Information Security and Privacy

INFO30006

Lecturer: Heidi Tscherning

Lecture 12: revision and sample exam

AGENDA

I INTRODUCTION

II A WORD ON CRYPTOGRAPHY AND PROTOCOLS

III QUESTIONS – PREPARATION EXAM

IV EXAM REMINDERS AND SAMPLE EXAM

V OTHER

AGENDA

I INTRODUCTION

II A WORD ON CRYPTOGRAPHY AND PROTOCOLS

III QUESTIONS – PREPARATION EXAM

IV EXAM REMINDERS AND SAMPLE EXAM

V OTHER

AGENDA

I INTRODUCTION

II A WORD ON CRYPTOGRAPHY AND PROTOCOLS

III QUESTIONS – PREPARATION EXAM

IV EXAM REMINDERS AND SAMPLE EXAM

V OTHER

Vanessa Teague on cryptography and protocols

AGENDA

I INTRODUCTION

II A WORD ON CRYPTOGRAPHY AND PROTOCOLS

III QUESTIONS – PREPARATION EXAM

IV EXAM REMINDERS AND SAMPLE EXAM

V OTHER

INFORMATION SECURITY AND PRIVACY

RELATIONSHIP BETWEEN INFORMATION SECURITY, PRIVACY, AND CRYPTOGRAPHY

This subject is *"Information Security and Privacy"* – with cryptography. Make sure you understand the link between the three related topics. Create a *Mindmap*, understand definitions, show how *constructs* (both overall and sub-constructs) *relate* to each other!

INFORMATION SECURITY AND PRIVACY

THE WHAT, WHY, WHEN, WHO, WHERE

Consider *why information security and privacy is important*. Why are we spending 12 weeks talking about it? What does it encompass? What are we trying to *protect*? *How*?

What are the threats out there and how are they classified? Where did they come from? What can be done about them? What may happen if we don't do something about them?

INFORMATION SECURITY

THINK ABOUT RISKS!

Why does risk play such a big role in the information security discussion? What are risks and how do we manage them?

INFORMATION SECURITY

WHAT ARE ORGANISATIONS DOING WRONG?

Make it clear what problems organisations are creating for ourselves. What are they doing right? What are the strategies they can use and how good are they?

INFORMATION SECURITY

CONTEMPORARY TOPICS

What is this thing called knowledge leakage? How is it different from data or information leakage?

Consider all the cases from the workshops… What do they have in common? What are the differences?

PRIVACY

THE AUSTRALIAN PRIVACY PRINCIPLES MATTER;

you may need to *apply* them in your jobs when you leave university. They have *legal relevance*, but also provide a *guide for organisations* which gather or store data on their customers. Learn them!

PRIVACY

If you didn't do the **IT SECURITY AUDIT BONUS TASK…**

…that's ok, but you should practice it at least a little at home for your own benefit. That includes *researching* and knowing the *different solutions* available to security problems, and their *strengths* and *weaknesses*.

PRIVACY

We discussed numerous **IT SECURITY BREACH CASES** that have been in the media.

These are excellent *case studies* for understanding what can (and has) gone wrong. Get familiar with them, and how they could have been prevented.

PRIVACY

DID YOU FIND OUT WHERE THAT CAT LIVES?

Metadata is a complex subject in the digital age; few IT by-products affect security and privacy as much. Be sure you understand it well, and the social and legal matters around it.

PRIVACY

US AND FIVE EYES GOVERNMENT DIGITAL SURVEILLANCE is far more widespread than we knew before the Snowden revelations. Be sure you can dimension the *nature and scope of the privacy intrusions*.

PRIVACY

- Be sure you can explain *why* privacy is important.
- Understand *barriers* to IT anonymity.

AGENDA

I INTRODUCTION

II A WORD ON CRYPTOGRAPHY AND PROTOCOLS

III QUESTIONS – PREPARATION EXAM

IV EXAM REMINDERS AND SAMPLE EXAM

V OTHER

EXAM REMINDERS

1. *Check* date, time and venue on the day
2. Remember student card!
3. 15 minute Q&A (only *comprehension questions*/only Heidi present)
4. 2 hours, *plan time* based on *marks* and *types of questions*
5. Provision of script book (*write on right-hand side only!*) and MCA sheet
6. Three parts (Information security, privacy, cryptography)
7. *Read* all questions with care: *what are we asking you to do? (NB! Which section is the question located under?)*
8. Answer *all* questions – a wrong answer will *not* cause deduction in marks
9. **TIME GOES FAST!!**

(SAMPLE) EXAM

INFO30006 – INFORMATION SECURITY AND PRIVACY SAMPLE EXAM

School of Computing and Information Systems

INFO30006 Information Security and Privacy SAMPLE EXAM

End of Semester 2 2017

Reading Time: 15 minutes

Writing time: 120 minutes

This paper has 4 pages including this page.

Authorised materials
None

- 15 MINUTE READING TIME (QA)
- 2 HOUR WRITTEN EXAM
- NO AUTHORIZED MATERIALS ALLOWED
- INSTRUCTIONS TO STUDENTS

PART I: INFORMATION SECURITY

The section on information security consists of 3 questions worth TEN (10) marks in total.

Question 1: **[3 marks]**

The CIA Triad represents fundamental security goals of Information Security. Describe two other security goals and briefly explain what they represent.

Question 2: **[3 marks]**

List 5 different types of security threats and provide an example of each.

Question 3: **[4 marks]**

You are conducting a risk management exercise in your company and you and your team have identified 10 risks that have been classified as project and business risks.

a) Describe what project and business risks are

b) Describe the processing of analysing the identified risks before you can respond with the proper response strategy.

PART II: CRYPTOGRAPHY AND PROTOCOLS

The section on cryptography and protocols consists of 4 questions worth TWENTY-FIVE (25) marks in total.

Question 4: Short answer questions **[15 marks]**

a) What is wrong with 512-bit RSA? Why was it mandated, for what purpose, and how long ago? [4 marks]

b) Write two desirable secrecy properties of a key exchange protocol, and write a sentence explaining what they mean. [4 marks]

c) List three crucial security properties necessary for elections. [3 marks]

d) You are a manager in an organisation and are explaining to a staff member why and how to use Signal. Briefly justify why they should use Signal, and at least one important applied security feature in it including instructions on how to use it. [3+1 marks]

(SAMPLE) EXAM

- THREE PARTS
- TOTAL OF 50 MARKS (*NOT* EQUALLY DISTRIBUTED)
- MIX OF QUESTIONS
  - MULTIPLE CHOICE
  - SHORT ANSWER QUESTIONS
  - SHORT ESSAY QUESTIONS

PART III: PRIVACY

The section on privacy consists of 2 main questions (7 and 6 sub-questions respectively) worth FIFTEEN (15) marks in total. The next 7 questions are about the Australian Privacy Principles (APPs).

Question 6: Multiple Choice Questions **[6 marks]**

The following 6 privacy questions are worth 1 mark each unless otherwise stated; total EIGHT (8) marks:

a) Is the following statement true or false: WhatsApp provides confidentiality of communication and anonymity?
- true
- false

b) Which of the following are examples of metadata:
- The creation date of a cell-phone photograph
- Your public key listed in your signature
- A video attachment sent over WeChat
- All of the above
- Two of the above

c) If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information without exception:
- true
- false

d) An APP entity must have a clearly expressed and up to date policy about the management of personal information by the entity which contains:
- the kinds of personal information that the entity collects and holds;
- how the entity collects and holds personal information;
- the purposes for which the entity collects, holds, uses and discloses personal information;
- all of the above

e) In relation an APP entity's functions or activities, the entity must take reasonable steps to make sure it complies with the Australian Privacy Principles in its:

(SAMPLE) EXAM

- **THREE** PARTS
- TOTAL OF 50 MARKS (***NOT*** EQUALLY DISTRIBUTED)
- MIX OF QUESTIONS
  - MULTIPLE CHOICE
  - SHORT ANSWER QUESTIONS
  - SHORT ESSAY QUESTIONS

(SAMPLE) EXAM

PART II: CRYPTOGRAPHY AND PROTOCOLS

The section on cryptography and protocols consists of 4 questions worth TWENTY-FIVE (25) marks in total.

Question 4: Short answer questions **[15 marks]**

a) What is wrong with 512-bit RSA? Why was it mandated, for what purpose, and how long ago? [4 marks]

b) Write two desirable secrecy properties of a key exchange protocol, and write a sentence explaining what they mean. [4 marks]

c) List three crucial security properties necessary for elections. [3 marks]

d) You are a manager in an organisation and are explaining to a staff member why and how to use Signal. Briefly justify why they should use Signal, and at least one important applied security feature in it including instructions on how to use it. [3+1 marks]

Location of question ***may*** help you find an answer

Question 5: Privacy **[10 marks]**

a) Give 3 specific examples of digital footprints that impinge on privacy. [6 marks]

b) Provide at least one way to improve user adoption of privacy-enhancing technologies and explain why it will improve adoption (briefly). [4 marks]

PART III: PRIVACY

The section on privacy consists of 2 main questions (7 and 6 sub-questions respectively) worth FIFTEEN (15) marks in total. The next 7 questions are about the Australian Privacy Principles (APPs).

Question 6: Multiple Choice Questions **[6 marks]**

The following 6 privacy questions are worth 1 mark each unless otherwise stated; total EIGHT (8) marks:

a) Is the following statement true or false: WhatsApp provides confidentiality of communication and anonymity?

AGENDA

I INTRODUCTION

II A WORD ON CRYPTOGRAPHY AND PROTOCOLS

III QUESTIONS – PREPARATION EXAM

IV EXAM REMINDERS AND SAMPLE EXAM

V OTHER

END-TO-END ENCRYPTION AND INTERCEPTION PUBLIC LECTURE *TODAY 5-6PM*

WHAT?

- This panel discussion will address the Australian government's proposal to insist on government access to encrypted data.
- The Australian Prime Minister Malcolm Turnbull and Attorney General George Brandis want to introduce laws that would compel technology companies to ensure their systems are capable of recovering terrorists' communications. Currently, there is very little publicly available information about how this will be achieved.

PANELISTS? MODERATOR?

- **FERGUS HANSON**, head of the international cyber policy centre at the Australian Strategic Policy Institute,
- **SCOTT LUDLAM**, former WA Greens Senator and deputy leader of The Greens,
- **VANESSA TEAGUE**, cryptographer in the department of computing and information systems, University of Melbourne.
- Moderated by **SUELETTE DREYFUS**

WHERE?

Herbert Wilson Theatre (Basement), Doug McDonell

Link to event: https://events.unimelb.edu.au/events/9613-end-to-end-encryption-and-interception

WHAT NOW?

Written assignments - status:

- We are currently correcting your assignments
- Assessment will be released end of next week (By Friday 27 October 2017)

Offer: one hour Q&A session on campus (recorded) or webinar:

- If you wish, I offer one 1-hour session for questions and answers as preparation for exam
- Contact your student representatives, who should coordinate with me
- I need:
  - 2-3 potential time slots at least 3 working days prior to session
  - List of questions to address

Questions via email:

- You can send me questions via email, and I will try to answer. I will post a list of questions I have received on LMS for the benefit of all
- I will post the remaining presentations and facilitation notes on LMS from workshops for your benefit when preparing for the exam. Please send!

Overall assessment

- Workshops
  - Presentation
  - Facilitation
  - participation
- Written assignment
- Exam – Hurdle requirement

STUDENT EVALUATION SURVEY (SES)

PLEASE FILL OUT THE STUDENT EVALUATION SURVEY!

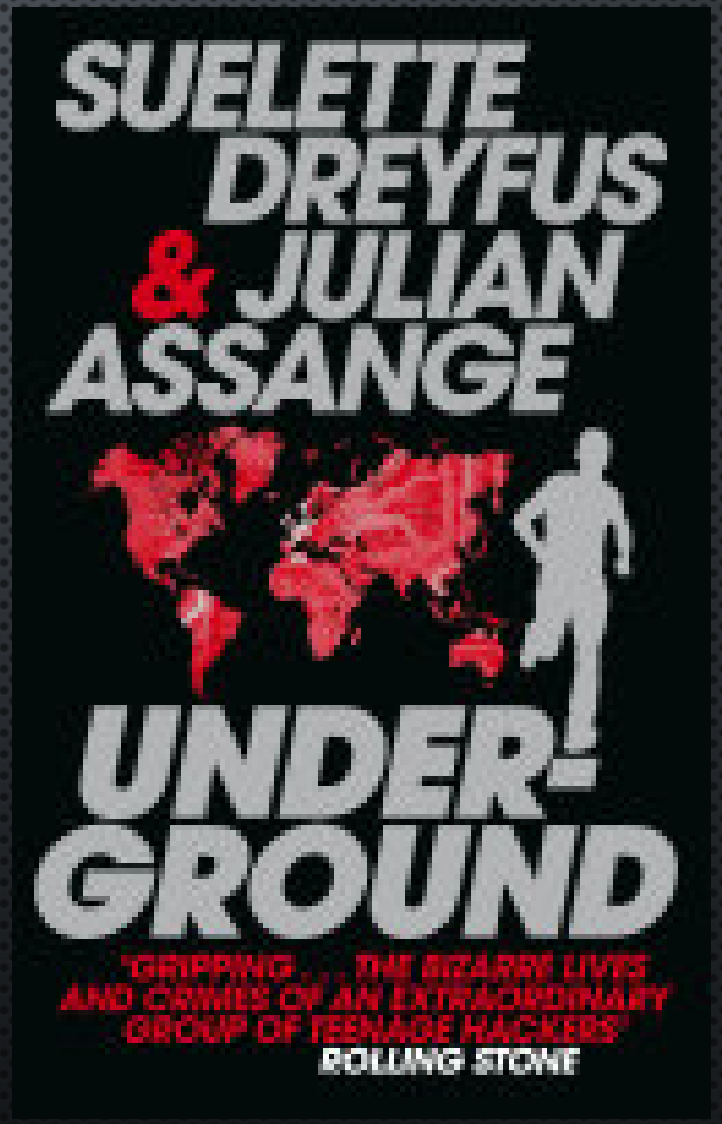
Bonus information…

BONUS INFORMATION…

SUELETTE DREYFUS & JULIAN ASSANGE: "UNDERGROUND"

"Suelette Dreyfus and her co-author, WikiLeaks founder Julian Assange, tell the extraordinary true story of the computer underground, and the bizarre lives and crimes of an elite ring of international hackers who took on the establishment. Spanning three continents and a decade of high level infiltration, they created chaos amongst some of the world's biggest and most powerful organisations, including NASA and the US military. Brilliant and obsessed, many of them found themselves addicted to hacking and phreaking. Some descended into drugs and madness, others ended up in jail. As riveting as the finest detective novel and meticulously researched, Underground follows the hackers through their crimes, their betrayals, the hunt, raids and investigations. It is a gripping tale of the digital underground."

Link: http://www.underground-book.net



THANK YOU!

QUESTIONS?