Orientation

- This course is **Secure Programming**.
- More accurately it might be called **Software Security**.
- Aimed at Informatics 4th year and MSc students.
- Primarily: those anticipating a career in software
  - **programming**: architects, developers, testers, . . .
  - **security**: pentesters, malware/reverse engineers
  - **researchers**: verification, compilers, language design, . . .
- It is taught by **David Aspinall**.
Known good practice ignored (2015)

Ostensibly, many security failures are due to software vulnerabilities. Are they inevitable?

Many surrounding questions. Can we:

▶ find vulnerabilities (before attacks)?
▶ detect exploits in-the-wild?
▶ repair vulnerabilities (routinely/automatically)?
▶ program better to avoid vulnerabilities?
▶ measure risk associated with software?
▶ design or verify to prevent them?
▶ develop new technology to help the above?

Questions beyond the technical, too. Can we:

▶ insure against cyber incidents?
▶ regulate for better security?

IoT: easily raise a DDoS botnet army (2016)

What is this course about?

Mainly: building software that’s more secure

▶ finding security flaws in existing software
▶ avoiding flaws in new software
▶ techniques, tools and understanding to do this

also infrastructure around software:

▶ language, libraries, run-time; other programs
▶ data storage, distribution, protocols and APIs
▶ development methodologies

and in the first place, policies for security

▶ what should be protected
▶ who/what is trusted
▶ risk assessment: cost of defences.

Target audience

▶ Aimed at 4th/5th year UGs, MSc
▶ Have passed Computer Security or similar
  ▶ Basic notions, crypto, protocols
▶ Programming practice
  ▶ should be confident in programming
  ▶ necessarily will use a range of languages
  ▶ … including some C and assembler
  ▶ but don’t have be “master hacker”
▶ Programming theory
  ▶ interest in PL concepts and design
  ▶ knowledge of compilers useful
  ▶ also software engineering, esp. testing
  ▶ theory courses helpful, semantics

Why should you take this course?

Want to work in the cyber security industry?

▶ security appraisal, system and code reviewing
▶ pen-testing, ethical hacking
▶ malware analysis, reverse engineering
▶ operations and response (SOCs)
▶ innovation: start-ups, spin-outs
▶ cyber defence, attack, espionage
▶ Want to work in security research?
▶ academic (conceptual advances, fixing, breaking)
▶ commercial (breaking, fixing, defending)

(Hopefully): you think it’s fun and interesting!
Why should you not take this course?

▶ None of the previous points apply.
▶ You don’t have the right background (see next slide)

Or perhaps, you don’t want to risk a relatively new course. This course is still “bedding in”. Frank and constructive feedback is very welcome.

Learning outcomes

Here is the list from the Course Catalogue Entry:

1. Know how to respond to security alerts (concerning software)
2. Identify possible security programming errors when conducting code reviews in languages such as Java, C or Python
3. Define a methodology for security testing and use appropriate tools in its implementation
4. Apply new security-enhanced programming models and tools which help ensure security goals, e.g., with access control, information flow tracking, protocol implementation, or atomicity enforcement.

Safety versus security

Safety is concerned with ensuring bad things don’t happen accidentally. For example, aeroplanes don’t fall out of the sky because maintenance checks are forgotten.

Security is concerned with with ensuring that bad things don’t happen because of malicious actions by others. For example, terrorists cannot drive bombs into airport departure halls.

The distinction is sometimes blurred, and the two interact in intriguing ways. (Q. why?)

The challenge of software security

Software artefacts are among the most complex built.

▶ Design flaws are likely
▶ Bugs seem inevitable

Flaws and bugs lead to vulnerabilities which are exploited by attackers.

Often to learn secrets, obtain money. But many other reasons: a security risk assessment for a system should consider different attackers and their motives.

Cost estimates are difficult

But it’s agreed they’re increasing…

THE COST OF CYBER CRIME.

A DETICA REPORT IN PARTNERSHIP WITH THE OFFICE OF CYBER SECURITY AND INFORMATION ASSURANCE IN THE CABINET OFFICE.
Cyber warfare is real

Privacy is being eroded

Why isn't software security better?

Why (else) isn't software security better?

What's the outlook?

Delivery and assessment
Lab sessions

Three 3hrs lab sessions.
Scheduled TBC.

▶ Week 4
▶ Week 6
▶ Week 8

Each session will examine some software vulnerabilities: why they exist, how they can be discovered, exploited, and repaired.

Labs may start with a short guided introduction.

Working together is encouraged. We want to foster a supportive learning environment. Students who have prior knowledge or expertise are especially welcome.

Formative feedback during Labs

One reason to introduce labs in this course is to allow us to give face-to-face formative feedback on your learning.

We will do this by reviewing the results from one lab session at the next lab session. To do this effectively we will ask that you submit your work and/or discuss it with us during the lab sessions.

Lab sessions will be run by me together with the course TAs, who are Joseph Hallett and Arthur Chan.

Coursework

The coursework will be an assignment following a similar pattern to the lab exercises: discover, exploit then repair.

1. as usual: your work should be your own
2. no publication, please do not publish solutions even after the deadline

(at least two reasons for last point).

The coursework deadline is scheduled for Week 8.

An ethical point (reminder)

Nothing in this course is intended as incitement to crack into running systems!

▶ Breaking into systems to “demonstrate” security problems at best causes a headache to overworked sysadmins, at worst compromises systems for many users and could lead to prosecution
▶ If you spot a security hole in a running system, don’t exploit it, instead contact the relevant administrators or developers confidentially.
▶ To experiment with security holes, play with your own machine, or better, your own private network of machines.

Communications

New, evolving course:
▶ honest, constructive feedback is very welcome
▶ As with any course, I welcome
  ▶ questions after lectures
  ▶ questions by email

Shall we have a course-wide online facility? Open to class opinion:

1. University forum (private in UoE)
2. University VLE tool (Learn)
3. Piazza for questions, discussion (signup)
4. None, but FAQs sent to class list sp-students by email

Piazza is ready to use.

Exam

Will follow the common format:
▶ Choose 2 questions to answer from 3
▶ Two hours allowed

Towards the end of the course I will provide:
▶ a list of topics and concepts that may be examined
▶ a hint about the format of the questions

There is some guidance on the web along with a sample question.
### Dimensions: practice and theory

**Practice**
- Programming securely, identifying security issues
- Mistakes in language, APIs, crypto, comms...
- Ultimately: *detailed, highly specific* knowledge

**Theory**
- Understand reasons for failure, ways to mitigate
- Understand advanced techniques, automated tools
- In general: *transferable* concepts and methods.

This is not really a “vocational” course. I hope it will give you the foundation to allow you to *rapidly develop* detailed specific knowledge needed later. There are a number of certification schemes for building practical knowledge.

### Overview of topics

General organisation:
1. **Threats**
2. **Vulnerabilities**
3. **Defences**
4. **Processes**
5. **Emerging Methods**

We’ll look at details under each of these headings (in various orders).

### 1. Threats
- What attackers want, can do
- Types of bad code: malware, spyware, PUPs
- How bad code gets in
- Classification of vulnerabilities and weaknesses, CVE/CWEs

### 2. Vulnerabilities
- Overflows
- Injections
- Race conditions
- Information leaks

### 3. Defences
- Protection mechanisms
- Avoidance by secure coding
- Trade-offs in adding protection mechanisms

### 4. Processes
- Secure design principles
- Testing and reviewing to find vulnerabilities
- Assessing/measuring security of code
5. Emerging methods

- Methods and tools to find problems
- Detecting buggy patterns automatically
- Building security in, methodology and technology

Review questions

**Safety versus Security**
- Explain the difference between these two, and why ensuring security may be harder.

**Security flaws and their impact on society.**
- Explain some recent secure programming flaws that made the news and explain what the underlying problems were.
- Discuss the fundamental reasons that software security fails and the wider questions around cyber security.

References and reading

The slides contain links which you can click on to find referenced or connected material.

References and reading will also be given for each lecture in a separate web page for that lecture. For this lecture, see here.

There is no single recommended course textbook, although a few books will be mentioned. See the page above for pointers.