ELEC5616 COMPUTER & NETWORK SECURITY

Lecture 0:

Class Mechanics

COURSE GOALS

- Understanding security fundamentals
- Introduction to applied cryptography
- Issues with designing secure systems
- Experience designing and implementing one
- Examining real world cryptosystems
- Understanding cross-disciplinary issues
- Why things break... *all the time*

ABOUT ME

Luke Anderson – Lecturer & Tutor

- Security Lecturer at USYD & UTS
- PhD Candidate – researching blockchain technology
- Previously:
  - Security Engineer @ Freelancer.com
  - Tech Lead @ Hagglr

B.I.T. (Hons) / B.Sc. (adv.) @ Sydney University
Double Degree in Computer Science + Physics

SYLLABUS

Hash functions

Authentication

Secret key (symmetric) and public key (asymmetric) encryption

Key exchange

Digital signatures

Cryptographic protocols

Software security

Network & web security

Real world systems and protocols

Attacks

Political and legal issues

How and why systems fail

The shape of things to come

COURSE MECHANICS

Two 1 hr. lectures per week, for twelve weeks

Friday 3pm to 5pm (PNR LT 1 - Farrell)

One two-hour lab working on projects

Tuesday 12pm to 2pm (EE Room 265)

OR

Friday 12pm to 2pm (EE Room 265)

COURSE ASSESSMENT

- **Assignments & Wargames (25%)**
  - Wargames (12.5%)
  - Assignment (exam preparation) (10%)
  - Weekly Quiz Participation (2.5%)

- **Project (25%)**
  - Part 1 – Securing a Botnet (9 %)
  - Part 2 – Securing a Botnet (9 %)
  - Part 3 – Software Security (7 %)

- **Final Exam (50%)**
  - Two hours, closed book
  - Must get at least 40%

EXPECTATIONS

- **All lectures are compulsory**
- **All labs are compulsory**
- **Attendance below 50% is grounds for failure**
- **It is your responsibility to make up for missed classes**
- **Late penalties will be 10% per day, rounded to a whole day, including weekends.**

No complaints if you can’t program

Programming is fundamental for this course
and your future career.

It is 2016.

If you can’t program by the time you leave
university you will be **road kill**
in the real world.

TEXTBOOK & RESOURCES

Handbook of Applied Cryptography
(available for free on our website)

Security Engineering
(available for free on our website)

Lecture notes and additional reading material will be available on our website

Papers will be handed out weekly that reinforce the material and **may be referenced in the quiz or exam**. They are also very interesting to read!

PROJECT :: DEFEATING SKYNET

It's 2016. Almost every device has a CPU in it and is connected to the Internet. Whilst this is a stunning advance for humanity, the security for these devices has come as an afterthought or not at all. Millions of computers and devices, all with valuable information and processing power, are left vulnerable to attack.

Blackhats, and even possibly **governments**, have created **viruses**, **worms** and other **dastardly schemes** to **mine for information** and **turn a profit** using these **weaknesses**.

PROJECT :: DEFEATING SKYNET

In this project, we'll be specifically looking at why they're valuable and why it's so difficult to defeat them

Botnets perform various tasks including but not limited to:

- Stealing confidential information (passwords, banking details, etc.)
- Sending spam email
- Distributed Denial of Service (DDoS) against chosen websites
- Mining for CryptoCurrency
- Providing a secure proxy network for other illegal enterprise

You are to work in teams of 2-3 in the labs.

This project will run all semester long and be in three parts.

In Part One, you will play the role of a **blackhat** and **implement a cryptographic protocol for your botnet to communicate** using **strong cryptography**, **key exchange**, **authentication** with **resistance** to a number of **attacks** like **replay** and **message tampering**.

WARGAMES

SHALL WE PLAY A GAME?

Wargames consists of a set of problems, or challenges
Challenges can be done individually or in teams (max: 4, can be different from project)
Difficulty ranges from easy to next-to-impossible

In the olden days some of the challenges had cash prizes (e.g. US$30,000 prize for the RSA challenge). Unfortunately due to the Global Financial Crisis, this has been discontinued. However we will be substituting with some k-rad security prizes!

Due: Thursday midnight before last lecture. Yes, midnight. You will see.

WARGAMES MARKING

Each challenge is worth a different number of points based upon difficulty

There are several types of challenges that include:

Single Solution: Points decay as more people get it correct. If you cheat and tell other teams the answer, you will all get lower marks.

Infinite Solutions: There may be an infinite number of solutions! The best solution gets the highest points. You may submit multiple solutions as you find better answers. Yes, this class is responsible for the secret load that suddenly hits the computer labs at the end of semester..

Your team's final mark will be scaled against the other teams competing in the Wargames, with a threshold to make the resulting marks fair.

Some tasks do have a first-mover advantage, so be sure to pay attention when challenges are released. These will be announced ahead of time.

WARGAMES RULES

- ~~No attacking / breaking into the Wargames website~~
  - This rule has been revoked, have at it.

    However, destructive actions to the scoreboard will result in a score of zero!
- No breaking the law (obviously)
- No signing up under multiple teams
- No destructive behaviour (e.g. no DoS – that’s not cool)
- High-value questions must be accompanied by an explanation to retain the points.

COURSE ASSISTANCE

Lectures, projects, assignments and notices can be found at both:

https://elec5616.com/ OR https://elearning.sydney.edu.au/

The discussion board is available via Ed, where lecturers and tutors can answer:

https://edstem.com.au/courses/150/discussion

(you will receive an invite e-mail at your university e-mail address)

Failing that, e-mail also works:

luke@lukeanderson.com.au

FOLLOW-ON COURSE

A new course, first run in 2015 semester 2:

INFO5010 – Advanced Topic A
Applied Information Security

Semester 2, 2016

While ELEC5616 provides an essential background knowledge in security, INFO5010 provides more practical knowledge around:

- Hacking software
- Hacking networks
- Incident Response
- Building Secure Environments
- Lock Picking

Due to the practical nature of the class, the class size is limited. The best students from ELEC5616 will have first preference for enrolment in INFO5010, at the discretion of the lecturer.