Security
– exercises

Markus Kuhn

Easter 2018 – CST Part IB

1 Introduction

Exercise 1: Estimate the length of a list of all computers that could have directly or indirectly caused you significant inconvenience if someone had illicitly manipulated them with hostile intentions.

Exercise 2: What would a security analysis for your bicycle look like? What assets does your bicycle provide to you, and what vulnerabilities and threats to you and others do they create? What other risks and requirements could you face as its owner and user?

Exercise 3: Suppose you are computerising Britain's medical records, and building a distributed database of all GP and hospital records, as well as all drugs prescribed. What would the main security requirements be?

Exercise 4: Describe some of the threats posed by the battlefield capture of a fighter aircraft. As its designer, what precautions would you take?

Exercise 5: Outline a possible security analysis and policy for a university department with regard to how exam questions are prepared by lecturers.

2 Access control

Exercise 6: While inspecting the discretionary access-control arrangements on a Unix computer, you find the following setup:

Members of group `staff`: `alex`, `benn`, `cloe`
Members of group `gurus`: `cloe`

```
$ ls -ld . * */*
drwxr-xr-x  1 alex staff    32768 Apr  2  2010 .
-rw----r--  1 alex gurus    31359 Jul 24  2011 manual.txt
-r--rw--w-  1 benn gurus     4359 Jul 24  2011 report.txt
-rwsr--r-x  1 benn gurus   141359 Jun  1  2013 microedit
dr--r-xr-x  1 benn staff    32768 Jul 23  2011 src
-rw-r--r--  1 benn staff    81359 Feb 28  2012 src/code.c
-r--rw----  1 cloe gurus      959 Jan 23  2012 src/code.h
```

The file `microedit` is a normal text editor, which allows its users to open, edit and save files.

Draw an access control matrix (arranged as below) that shows for each of the above five files, whether `alex`, `benn`, or `cloe` are able, directly or indirectly, to obtain the right to read (R) or replace (W) its contents.

	manual.txt	report.txt	microedit	src/code.c	src/code.h
alex					
benn					
cloe					

Clarify how each access right R or W was obtained by marking it as follows:

- underline if obtained via rights elevation,
- append * if obtained via the parent directory (delete and replace),
- append $^+$ if obtained through ownership (`chmod`).

Exercise 7: Which Unix command finds all installed setuid root programs?

Exercise 8: Which of the Unix commands that you know or use are setuid root, and why?

Exercise 9: What Unix mechanisms could be used to implement capability-based access control for files? What is still missing?

Exercise 10: If a multilevel security OS has to run real-time applications and provides freely selectable scheduling priorities at all levels, how does that affect security?

Exercise 11: How can you implement a Clark-Wilson policy under Unix?

Exercise 12: How can you implement a Clark-Wilson policy under Windows?

Exercise 13: How can the *GNU Revision Control System (RCS)* be set up to enforce a Clark/Wilson-style access control policy? (Hint: `man ci`)

3 Operating-system security

Exercise 14: Read

> Ken Thompson: *Reflections on Trusting Trust*, Communications of the ACM, Vol 27, No 8, August 1984, pp 761–763
> `http://doi.acm.org/10.1145/358198.358210`

and explain how even a careful inspection of all source code within the TCB might miss carefully planted backdoors.

Exercise 15: You are a technician working for the intelligence agency of Amoria. Your employer is extremely curious about what goes on in a particular ministry of Bumaria. This ministry has ordered networked computers from an Amorian supplier and you will be given access to the shipment before it reaches the customer. What modifications could you perform on the hardware to help with later break-in attempts, knowing that the Bumarian government only uses software from sources over which you have no control?

Exercise 16: The Bumarian government is forced to buy Amorian computers as its national hardware industry is far from competitive. However, there are strong suspicions that the Amorian intelligence agencies regularly modify hardware shipments to help in their espionage efforts. Bumaria has no lack of software skills and the government uses its own operating system. Suggest to the Bumarians some operating system techniques that can reduce the information security risks of potential malicious hardware modifications.

Exercise 17: Read in the Common Criteria "Controlled Access Protection Profile" the "Security Environment" section. Was this profile designed to evaluate whether a system is secure enough to be connected to the Internet?

`http://www.commoncriteriaportal.org/files/ppfiles/capp.pdf`

4 Software security

Exercise 18: Suggest a mandatory access control policy against viruses.

Exercise 19: How can you arrange that an attacker who has gained full access over a networked machine cannot modify its audit trail unnoticed?

Exercise 20: On an operating system of your choice, call `getsp()` (slide 91) repeatedly and output the resulting stack-pointer address as a hexadecimal number.

(a) How many and which bits of the stack-pointer address does your operating system apparently chose at random when it starts a new process?

(b) Let's assume an attacker can afford a 4096 bytes long landing pad and can try one buffer overflow every 20 ms. How long does this attacker then have to try on average until the return address hits the landing pad?

(c) On a little-endian processor, the attacker does not have to overwrite all bytes of a return address, as some of the most-significant bytes of the original address will already have the correct value. If the original return address points to a function in a shard library (libc) that is mapped into memory less than 16 megabytes away from the current stack pointer, how can that help to reduce the average number of attempts required compared to part (b)?

Exercise 21: The log file of your HTTP server shows odd requests such as

```
GET /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+C:\
GET /scripts/..%u002f..%u002fwinnt/system32/cmd.exe?/c+dir+C:\
GET /scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+C:\
```

Explain the attacker's exact flaw hypothesis and what these penetration attempts try to exploit.

(Is there a connection with the floor tile pattern outside the lecture theatre?)

5 Cryptography

6 Entity authentication

Exercise 22: Login names are usually not considered secret, but passwords are. Therefore it is common practice to display login names while they are entered on a keyboard, but not passwords, such that bystanders cannot read the latter off the display ("shoulder surfing"). Instead, password entry fields typically just indicate with a generic symbol that a keystroke was received, which reveals only the length and typing rhythm of the password. Likewise, a log file for auditing logins will usually record an entered user name, but not the password supplied.

Users often mix up user-ID and password at login prompts. How should the designer of a login function take this into consideration?

Exercise 23: The runtime of the usual algorithm for comparing two strings is proportional to the length of the identical prefix of the inputs. How and under which conditions might this help an attacker to guess a password?

Exercise 24:

(*a*) In the original Kerberos implementation of the Needham–Schroeder protocol, key K_{AS} is derived from a user password using a pasword-based key derivation function (PBKDF). What implications does this have for the minimum strength of passwords suitable for use with Kerberos?

(*b*) Modern implementations of Kerberos change the first message to

$$A \to S : \qquad [T_A]_{K_{AS}}, A, B$$

What is the purpose of including this "preauthentication" data?

7 Network security

Exercise 25: Suggest countermeasures against "SYN flooding" attacks. In particular, can you eliminate the need for keeping a data record on the destination host by appropriately choosing the sequence number y?

Exercise 26: How could you "hijack" a telnet session? Possible countermeasures?