Computer Security

Introduction, history, today, and terminology

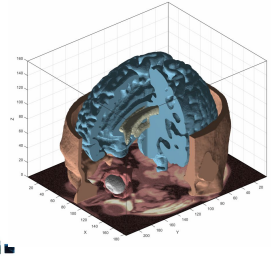
Dr Chris Willcocks

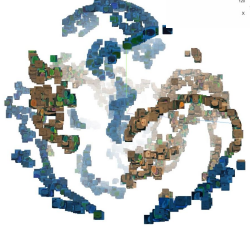
Durham University

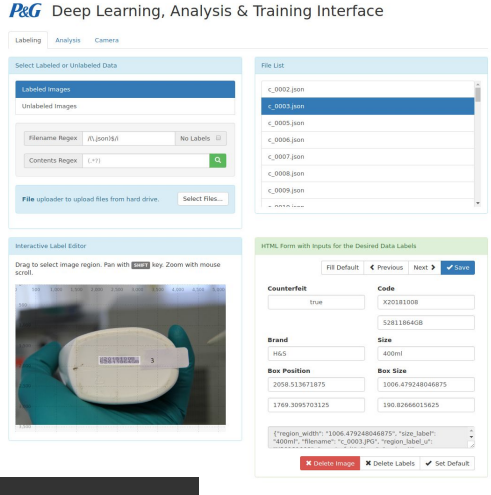
About me

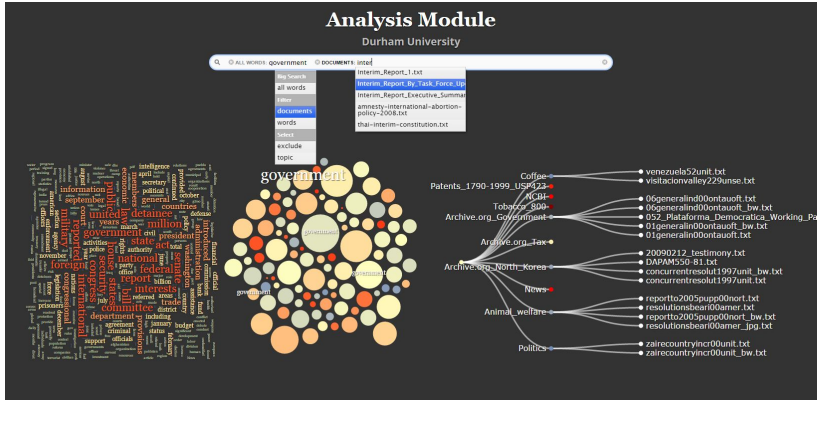
- Worked on various industry projects
- Government (defence) projects
- Medical projects with sensitive data
- Multi-user counterfeiting

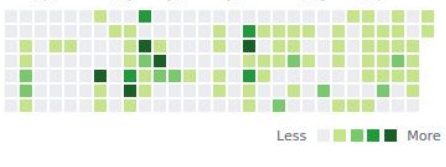
1. DSTL
2. P&G
3. Unilever
4. Dyson
5. AstraZenica











Introduction to the course

- New course with 10 lectures
- 4x 2-hour practicals
    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 assignment
    1. Given **early on** teaching week 2.
    2. Due on teaching week 9 (**3rd December**).

WARNING: Not everything you can technically do is **legal**!

Durham University

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.

What is computer security?

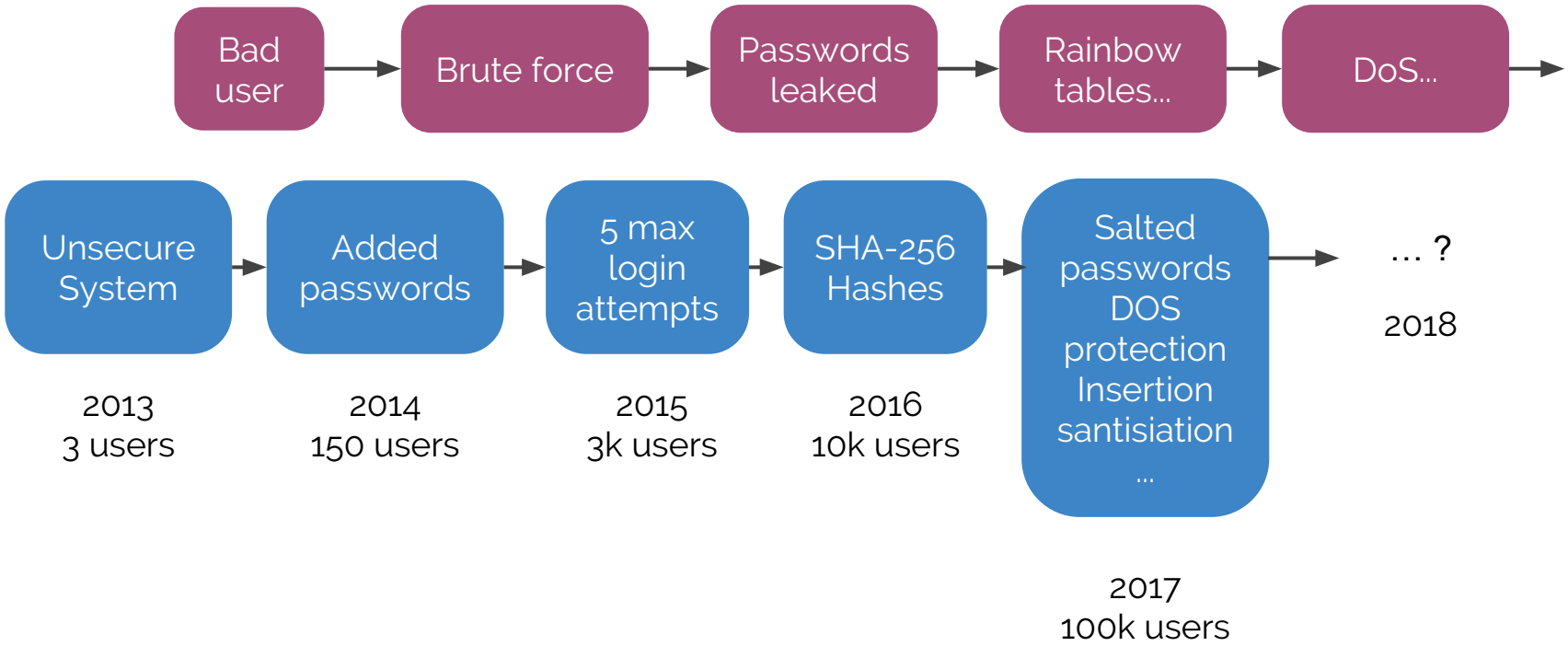
Durham University

"Computer security is the protection of computer systems against adversarial environments"

conflicting/competing/attacking

1. Allow intended use
2. Prevent unintended use

...an arms race


Bad user
Brute force
Passwords leaked
Rainbow tables...
DoS...
Unsecure System
Added passwords
5 max login attempts
SHA-256 Hashes
Salted passwords DOS protection Insertion santisiation ...
... ?
2018
2013
3 users
2014
150 users
2015
3k users
2016
10k users
2017
100k users

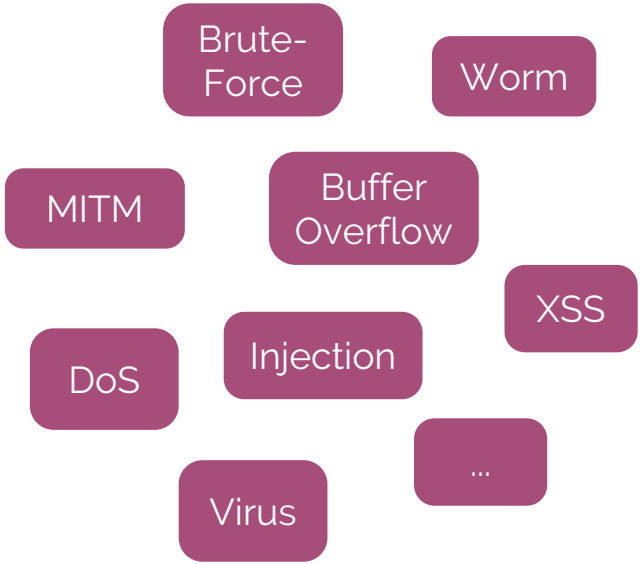
However...

Durham University

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?

Durham University

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

   ...

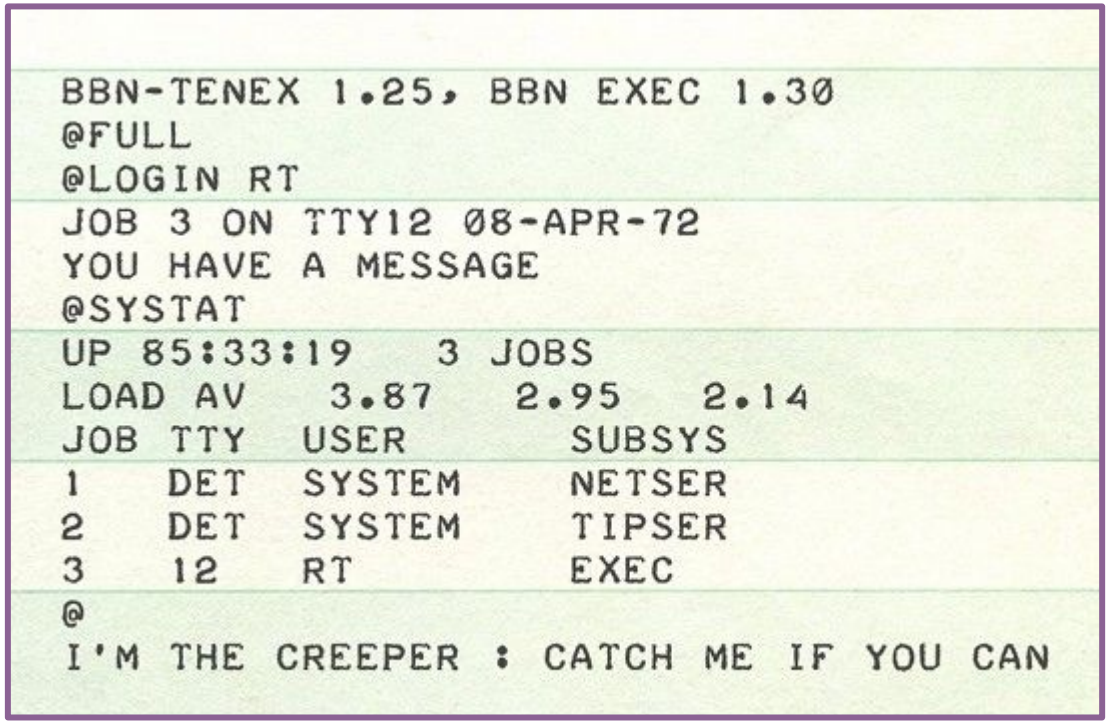
A brief history of cybersecurity

Durham University

Major historical events:

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

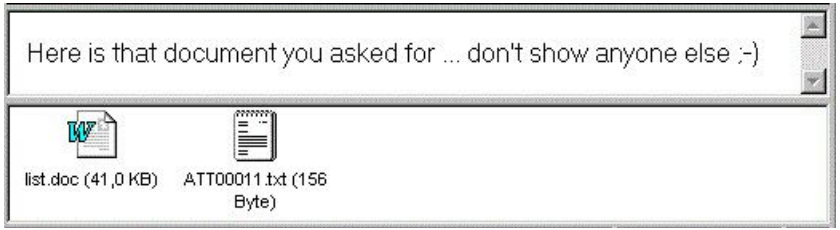
1988: The Morris worm, created by Robert Morris to assess the size of the internet. First to be convicted under misuse act. Now a professor at MIT.



Selection of historical hacks

Durham University

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 (new news since 3 October).

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 cybersecurity 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 cybersecurity centre, part of GCHQ.

Most of it is unreported

Durham University

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

2 October 2017 (last week):

1. Privilege escalation
2. Arbitrary code execution

archlinux

Home | Packages | Forums | Wiki | Bugs | Security | AUR | Download

issues advisories todo login

Issues

vulnerable all

Group	Issue	Package	Affected	Fixed	Severity	Status	Ticket	Advisory
AVG-369	CVE-2017-12133 CVE-2017-12132	lib32-glibc	2.25-7		Critical	Vulnerable		
AVG-368	CVE-2017-12133 CVE-2017-	glibc	2.25-7		Critical	Vulnerable		
AVG-417	CVE-2017-12154	linux	4.13.3-1		High	Vulnerable		
AVG-390	CVE-2017-12858	libzip	1.2.0-1		High	Vulnerable		
AVG-359	CVE-2017-11608 CVE-2017-11605 CVE-2017-11555 CVE-2017-11554	libsass	3.4.5-1		High	Vulnerable		
AVG-355	CVE-2017-13066 CVE-2017-13065 CVE-2017-13064 CVE-2017-13063 CVE-2017-12937 CVE-2017-12936 CVE-2017-12935 CVE-2017-11403	graphicsmagick	1.3.26-1		High	Vulnerable		
AVG-331	CVE-2017-9986 CVE-2017-9985 CVE-2017-9984	linux	4.11.7-1		High	Vulnerable		
AVG-328	CVE-2017-9257 CVE-2017-9256 CVE-2017-9255 CVE-2017-9254 CVE-2017-9253 CVE-2017-9223	faad2	2.7-4		High	Vulnerable	FS#54613	

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

Terminology 1/2
(not examined, lots of definitions)

Durham University

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

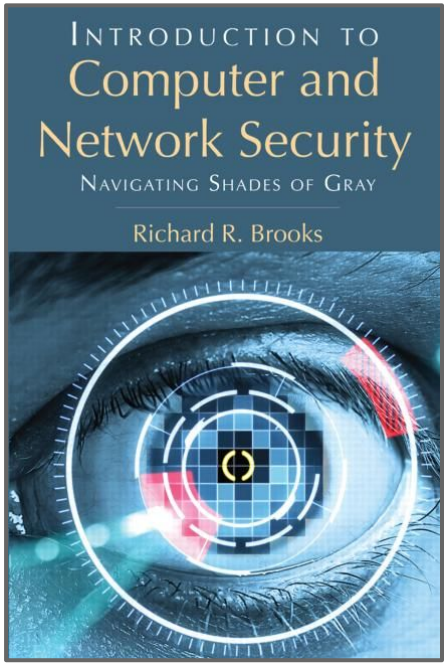
Terminology 2/2
(not examined, lots of definitions)

Durham University

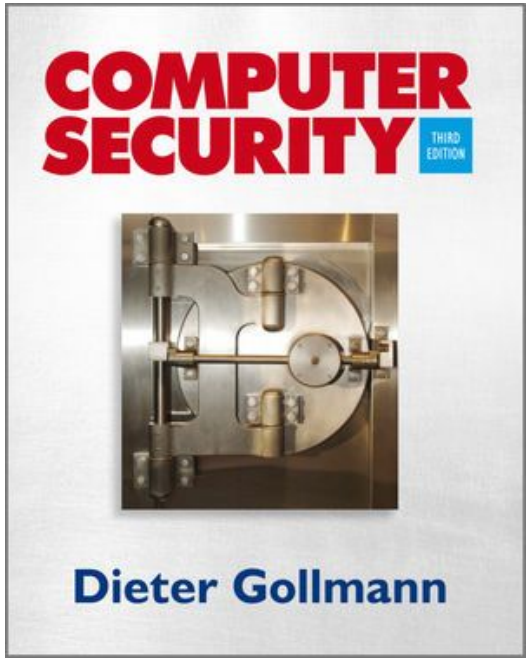
7. **Countermeasure**
   - Actions/processes that an owner may take to minimize risk of a vulnerability.
8. **Confidentiality**
   - Ensuring assets are only available to those who should be allowed.
9. **Integrity**
   - Ensuring consistency, accuracy and trustworthiness of data..
10. **Availability**
    - Ensuring that assets are only available to those who are permitted to use it.
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

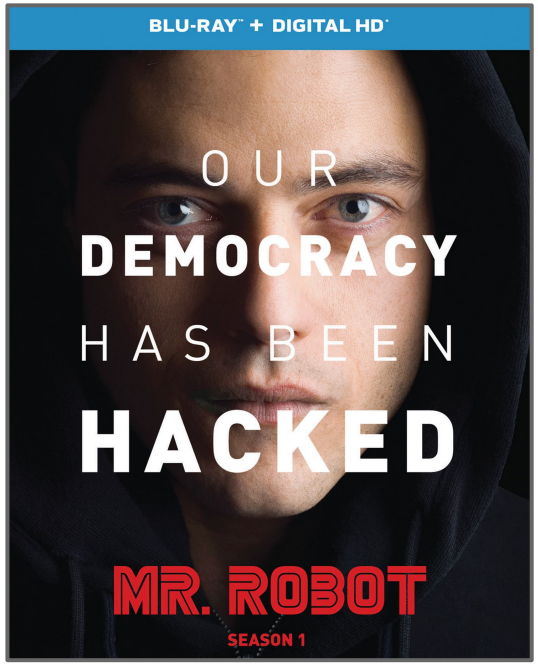
Durham University



Recommended book



More traditional, level 3-4



Very good TV series!