About me

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

1. DSTL
2. P&G
3. Unilever
4. Dyson
5. AstraZenica
Introduction to the course

- This course is not like the others
  - Cyber security is not really a science.
- 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 coursework assignment
  1. Given early on teaching week 3.
  2. Due on teaching week 9 (6th December lunchtime).
This course

- 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

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.
Getting the most of of this

- Create your own mini cyber security lab

Install VirtualBox on your PC

Your lab
Learn the tools, learn the culture...

ATTACK!

Target on LAN or further...

Kali

Arch Linux

BlackArch

Ubuntu

Windows 10
“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 sanitisation ...

2015 3 users
2016 150 users
2017 3k users
2018 10k users
2019 100k users
2020... ?
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

- Brute-Force
- Worm
- MITM
- Buffer Overflow
- XSS
- DoS
- Injection
- Virus
- ...
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

...
A brief history of cybersecurity

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


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: 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

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

1. Privilege escalation
2. Arbitrary code execution
...so much to choose from!

<table>
<thead>
<tr>
<th>Type</th>
<th>Issues</th>
<th>Local</th>
<th>Remote</th>
<th>Open</th>
<th>Fixed</th>
<th>Advisories</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiple issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>211</td>
</tr>
<tr>
<td>unknown</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>access restriction bypass</td>
<td>103</td>
<td>23</td>
<td>80</td>
<td>9</td>
<td>84</td>
<td>74</td>
</tr>
<tr>
<td>arbitrary code execution</td>
<td>676</td>
<td>654</td>
<td>16</td>
<td>36</td>
<td>640</td>
<td>118</td>
</tr>
<tr>
<td>arbitrary command execution</td>
<td>30</td>
<td>8</td>
<td>22</td>
<td>1</td>
<td>29</td>
<td>16</td>
</tr>
<tr>
<td>arbitrary file overwrite</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>arbitrary file access</td>
<td>11</td>
<td>3</td>
<td>8</td>
<td>0</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>arbitrary file upload</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>authentication bypass</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>certificate verification bypass</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>content spoofing</td>
<td>83</td>
<td>1</td>
<td>82</td>
<td>2</td>
<td>81</td>
<td>2</td>
</tr>
<tr>
<td>cross-site request forgery</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>cross-site scripting</td>
<td>61</td>
<td>2</td>
<td>59</td>
<td>2</td>
<td>59</td>
<td>8</td>
</tr>
<tr>
<td>denial of service</td>
<td>645</td>
<td>28</td>
<td>622</td>
<td>38</td>
<td>607</td>
<td>85</td>
</tr>
<tr>
<td>directory traversal</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>incorrect calculation</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>information disclosure</td>
<td>185</td>
<td>38</td>
<td>147</td>
<td>12</td>
<td>173</td>
<td>28</td>
</tr>
<tr>
<td>insufficient validation</td>
<td>34</td>
<td>5</td>
<td>29</td>
<td>1</td>
<td>33</td>
<td>6</td>
</tr>
<tr>
<td>man-in-the-middle</td>
<td>11</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>open redirect</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>private key recovery</td>
<td>12</td>
<td>5</td>
<td>7</td>
<td>0</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>privilege escalation</td>
<td>66</td>
<td>2</td>
<td>16</td>
<td>1</td>
<td>65</td>
<td>35</td>
</tr>
<tr>
<td>proxy injection</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>same-origin policy bypass</td>
<td>17</td>
<td>1</td>
<td>16</td>
<td>3</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>sandbox escape</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>session hijacking</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>signature forgery</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silent downgrade</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>sql injection</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>time alteration</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>url request injection</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>xml external entity injection</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1994</td>
<td>368</td>
<td>1626</td>
<td>106</td>
<td>1888</td>
<td>552</td>
</tr>
</tbody>
</table>
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)
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
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

Cybersecurity - Attack and Defense Strategies

Good, recent, “mindset”

Introduction to Computer and Network Security
Navigating Shades of Gray
Richard R. Brooks

Good book, good scope

Mr. Robot
Season 1

Very good TV series!