UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

Security II — Exercises

Academic year 2014–2015

Lent term 2015

http://www.cl.cam.ac.uk/teaching/1415/Algorithms/

frank.stajano--sec2@cl.cam.ac.uk (author of this handout)

Revised 2015 edition

Revision 7 of 2015-01-10 19:23:37 +0000 (Sat, 10 Jan 2015).

Introduction

I now encourage all students and supervisors to use the wonderful Otter system, even though it is still somewhat experimental (feedback on your experience with it will help us improve it). This pdf is a legacy document and Otter by now contains additional questions that do not appear in this document. The supervision aids provided by Dr Stajano cover his lectures and those of the guest lecturers. Separate supervision aids are provided by Dr Kuhn for his own part of the course.

The official historical repository of exam questions is accessible from the course web page.

As this is a final-year Part II course, students who study this course are encouraged and expected to read the papers in the syllabus as opposed to relying only on the course handout. The advice in the following two-page paper may be helpful in acquiring this vital research skill: S. Keshav, "How to Read a Paper", *ACM SIGCOMM CCR* 37(3):83–84, 2007. `http://www.sigcomm.org/sites/default/files/ccr/papers/2007/July/1273445-1273458.pdf`

Students seeking clarification about these exercises are encouraged to contact their supervisor in the first instance. If this is unsuccessful, email to the lecturers about this course will be treated with higher priority if sent to the correct address listed on the front page (note that Dr Stajano's priority address contains a double hyphen).

This is a 16-lecture course with 4 supervisions, thus averaging one supervision every four lectures. Topics to be covered in supervisions are at the discretion of the supervisor but as a rough guideline you might use the first two lectures for the topics covered by Dr Stajano and the guest lecturers and the second two for the topics covered by Dr Kuhn.

Exercise 1
Pick any version of the encryption program PGP or its free equivalent GPG—preferably one with a GUI—and list:

- Three potentially dangerous irreversible actions that a user might perform by accident (higher marks the more dangerous the action and the more likely the user is to invoke it by accident)
- Three common actions that users might get wrong, with explanations of why they might get it wrong and of how the user interface might be improved to decrease the likelihood of that happening.

Exercise 2
Describe at least 3 practices commonly adopted by system administrators to enhance password security that instead have the opposite effect. Explain why they backfire and discuss ways to improve them.

Exercise 3
How would you get hold of:

- The employee number of a mark in a corporation? (And, having obtained it, how could you use it?)
- A company-confidential internal phone directory?
- The credit card number and expiry date of a mark? (And, having obtained it, how could you get a couple of grand out of it without getting caught? Assume for simplicity that that's in the days before CVV.)

More generally, what are the important traits of a successful social engineer?

Exercise 4
Explain three principles of human psychology that you can exploit to steal a hundred pounds cash from a stranger. Explain how you can exploit those same principles to attack a computer system. Explain how you can exploit those same principles to sell an overpriced car to a mark.

Exercise 5
Construct an example test of the type "Would you rather take choice A or choice B?" to illustrate the crucial insight of Bernoulli's Expected Utility Theory, and explain what that insight is.

Exercise 6
Construct an example test of the type "Would you rather take choice A or choice B?" to illustrate what Tversy and Kahneman call "Bernoulli's error", and explain what that is.

Exercise 7
Describe seven *qualitatively different* password replacement schemes and, for each, point out its most significant advantage over passwords and its most significant disadvantage. If two of your schemes have the same (best advantage, worst disadvantage) pair, they are not sufficiently different.

Exercise 8
List three kinds of "costs" perceived by individuals of security tasks imposed by system administrators.

Exercise 9
Bell-LaPadula consists of two rules. What is the invariant that both rules are intended to preserve?

Exercise 10
In a military context, you have a BLP compliant system with a subject (= process) A cleared to TOP SECRET and a subject B cleared to CONFIDENTIAL. A file X containing nuclear launch codes is labelled as TOP SECRET. Is it possible for A to transmit the content of X to B? If yes, how (and why would A want to do that)? If no, why?

Exercise 11
Assume the use of 6-pin locks where each pin can be cut to 6 possible depths labelled from 1 to 6. Describe how a locksmith would build a simple master key system in which each lock is individually keyed but there is also one master key that opens all the 100 doors in the building. (Here you must explain precisely how the locksmith will cut the pins in each of the 100 doors and how she will generate the corresponding keys.) Then, switching from defense to attack, assume you have unsupervised access to one of the doors, that you also have key cutting equipment that allows you to cut a key to any specified pattern, and that you have a reasonable supply of key blanks. Without lockpicking, how many attempts will it take you to create a key that will open the door? And what if the lock were not master-keyed? And finally: assuming you are also given the individual change key for that door (ie not the master key), how will you go about creating a master key that will open all the other doors, and how many attempts will it take?

Past exam questions

You may obtain PDFs of these and many more exam questions from the course web site. Please also consider suitable exam questions from the predecessor course that used to be called "Security" but also double-check, perhaps with the help of your supervisor, that the questions are covered in this year's syllabus as defined in this year's course web page.

Security II 2010–2011 – Question 1 (RJA/FMS)

(*a*) Write out the Needham-Schroder protocol, explaining the notation you use. [5 marks]

(*b*) Describe the "bug" in the protocol, stating why some people think it to be a bug and other people consider it not to be. [5 marks]

(*c*) Provide an amended protocol that does not have the "bug" but which (unlike Kerberos) uses random nonces rather than timestamps. [10 marks]

Security II 2010–2011 – Question 2 (RJA/FMS)

You are consulting for a large online services company which stores personal information on millions of customers. Your client's directors are alarmed by the Wikileaks saga and are concerned about damage to their company's reputation should a disaffected member of staff steal and publish personal information on a large number of customers.

Discuss the security policy options available to your client to minimize the damage that a member of staff could do. [20 marks]

1

Security II 2012 – Paper 7 Question 12 (FMS)

The RSA cryptosystem can be tuned to make the workload asymmetric: with $d = 3$, encryption (cubing modulo n) becomes very cheap and almost all the computational expense shifts to decryption (extracting cubic roots modulo n).

The following public-key protocol uses the above property to allow two principals A and B to establish a common secret key N_b (invented by B) without incurring a high computational load, thanks to the help of a server S who computes all the cubic roots in the protocol. Attackers are assumed to be able to overhear, but not alter, the messages between A, B and S.

$$\begin{array}{ll} A \to S: & B, N_a^3 \bmod n. \\ S \to B: & A. \\ B \to S: & A, N_b^3 \bmod n. \\ S \to A: & B, N_a \oplus N_b. \end{array}$$

(a) What is the purpose of N_a? [3 marks]

(b) Describe in detail a protocol attack that will allow two colluding attackers C and D to recover N_b. Assume that S is stateless. [5 marks]

(c) Stop the attack you described in (b) by making S stateful. [5 marks]

(d) Describe in detail a more sophisticated protocol attack whereby the colluding attackers will recover N_b even if S adopts the precaution you described in (c). [4 marks]

(e) Fix the protocol to defeat the attack you described in (d). [3 marks]

Security II 2012 – Paper 8 Question 12 (FMS)

The lifecycle of an exam question in a fictitious university includes at least the following stages, which take place over several months:

1. Professor invents question.
2. Chief examiner sanity-checks it.
3. Professor amends it if necessary.
4. External auditor sanity-checks it.
5. Professor amends it again if necessary.
6. Chief examiner approves final version.
7. Clerk prints question in required number of copies.

Following a scandal whereby some dishonest candidates got hold of questions ahead of time, thus forcing the whole exam to be invalidated and repeated to the dismay of the honest participants, the university has put pressure on its departments to ensure this won't happen again.

(a) The head of department A, where the leak occurred, is now paranoid about computer networks and insists that no exam question shall ever reside on any networked computer system until after the corresponding exam takes place.

(i) Describe four ways that a determined undergraduate might nonetheless get hold of exam questions before the exam even if that requirement were observed. [4 marks]

(ii) Describe a security policy suitable for department A, taking into account the head-of-department's requirements and the staff workflow. Discuss it thoroughly, including incentives and technical mechanisms. [4 marks]

(b) The head of department B finds that A's requirement would impose an excessive penalty on the productivity of her staff. At the same time, she certainly doesn't want to be blamed for the next leak.

(i) Describe a security policy suitable for department B, taking into account the head-of-department's requirements and the staff workflow. Discuss it thoroughly, including incentives and technical mechanisms. [6 marks]

(ii) Describe three trade-offs between security and usability that you considered in devising the policy in (b)(i) and justify the choices you made. [6 marks]

1