

COMP9447 15s2

Lecture 1A – META INFO

Course Schedule

This is a rough plan only – real life may affect this – any changes will be reflected on OpenLearning

WHAT	WHEN	WHENNNNNN
WEEK 1 LECTURE	28-Jul	6pm-9pm
WEEK 2 LECTURE	4-Aug	6pm-9pm
WEEK 3 LECTURE	11-Aug	6pm-9pm
WEEK 4 LECTURE	18-Aug	6pm-9pm
Written submission including group enrolment and software selection for assignments	24-Aug	9am
WEEK 5 LECTURE	25-Aug	6pm-9pm
WEEK 6 LECTURE	1-Sep	6pm-9pm
WEEK 7 LECTURE	8-Sep	6pm-9pm
PRESENTATION SLIDES ARE DUE	14-Sep	9am
WEEK 8 - PRESENTATIONS	15-Sep	6pm-9pm
WEEK 9 - PRESENTATIONS	22-Sep	6pm-9pm
WRITTEN ASSIGNMENTS ARE DUE	10-Nov	9am
EXAM	LATE IN EXAM PERIOD (TBC)	

Richard Buckland

Richard Buckland is the chief of the course

Working out how to contact him is a part of the UNSW CSE experience.



People who run 9447 + Asking for help

OpenLearning usage is mandatory for this course, and your first point of contact with questions should be the forum etc.

comp9447@gmail.com Checked by all of us - Use this one unless private

Brendan.hopper@gmail.com (That's me – I design the structure and do most of the talking)

thouth@gmail.com (Fionnbharr Davies, pictured below – writes a lot of the course content and can help in lots of ways – has slightly more time than I do)

Evgeny Martynov + John Cramb are helping out too and will be writing wargames and giving lectures. I need permission to put their email addresses up.


There is a significant expectation of 'self-learning' for a lot of this stuff. The recommended textbooks and reading will help, but you will need to tinker and learn on your own or in private groups. I will not personally have a lot of time to help you, but the other guys may. – Treat all of our time as precious.






How this course is marked

A final exam for 50%

- Will be late in the exam period
 - Open book (i.e. you have Internet access and are allowed to Google)
 - Entirely practical and applied – minimal theory
 - Modelled after the war-games, homework and lectures
- 

A major assignment for 50%

- Perform a real world security assessment on a piece of software (or multiple related pieces)
 - Attempt to find real vulnerabilities and write exploits
 - Presentation due in Week 9 as a “halfway” status update
 - Results due at end of semester
- 

**Non-Mandatory Bonus Assignments
(up to an extra 10% in total)**

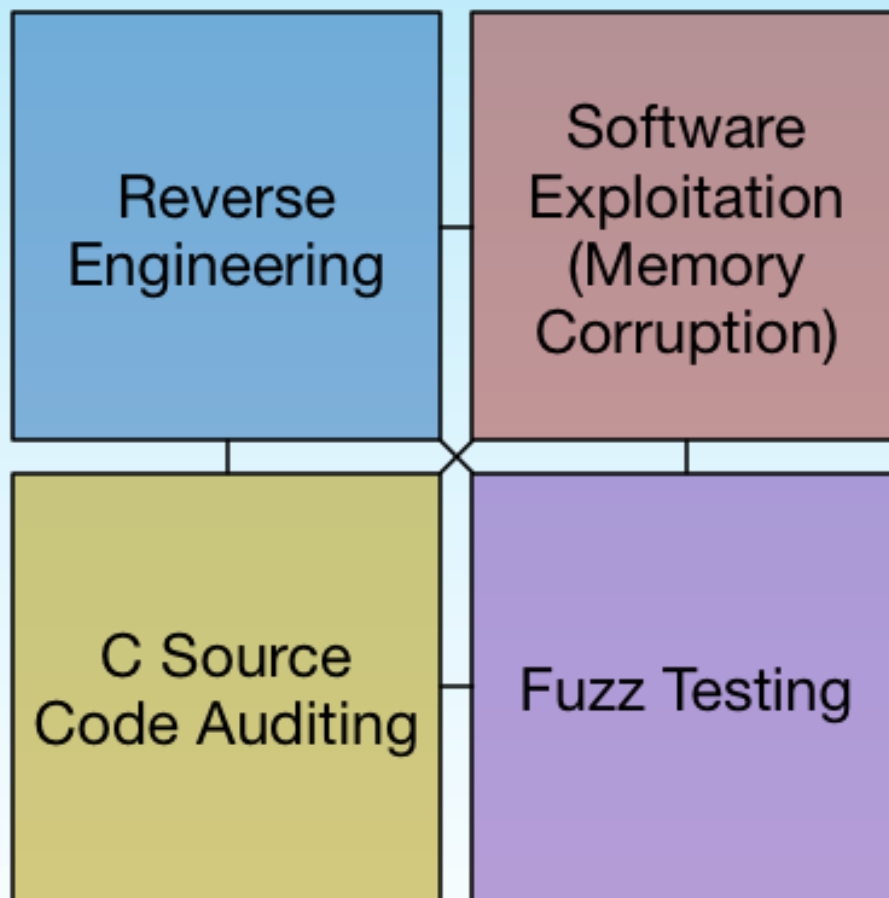




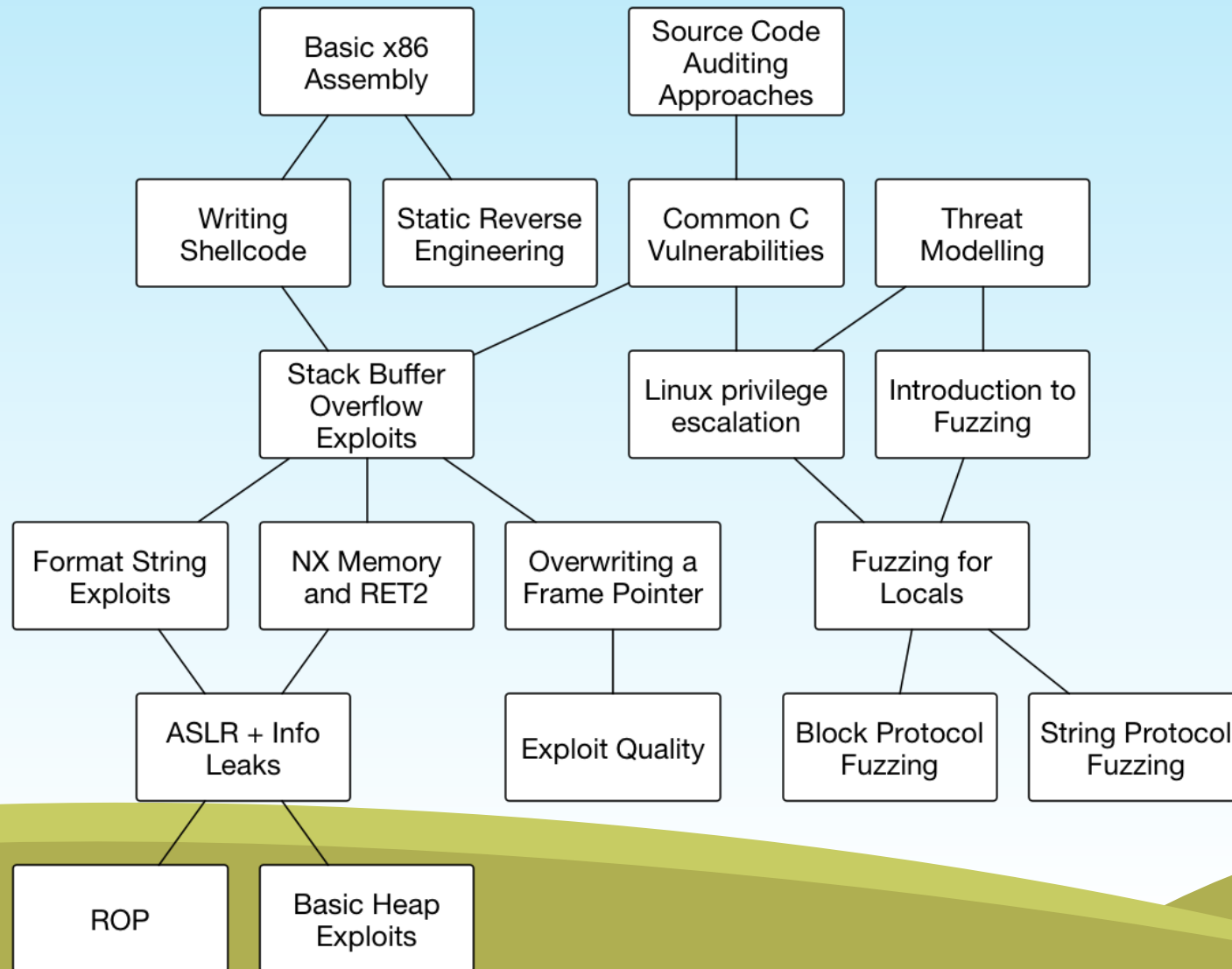
Major Assignment

- Everyone works in a group of 3 (postgrads with a really good reason to work solo, email comp9447@gmail.com)
- Pick a piece of software (i.e. OpenSSH – but this is probably too secure) or a bunch of pieces of software that share a protocol (i.e. 5 different DHCP servers) – do an assessment including fuzzing, source code/reverse engineering review, and try to find real vulnerabilities to write real exploits. **Each team needs to submit 3 preferences (1st, 2nd, 3rd).**
- If you pick closed source, you will need to reverse engineer, obviously. Might be good if you are interested in that, though.
- A presentation will be done by each team mid-way through the semester, and a short written report should be presented on your approach, success, learnings, etc. More advice on report as we get nearer to the end of semester.
- If you find bugs and get working exploits, great. If not, if you can show you did a solid job doing the security assessment, that's good too. (It's probably easier to find 10 linux kernel vulns than it is to find a single Apache vuln)

What you will learn



A bit more detail – I hope we can include all this



Recommended Pre-requisites (Catch up soon!)

- C
- GDB debugger (go do some tutorials)
- Recommended but not essential: A quick to write language, either python or ruby, generally. If you need to pick one to learn now, python – much greater use by low-level security community (ruby seems to be favoured by the webapp guys). If you are already good at ruby, and don't know python, use that
- X86 Assembly (we teach this, but previous knowledge helps)

What you will not learn (and may have been expecting)

- Formal methods / automated static analysis (Nope. I think some of this may be in COMP4141 but I don't honestly know)
- Web Application Security (We will be making a new dedicated course)
- Cryptography (Go to COMP3441/COMP9441)

Will this class be available recorded/video?

Maybe! But only bits of it. Don't depend on this. If you have a lecture conflict, and the other class has video, come to this one, definitely.

Will slides be available?

Some of them! All of the ones that are actually examinable. The one today about history will not, and neither will a couple of future 'bonus talks'.



ETHICS, THE LAW, AND MORAL CONDUCT

Ethics:

1. relating to moral principles or the branch of knowledge dealing with these.
3. avoiding activities or organizations that do harm to people or the environment.

Law:

1. the system of rules which a particular country or community recognizes as regulating the actions of its members and which it may enforce by the imposition of penalties.

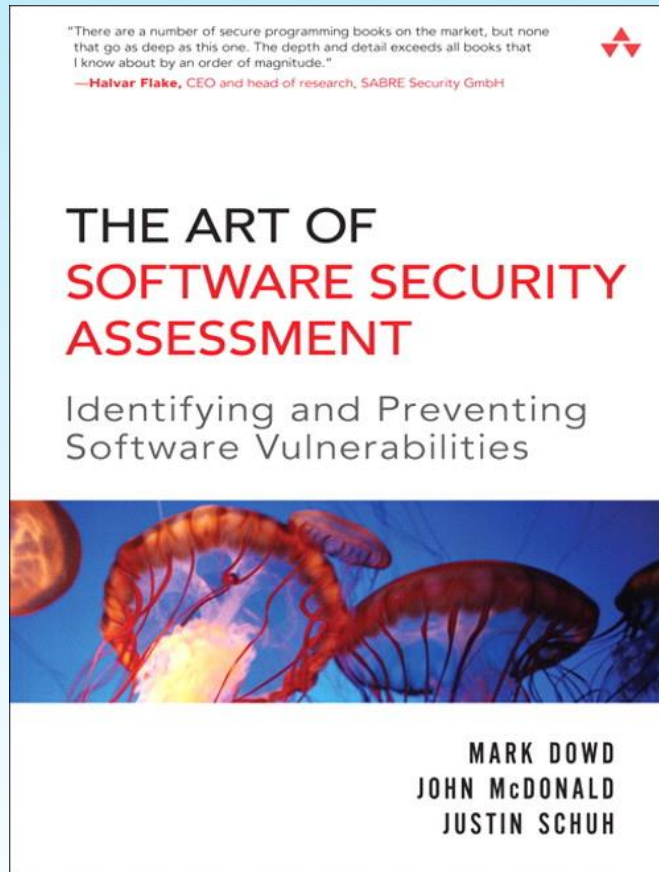
DO NOT 'HACK' INTO UNSW, CSE, OR ANYTHING ELSE WITHOUT PERMISSION! (Even if I do..)
You will get expelled! And you may seriously go to jail. Not a joke. STAY WITHIN THE BOUNDS OF THE LAW.

DO NOT ASSUME THAT YOUR ACTIONS WILL BE UNDETECTED, OR THAT WHAT YOU ARE DOING IS OKAY OR SAFE.

DO NOT ASSUME THAT "GOOD INTENTIONS" WILL HELP AT ALL.

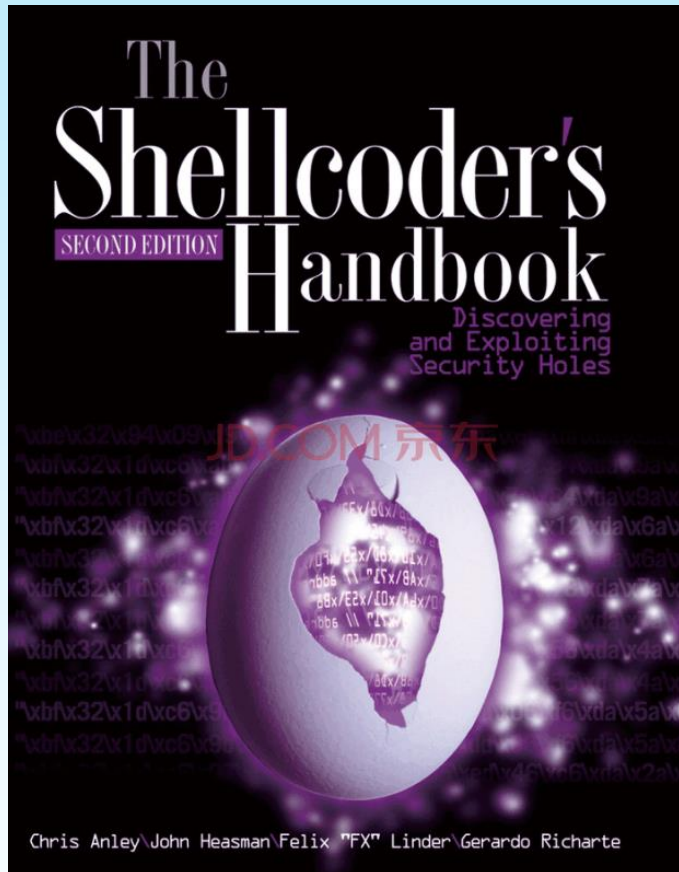


Text Books – Not mandatory but useful



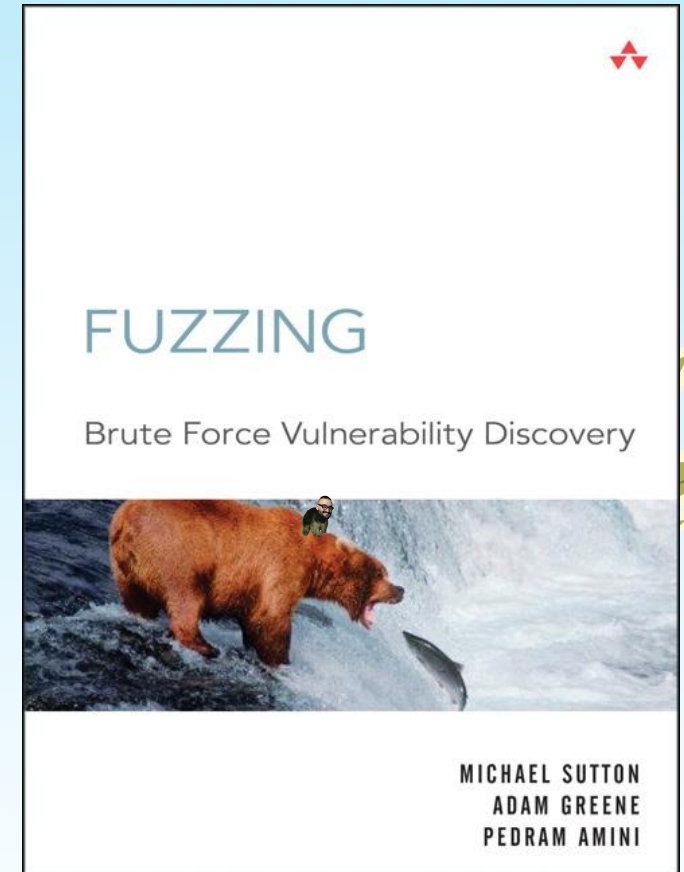
General Theory,
Vulns, Source Review

Highly Recommended



Exploit focused,
applied and meaty.

Recommended



Fuzzing focused

Up to you, recommended if
you struggle with fuzzing

Questions?

