COMP6441 and COMP6841
SECURITY ENGINEERING AND CYBERSECURITY
COURSE INFORMATION Term 1 2020

Cybercrime, Cyberwar, ...
Security Engineering - T... ce of designing and securing complex systems

Welcome to UNSW Sec... 6441/6841)
In this introductory cyb... k at Security Engineering – the engineering principles behind designing and maintaining security. We will delve into selected case studies and examine the principles behind effective security. We cover theory and then we look at how it is applied in current cyber security practice. We will pay particular attention to systems which fail. This course involves analysis, critical thinking and design. A cunning and devious mind will be an asset. Although our main concern is cybersecurity, the engineering principles we cover apply to security more generally.

OVERVIEW

This course introduces modern cybersecurity design and practice, and is suitable for anyone with a playful analytical mind and a general interest in security. We concentrate on **analytical skills** and an **engineering approach to security design**. We'll also bring you up to date with the current main trends in cybersecurity.

Core Course (6441)
The core course is open to everyone. Many of the topics do not require any specific technical or computing background. There will be times where we delve into things that require an understanding of particular computational mechanisms (such as programming language implementation, or database queries) that are being attacked. We will give some background on the mechanisms in these cases, or enough keywords that you can look it up yourself, but a student without a computer science background should expect to have to invest a bit of extra time to obtain a full understanding of the topic.

Extended Course (6841)
The extended course is for students who can code, ideally in C, and who know low level concepts such as memory implementation and function calling. In this course we expect you to undertake a technical security project. The extended course is the core course plus extra technical material.

After completing one of these courses you can proceed to the other UNSW Computing Security Courses covering topics in:

- Digital forensics
- Penetration testing
- Memory corruption and exploitation
- Software assurance
- Incident response
- Malware analysis and reversing
- Cryptanalysis
- Professional issues and leadership in security
- Web application security
- Special projects
- Masterclass

The precise topics covered in this introduction course are likely to change somewhat from year to year to keep the coverage up-to-date and relevant. As you will see cybersecurity has recently been and remains a rapidly changing field. The field is now way too big for us to cover everything in one course but by the end of this

course you will have an overview of the major topics in contemporary security, a good understanding of the current state of play, and have begun to think like a security engineer.

Our intention is to make course. The field is a great deal of fun with puzzles, cunning, cloak-and-dagger antics ply of great stories. However it will not be an easy course – you are expected to master nd* to be able to apply it to real world situations. There is a lot to learn and we exp study it in your own time.

AIM OF THE COURSE

There are 4 desired objectives of this course:

1. Think like a security engineer
2. Cybersecurity literacy
3. Crypto literacy
4. Security engineering professional skills

At the end of this course you should:

- Be able to **think like a Security Engineer**
  - critically analyse scenarios
  - design effective secure systems
  - make appropriate security decisions
  - at an organisational level be able to identify and ensure an appropriate level of security
  - analyse and assess risk, gather appropriate data, and make appropriate decisions in an uncertain environment
  - use new skills to
    - effectively communicate,
    - bring about change, and
    - lead others

- Have an **understanding of fundamental applied cyber security concepts** including
  - vulnerabilities, buffer overflow, heap attacks, return oriented programming, web attacks
  - exploits, privilege escalation
  - reverse engineering
  - rootkits and malware
  - social engineering
  - honeypots, firewalls, intrusion detection systems, logging
  - denial of service attacks
  - static code analysis
  - fuzzing
  - assurance and audit
  - red teams, penetration testing
  - incidence detection and response
  - network forensics, computer forensics

- Have an **understanding of fundamental cryptographic concepts** including
  - cryptographic primitives: cyphers, hashes, random number generators, steganography, modes, key generation
  - attacks on primitives: cryptanalysis, collisions
  - information theory and entropy
  - side channels
  - protocols: analysis, protocol failure, protocol design
  - fundamental properties: confidentiality, integrity, authentication, repudiation, privacy, zero knowledge
  - key distribution
  - authentication: shared secrets, biometrics

- Have the **professional skills** you need to be a successful security professional
    - be a li ty
        - analyse new developments in cyber security
        - importance and implications of emerging technologies, trends,
        - g and own process of learning
    - be eff
        - ment
        - and spoken communication
        - Work effectively in a team
        - Critically review the work of others and give effective feedback

TEACHING STYLE AND HOW TO APPROACH THE COURSE

In this course you are expected to engage in self-directed learning. The core content will be introduced in lectures but it will be up to you to arrange your study to that you further research, practice, and master the material. You will be able to specialise in the areas in which you are most interested but you are expected to have a basic literacy and understanding of all the topics covered.

This is not a course where you can do little work throughout session and then cram for the final exam. You will need to be active in your learning each week.

There is weekly homework consisting of readings to prepare for tutorials that involves researching and writing regular analytic reports, and practical homework exercises.

Topics are introduced in lectures. You will need to do further work after the lecture to master the topics.

In addition to the face to face course hours each week you should engage in personal research, practice, and engage with the course community on the course website – both helping and being helped and sharing ideas and practicing on course activities. As a university student we expect you to spend about 15 hours per week the course for a credit level grade.

We don't know of any textbook which covers the bulk content of the course adequately. So you should ensure you attend the lectures or have friends who will attend and tell you what we covered. Richard's lecture slides are generally just bullet points so you will need to make notes for your learning. There is a collaborative course textbook to which you are expected to contribute and which will be made available to you in the final exam.

In the face to face lectures guest speakers and Richard may speak frankly about events and case studies which shouldn't be made public. For that reason please do not record any of the lectures. If you need a lecture recording for some special reason (e.g. medical condition) please make arrangements with Richard in advance.

There will be plenty of opportunities for you to self-assess your progress in the course. If you are unsure about how you are progressing or are unsure about what you should be doing please don't be shy, just ask. It would not be good to wait until the end of the course before finding that you are falling behind or are not studying effectively.

COURSE RULES AND TIPS FOR SUCCESS

Be excellent to each other.

Have fun! Security is a extremely enjoyable and stimulating field. Approach it in a spirit of adventure and a desire to embrace challenge.

Acknowledge the contributions of others when you submit work which is not whole your own work. The assessable activities in the course (Job-Applications, weekly exercises, and Final exam) are to be your own work but most other ac e or with others as you find most helpful and enjoyable. Don't do everything alone ho emonstrate your ability to work in teams as part of your Job Application.

Work steadily each wee at can be stressful and tends to lead to surface rather than deep learning when you to catch up. Past students suggest putting aside a regular scheduled time each we e.

Join in the course community, share ideas and insights, and help others.

Make sure you prepare before each weekly analysis class. The quality of the discussion and analysis depends on the quality of the preparation everyone in the put in. Freeloaders let everyone down and miss out on the opportunity to practice for the exam (the final exam is closely modelled on the weekly analysis sessions and the weekly homework.)

Read around and actively extend yourself during the course. If you already know some topics then set yourself challenges or learn about extension areas. Make sure you come out of this course substantially better than when you came in.

ASSUMED KNOWLEDGE

You don't need to be able to program to take the core course but should have some basic understanding of computing. You should be able to program in C to take the extended course. Some of the topics in both courses will use programming concepts such as stack frames. In a few cases we refer to basic concepts from probability theory. Some of the topics involve working with cryptographic protocols require a little knowledge of algebra and modular arithmetic. A course in Discrete Maths is sufficient background for these mathematical topics.

In general, less background is ok PROVIDED THAT you are keen and prepared to teach yourself the things that you lack. Talk to your tutor if you have any questions about this.

Doing COMP3331/9331 (networks) and COMP3231/9201 (operating systems) in advance may well help you with a number of the topics in this subject so do them if you can. We haven't made them compulsory prerequisites however as we will only use a small amount of material from them.

TEXT AND REFERENCES

Although there is no textbook for the course a reasonable general introduction is provided in

- *Security Engineering*, Ross Anderson, Wiley, 2nd Ed. 2008, which is also less technical, but provides extensive discussion of how to think like a security engineer and many excellent war stories and case studies. It also brings to bear ideas from social science disciplines such as psychology and economics that are emerging as important new approaches to understanding security engineering at the systems scale.
- *Applied Cryptography*, Bruce Schneier, John Wiley, 2nd Ed. 1996, which is a wonderful compendium of all things cryptographic with some coverage of many of the topics we treat.

- *Computer Security: Principles and Practice*, W. Stallings and L. Brown, Pearson International, 2nd Edition, 2011, which is a book lots of other courses use.

A number of security books are available in the UNSW Library. If you find texts which we should ask the library to acquire let us know and we will make a request.

SUBMITTED WORK

This is an open course a student submitted material for others to see and learn from. **In this course submitting e university a perpetual royalty free license to use the submitted material in a** cludes but is not limited to comments, assignments, questions, messages, u wiki text and activity submissions. If submission sharing might impact on your learning cuss this with us *before* you submit.

GOOD FAITH POLICY

This course has a "Good Faith Policy". This means we expect you to act in good faith at all times. You must not act in any way so as to bring disrepute to the reputation of the course, the course staff, fellow students, the school, the university, or the ICT profession. We expect you to be a good citizen. To not invade, alter or damage the property of others including the university, invade the privacy of others, break any laws or regulations, annoy other people, deprive others of access to resources, breach or weaken the security of any system, or do or omit to do anything else which you know or suspect we would not be happy about. Furthermore, you are not to do anything which appears OK but a loophole or a strict interpretation of "the letter of the law" but which is not consistent with the spirit. Also, don't be a dick.

If you are unsure, ask!

If, in our sole discretion, we feel you have violated the Good Faith Policy you will be awarded 0 Fail for the course. Further penalties may apply also depending on the nature and severity of the violation. Students who have seriously violated the Good Faith Policy may not be permitted to re-enrol in future offerings of the course.

Students who are found (or who have previously been found and have not disclosed this) guilty of academic or computer related misconduct or any other activity in a way which casts doubt on their ability or willingness to comply with the Good Faith Policy will be disenrolled and will be not permitted to re-enrol in future offerings of the course. If you have ever been found guilty of such an activity you must disclose it to the lecturer in writing immediately.

KEEPING INFORMED

Subscribe to the course page on OpenLearning to be informed when people comment on it. Richard makes regular comments and announcements. You can see what (if anything) has changed by clicking on the "history" button.

Important notices related to this course may be announced on the home page on the course web site from time to time. It is your responsibility to check this site regularly. You can configure email alerts when announcements are posted.

Sometimes urgent information may also be sent to you by email. Make sure you pay careful attention to any email you receive. All official email will be sent to your UNSW email address. If you prefer to read your mail at some other address you will need to redirect your mail, for example by using idm. Ask your tutor if you need help doing this.

Additional information will be provided in the course discussion forums and elsewhere on the course site as the session progresses. You should explore the course web site, and read the announcements, tagged comments, FAQ, and this page regularly for updates.

ASK FOR HELP

if you need help at any mment section at the foot of the relevant page. And if you see someone asking a quest - please do! This course works best when we form a collaborative communit

COURSE STRUCTURE

Assessment

- Final Exam 40%
- Job Application (Portfolio) 40%
- Weekly Activities 20%
- Bonus marks (yes Virginia, there are bonus marks possible)

Final exam will be held in the exam period, a mix of theory and practical questions. A past exam is available in week 2 for you to look over. You get a copy of the class textbook during the exam.

Job Application – due in week 8 or 9 – a summary of your work over the whole semester – your tutor will let you know about it in your first tutorial. Includes Something Awesome project.

Something Awesome – a self-directed project you get to select the topic and then deliver in week 8 or 9 by presentation to your tutorial class. Discussed and explained in your week 1 tutorial. Topics and marking criteria must be proposed by you and accepted by your tutor. Former students strongly suggest you have this approved in week 1 so you can get immediately underway before term gets busy. Must be approved no later than week 2.

Weekly Activities – weekly activities on OpenLearning. Do in your own time. Your proportion completed is your mark. Gotta Catch-em-all. Extended students must also do the extended activities. These are optional for core students (but we strongly suggest you try to do a few of them and stretch yourself).

Bonus marks – one bonus mark (two in extreme cases), for each time you get something into the hall of fame. Tutors make the recommendation, and Lachlan and Richard post in the hall anything which is super impressive. Includes great lightning presentations, getting a CVE of your own, impressive twitter analysis post, basically anything which really impresses. Judges' decision final.

WHAT TO DO EACH WEEK

Spend 15 hours per week - (credit level amount of work). We won't chase you up - you can slack around and do none - but don't waste the opportunity to develop, stretch yourself, and become awesome.

What to do:

Blog

Blog at least 3 security observations and analysis each week and follow and comment on the blogs of each other. Can relate to current affairs or random interesting things you find about. Needs to relate to what we have learned. Most good posts are analytical (i.e. not descriptive) – ask your tutor if the difference is unclear to you. Set up your blog on OpenLearning in week 1. Tutor will show you how if you have troubles.

Twitter

Set up a twitter account (fine to use fake identity if you wish) and post one security relevant tweet per week. Your future employers and professional peers are watching so take it seriously. Follow each other and interesting security professionals.

Portfolio

Create on OpenLearning. Five sections all equally weighted. More info in week 1 tutorial.

1. Community an
2. Time Managen
3. Analysis
4. Technical Skills
5. Something Aw

Case Studies

We suggest 1-2 hours per week for reading preparation and self-directed case study research before the class, and about 30 minutes for reflection and write up when you get home from your class.

Lightning talks

If you find something interesting – share and teach your tutorial class in a lightning talk (and be eligible for the hall of fame), plus gather great evidence for your portfolio. Arrange with your tutor in advance. Talks go for 3 mins max at the start of the tutorial class. Everyone should aim to do at least one over the term.

Security Everywhere

Find anything in the real world which related to the topics and concepts we have studied. Post a picture or brief summary on **Security Everywhere** OpenLearning page. Extra impressive if it makes the class laugh or think. Expect everyone to post one per week and comment on two posted by others.

Security Theatre

If you want some cinema on a Wednesday night - immediately after the class we watch a security related film together. Optional and fun. We spend a few mins at the end analysing the security implications. You will see some classic, excellent films - come along! Life isn't just study...