Cyber Security

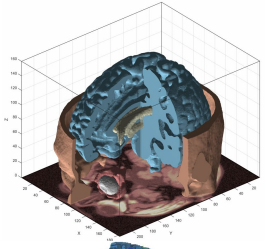
Introduction, history and terminology

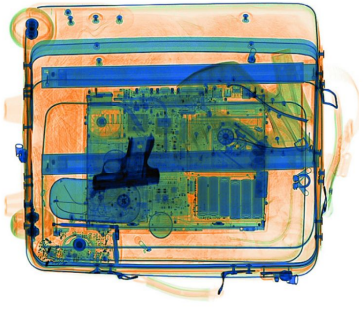
Chris G. Willcocks
Durham University

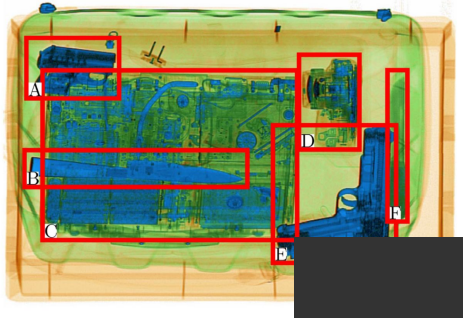
Introduction about me

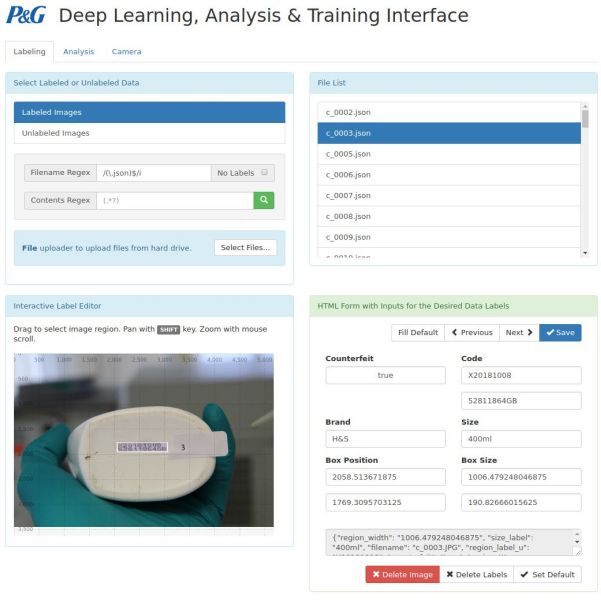
- DL & Cyber: Mostly industry projects
- Government (defence) projects
- Medical projects with sensitive data
- Anti-Counterfeiting

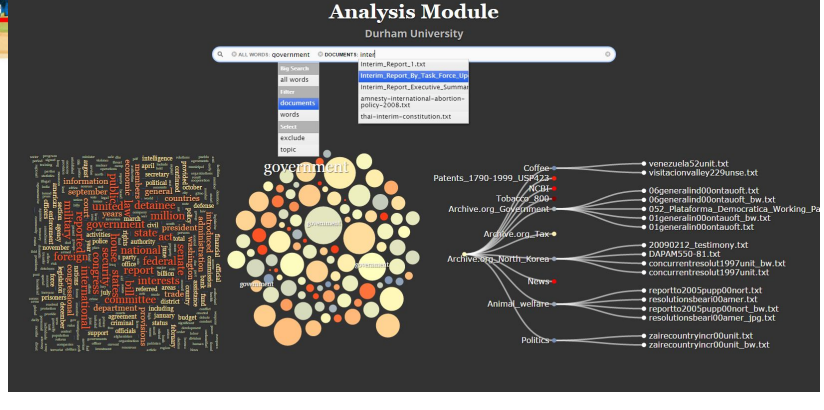
1. NHS
2. DSTL
3. Unilever
4. P&G, Dyson
5. AstraZenica
6. NERSOU











Ministry of Defence [dstl]

NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT
Protecting communities from organised crime

Introduction submodule outline

- This course is not like the others
  - Cyber security is not really a science.
- Course with 10 lectures
- Specialist lab with NERSOU
  - This is excellent security experience
- 3x primary 2-hour labs
  1. Building a secure system
  2. Hacking the system
  3. Securing the system from the vulnerability
  4. Hacking the system again with a smarter method
  5. Repeating
- Summative coursework assignment
  - Given **early on** teaching week 13
- 100% assessed by the coursework

NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT
Protecting communities from organised crime

Introduction teaching approach

- Prioritising breadth >> depth
  - Introductory coverage of all main areas
  - Awareness is important in your future careers
- Prioritised by popularity
  - There are lots of “interesting” small hacks in limited domains, we cover main stuff that you will most likely encounter
- Offensive & defensive
  - Learning where to look
  - Learning what not to rush & what needs doing

image from https://mile2.com

Pentester mindset

- “Surely they won’t do that” → “Surely they will!”
- Think like a hacker, “where are the easy assets?” Think blue to assess the threat and risk.

WARNING: Not everything you can technically do is legal!

You will learn things in this module that are technically possible. **But**!

Nothing here is intended as an incitement to crack.

Breaking into systems to "demonstrate" security problems best causes a headache to overworked sysadmins, and at worst compromises the system for many users and could lead to **prosecution**.

If you spot a security hole, **don't exploit it**, instead report it to the relevant administrators confidentially.

Introduction pathway to becoming a Cyber Security professional

- Create your own mini cyber security lab

Install VirtualBox on your PC

vmware

Your lab

Learn the tools, learn the culture...

KALI

archlinux

BLACK ARCH

ATTACK!

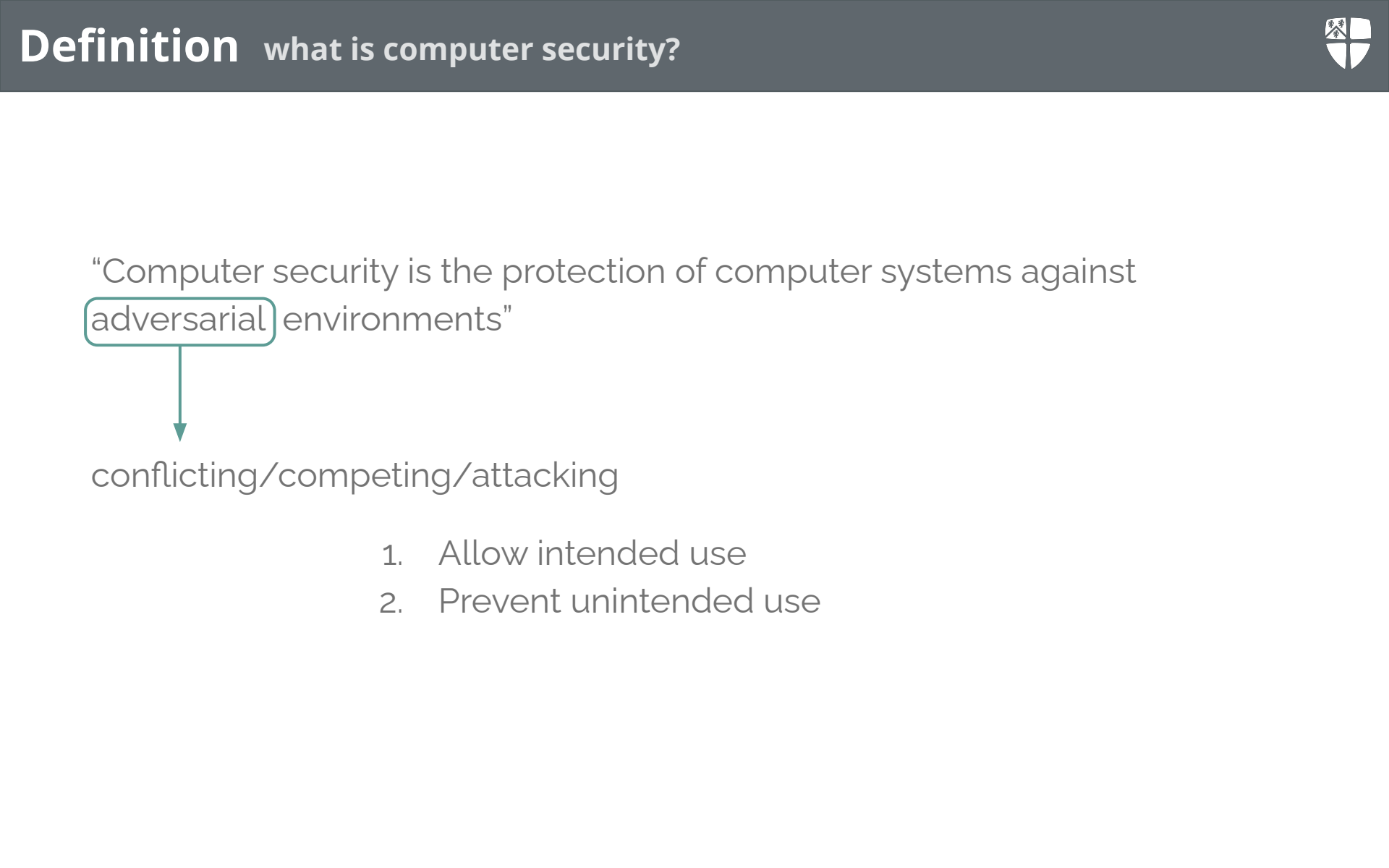
Target on LAN or further...

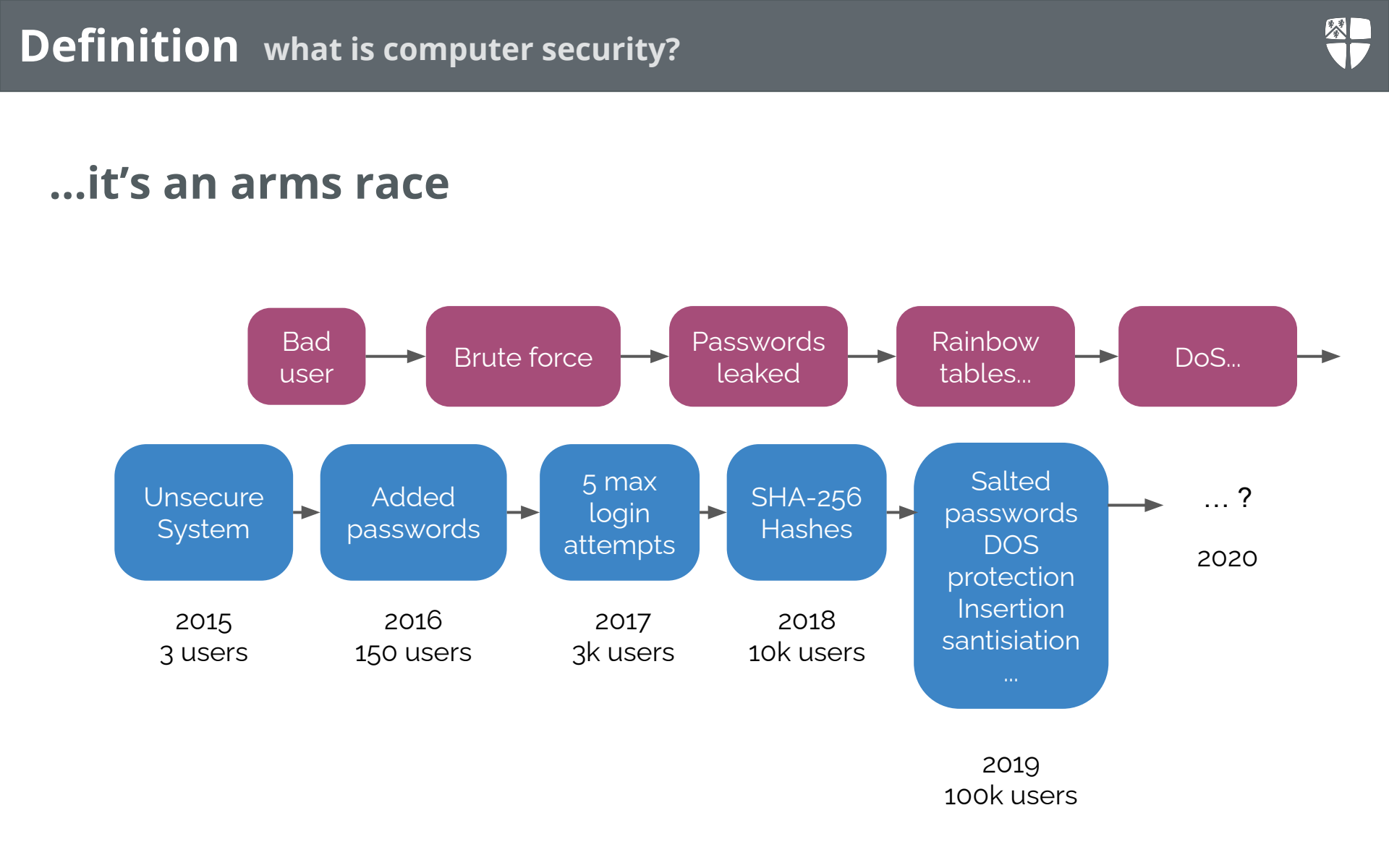
Windows 10

debian

ubuntu
linux for human beings

Definition what is computer security?





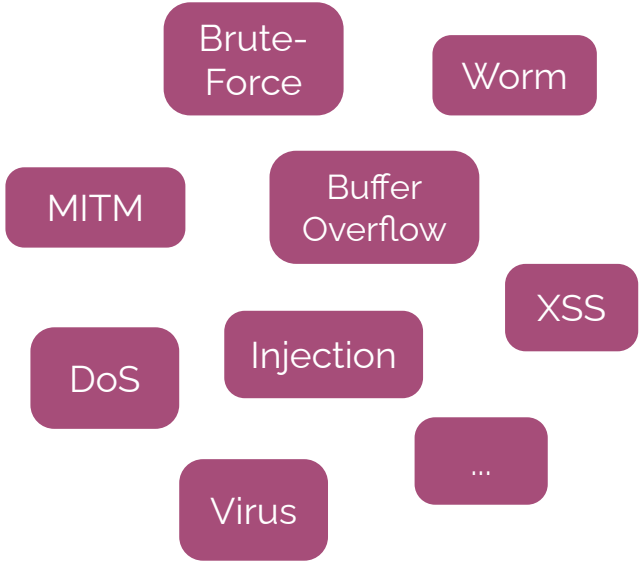
...it's an arms race

...however

The same patterns tend to crop up again and again with new and evolving variations.

In this short course you will:

1. Learn these **patterns**
2. Learn how **easy** they are to exploit
3. Learn how to **protect** against them
4. Raise **awareness** of issues



Why is this compulsory?

Undergraduate jobs:

1. **Software developer**

   Client logins at Tesla, billing systems at Ebay, User data at Facebook, Gmail, databases at AWS, ...

2. **Manager** with tight deadlines - hope you'll remember this sub-module
3. **Research** job with sensitive data
4. **Systems administrator** with user data
5. **Game developer** with user data
6. **Data analyst** with sensitive patient information on your local machine

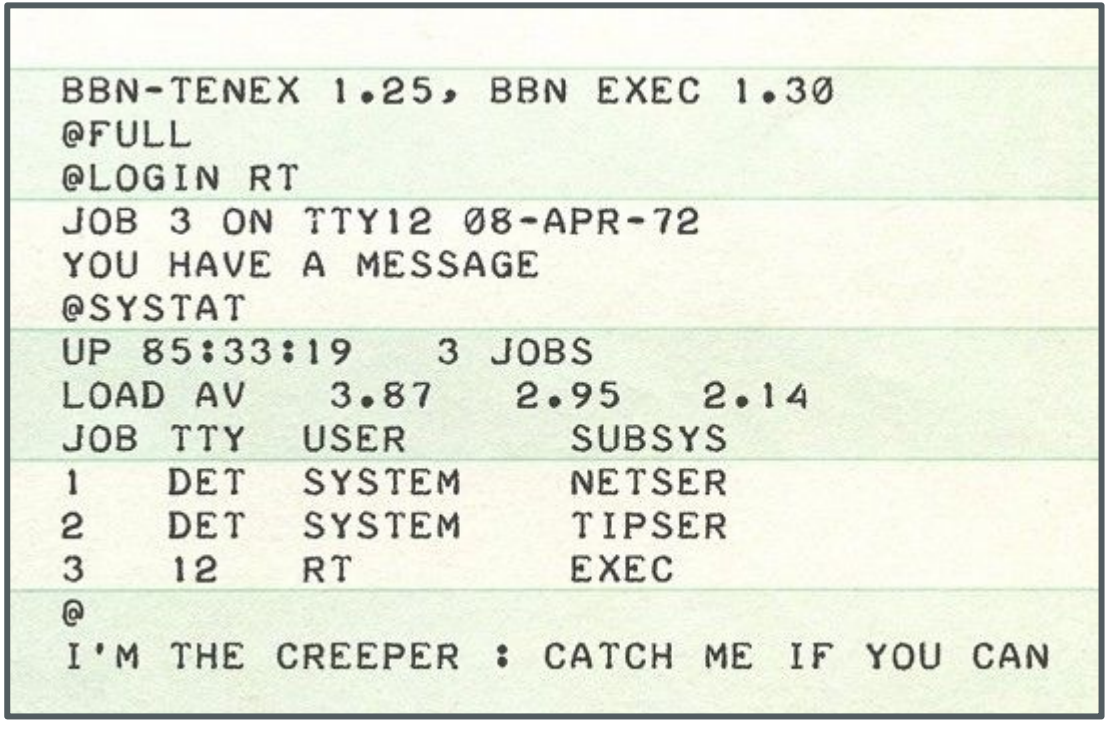
   ...

History a brief history of cyber security

Major historical events:

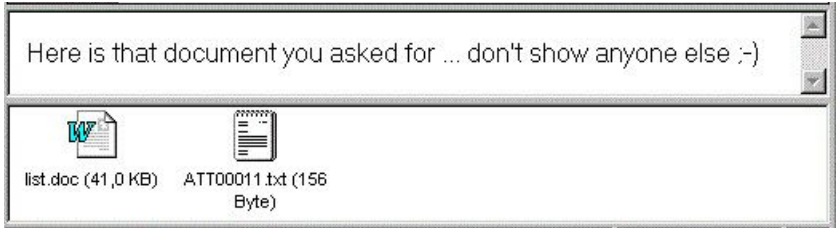
1971: Creeper- first worm. On teletype! Reaper was made to delete Creeper.

1988: The Morris worm, created by Robert Morris to assess the size of the internet. First to be convicted under misuse act. Now a professor at MIT.



History a selection of historical hacks

2000: The **Melissa** and **ILOVEYOU** virus. LOVE-LETTER-FOR-YOU.txt**.vbs** Windows hid extensions by default.



2005-2007: TJX was hacked (TK Maxx) 45 million credit card details stolen. Cost the company $256 million.

2013: Yahoo breach. Worse than initially reported; all 3 billion Yahoo users details stolen (news since 3 October 2018).

2017: WannaCry ransomeware. Encrypted hard drive demanding BitCoins. Not much money retrieved by estimated damage $4 billion.

2017: Net neutrality debate. Age of botnets 80% bots on FCC.

How big is cyber security today?

1. As of 2004 the cybersecurity market was **$3.5 billion**
2. As of 2017 the cybersecurity market is **£120 billion**
3. Spending predicted to exceed **$1 trillion** from 2017 to 2021 (report)

Link to real-time map

Link to visualisation of security breaches

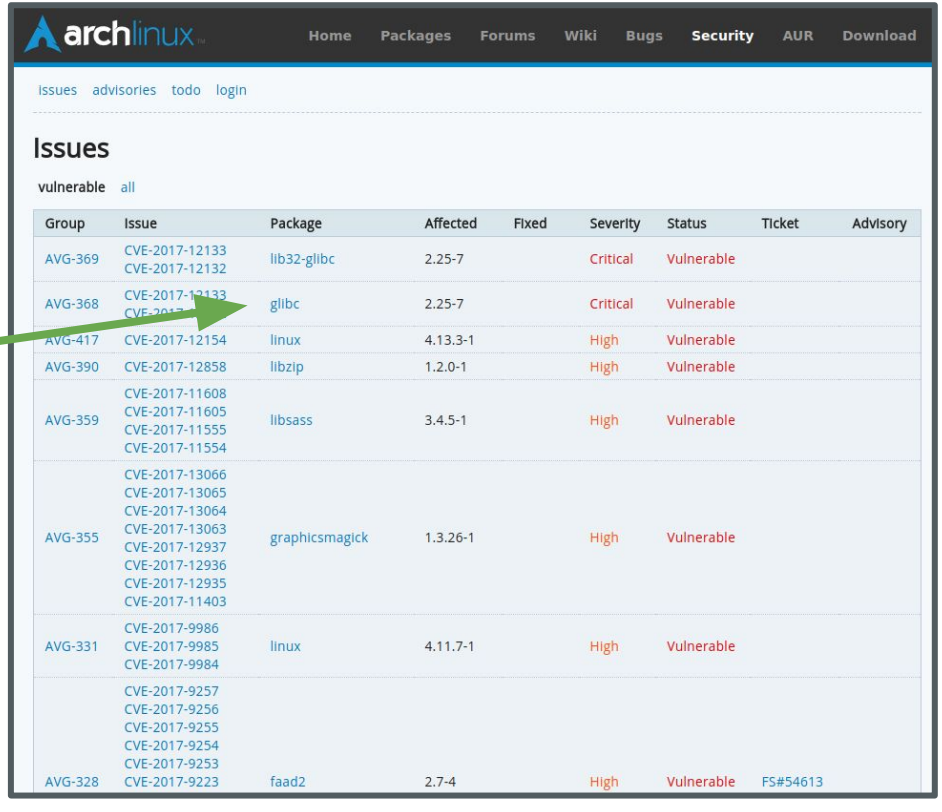
New national cyber security centre, part of GCHQ.

Most of it is unreported

Big stories hit the news every so often, but actually every day:

1. Privilege escalation
2. Arbitrary code execution

Type	Issues	Local	Remote	Open	Fixed
Unknown	0	0	0	0	0
Critical	390	0	390	32	358
High	545	122	423	24	521
Medium	806	154	652	29	777
Low	253	92	161	21	232
Total	1994	368	1626	106	1888



...so much to choose from!

Type	Issues	Local	Remote	Open	Fixed	Advisories
multiple issues	-	-	-	-	-	211
unknown	0	0	0	0	0	0
access restriction bypass	103	23	80	9	94	14
arbitrary code execution	676	[illegible]	616	36	640	118
arbitrary command execution	30	8	22	1	29	16
arbitrary file overwrite	6	5	1	1	5	3
arbitrary filesystem access	11	3	8	0	11	1
arbitrary file upload	0	0	0	0	0	0
authentication bypass	10	0	10	0	10	2
certificate verification bypass	3	0	3	0	3	3
content spoofing	83	1	82	2	81	2
cross-site request forgery	8	0	8	0	8	2
cross-site scripting	61	2	59	2	59	8
denial of service	645	[illegible]	[illegible]	38	607	85
directory traversal	8	0	8	0	8	2
incorrect calculation	8	0	8	0	8	0
information disclosure	185	38	147	12	173	28
insufficient validation	34	5	29	1	33	6
man-in-the-middle	11	0	11	0	11	3
open redirect	5	0	5	0	5	2
private key recovery	12	5	7	0	12	6
privilege escalation	66	[illegible]	16	1	65	35
proxy injection	1	0	1	0	[illegible]	3
same-origin policy bypass	17	1	16	3	14	0
sandbox escape	4	1	3	0	4	0
session hijacking	2	0	2	0	2	1
signature forgery	0	0	0	0	0	0
silent downgrade	1	0	1	0	1	0
sql injection	1	0	1	0	1	0
time alteration	0	0	0	0	0	0
url request injection	1	0	1	0	1	0
xml external entity injection	2	0	2	0	2	1
Total	1994	368	1626	106	1888	552

Execute whatever you like...

Get whatever you like from others...

...and do whatever you like...

Topics in this sub-module

1. History, cybersecurity today and basic terminology (this week)
2. Applied cryptography
3. Identification, authentication, authorization
4. Operating system security (recommended for coursework)
5. Network & web security
6. Database security
7. Exploits and malware
8. Human factors
9. Software security (a double lecture as needs some training in assembly)

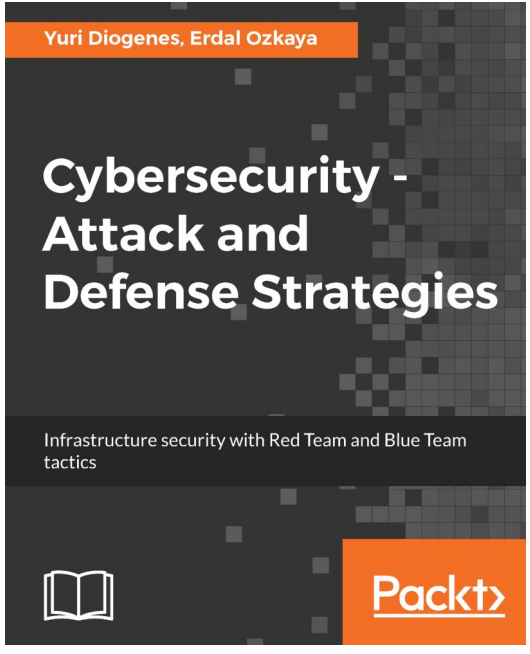
Terminology 1/2

1. **Assets**
   - Something of value to a person or organisation.
2. **Vulnerability**
   - Weakness of a system that could be accidentally or intentionally exploited to damage assets.
3. **Threat**
   - Potential danger of an adversary exploiting a vulnerability.
4. **Risk**
   - Asset x Threat x Vulnerability.
5. **Adversaries**
   - An agent (person, government, press, ...) that circumvents the security of a system.
6. **Attack**
   - An assault on system security

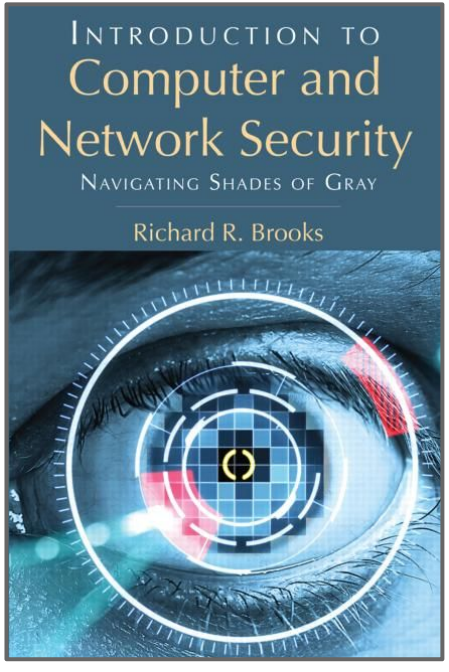
Terminology 2/2

7. **Countermeasure**
   - Actions/processes that an owner may take to minimize risk of a vulnerability.
8. **Confidentiality**
   - Ensuring assets are only available to those who should be allowed.
9. **Integrity**
   - Ensuring consistency, accuracy and trustworthiness of data..
10. **Availability**
    - Ensuring that assets are always available (e.g. in the event of an attack)..
11. **Accountability**
    - Recording actions so that users can be held accountable for their actions.
12. **Reliability**
    - Ensuring that a system can progress despite errors.

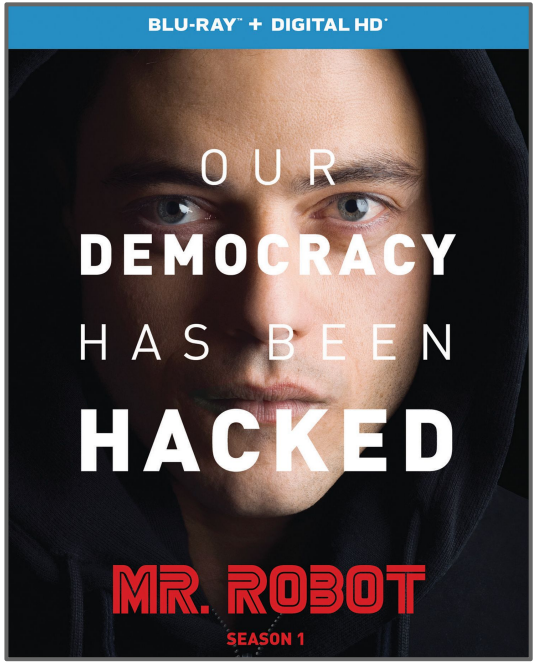
Not compulsory reading/watching



Good, recent, “mindset”



Good book, good scope



Very good TV series!