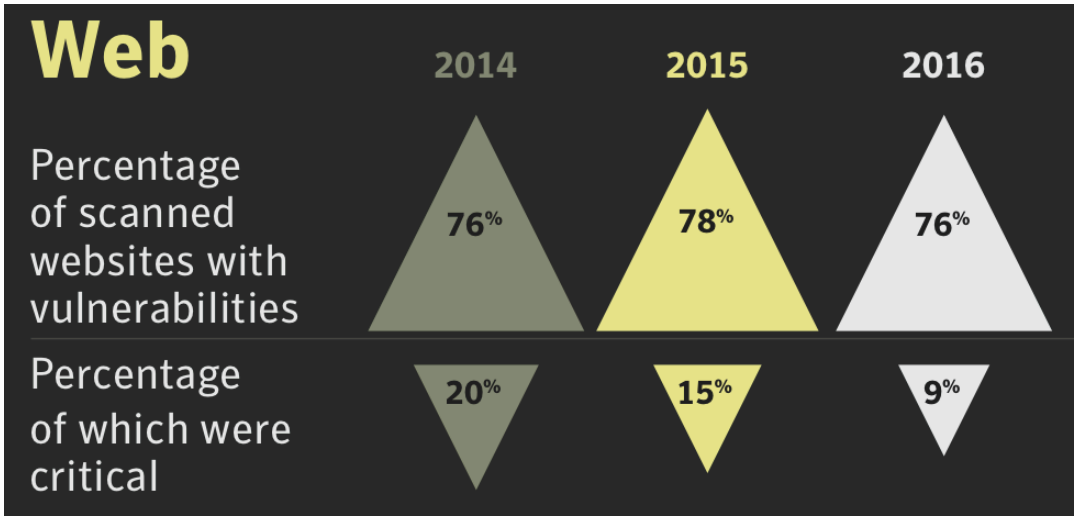
Imperial College London

- CVE entries give concise descriptions of the issue and references to reports or advisories
- Vulnerabilities are reported in various formats
  - Bugs and systems differ from each other
  - Researchers put different levels of effort
  - Some bugs are hard to exploit
  - Some are hard to fix
- Key information (if available)
  - Date
  - Affected system
  - Description of vulnerability
  - Assessment of impact
  - Proof of concept exploit code
  - Proposed fix
  - Credits: who found it?

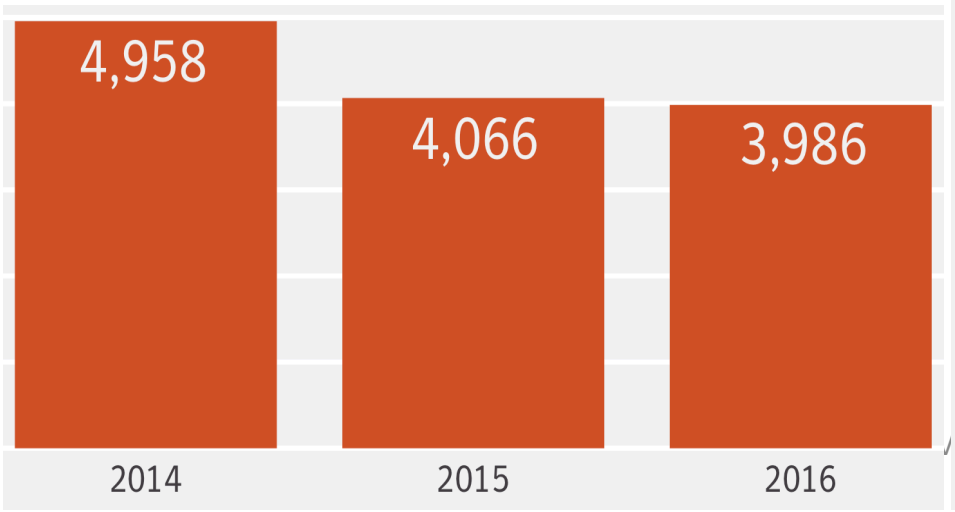
Some stats

Imperial College London

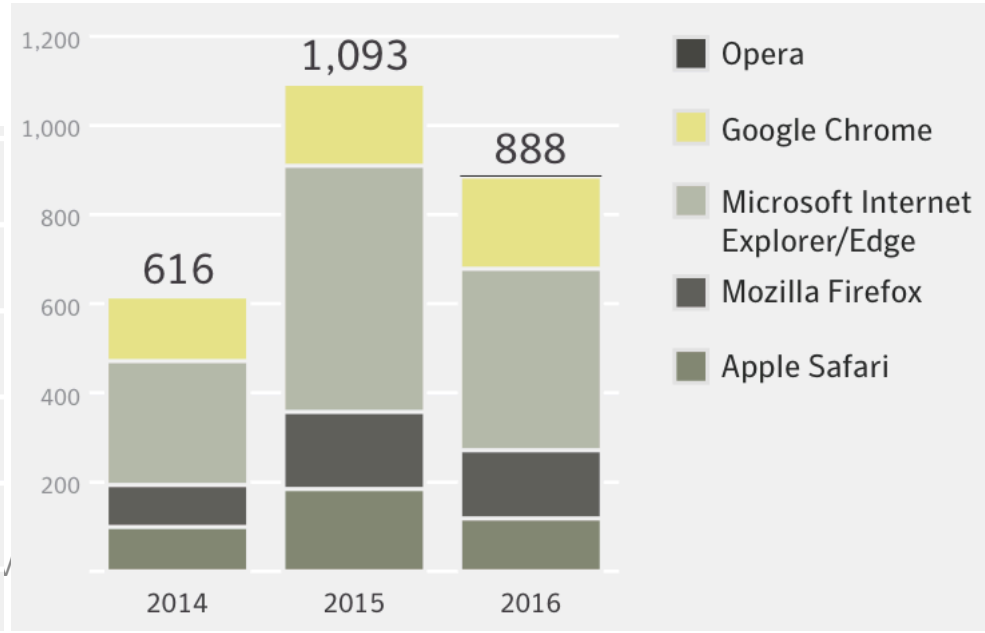
Internet Security Threat Report, Symantec, 2017



"0-day" vulnerabilities



Browser vulnerabilities



Ethics

Imperial College London

You discover a vulnerability in a popular piece of software. What to you do?

- "***Full disclosure*** *-- the practice of making the details of security vulnerabilities public -- is a damned good idea. Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure*" (Bruce Schneier)
  - Preferred by prominent security researchers, open source community
  - May expose users to attack until a patch is available
  - But attackers may already know about the vulnerability anyway
- **Responsible disclosure**: affected vendor decides when to release information, and how much
  - Preferred by software vendors
  - Motivation: "end-users will not develop their own patches"
  - Can lead to excessive long time from discovery to fix
- **Non disclosure**: keep the vulnerability secret
  - Preferred by parties that intend to exploit vulnerabilities, and by vendors unwilling to invest resources in fixing them
  - Based on discredited principle: "security by obscurity"

Hoarding vulnerabilities?

Imperial College London

c|net

REVIEWS | NEWS | VIDEO | HOW TO | SMART HOME | CARS | DEALS

SECURITY

'Doomsday' worm uses seven NSA exploits (WannaCry used two)

The recently discovered EternalRocks joins a set of highly infectious bugs created from the NSA's leaked tools.

BY ALFRED NG / MAY 22, 2017 1:08 PM PDT

ZDNet

RE | APPLE | MORE | NEWSLETTERS

MUST REA

HE ONEPLUS 5T

Windows 10: UK's GCHQ found out how to hack Windows Defender to own your PC

And it didn't keep the vulnerability to itself.

By Liam Tung | December 8, 2017 -- 12:10 GMT (12:10 GMT) | Topic: Enterprise Software

For fun and for profit

Imperial College London

- Bug bounty programs
  - Some software vendors offer rewards for vulnerabilities in their products
    - Mozilla up to $30k, Google up to $20k, Microsoft up to $100k
    - Some companies just offer recognition
  - Looking for vulnerabilities can be instructive, fun and profitable
    - Companies give explicit permission on what can be attacked
    - Don't overstep their boundaries
  - Most relevant to this course: https://hackerone.com/internet-bug-bounty
- Competitions
  - "Capture the flag" (CTF): highly visible recognition
    - Ghost in the Shellcode, UCSB iCTF, …
  - Pwn2Own: $15k
- 331 Bug Bounty!
  - Full coursework marks if you report CVE or Hackerone vuln credited between now and week 10

Vulnerability markets

Imperial College London

- Legitimate vulnerability markets
  - Run by security companies: ZDI, iDefense
  - Paid like a bug bounty program
  - They buy vulnerabilities and re-sell them to vendors
- Black market
  - Mostly on the dark web
  - More profitable
    - But figures are dubious
    - Mutual trust issues
  - It's illegal!

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Black market prices (Forbes, 2012)

Stay out of trouble

Imperial College London

- To defend a system you need to be able to think like an attacker
  - That includes learning techniques that can be used to compromise security
  - Do not attack systems that do not belong to you or for which you do not have explicit consent by all involved parties
  - Ignoring this may result in severe penalties, including expulsion from college, fines, and criminal lawsuits
- Imperial college policies: https://www.imperial.ac.uk/admin-services/secretariat/college-governance/charters/policies-regulations-and-codes-of-practice/information-security-/policy/it-resources/
- UK Computer Misuse Act 1990: used for criminal prosecution of
  - Denial of service attacks
  - Fraudulent activities in online games
  - Illegal access and disclosure of confidential emails and personal information
  - Theft from online banks
  - Piracy

Jail for 'ethical' hacker who bypassed Facebook security from his bedroom

20 FEB 2012 54

Data loss, Facebook, Law & order, Social networks, Vulnerability

f 287

by Graham Cluley

A British student who breached security at Facebook last year has been sentenced to eight months in jail, despite arguing that his intentions were not malicious.

Glenn Mangham, who had previously been rewarded by Yahoo for finding vulnerabilities in its systems, unlawfully accessed and hacked into Facebook's computer systems between April and May last year from his bedroom in York.

Specifically, Mangham breached a webserver used by Facebook to set puzzles to software engineers who might be interested in working for the social network.