Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT145G Computer Security

Daniel Bosk

Department of Information Systems and Technology,
Mid Sweden University, SE-851 70 Sundsvall
Email: daniel.bosk@miun.se
Phone: 010-142 8709

2018-08-27

Instructions

Carefully read the questions before you start answering them. Note the time limit of the exam and plan your answers accordingly. Only answer the question, do not write about subjects remotely related to the question.

Write your answers on separate sheets, not on the exam paper. Only write on one side of the sheets. Start each question on a new sheet. Do not forget to *motivate your answers.*

Make sure you write your answers clearly, if I cannot read an answer the answer will be awarded no points—even if the answer is correct. The questions are *not* sorted by difficulty.

Time 5 hours.

Aids Dictionary.

Questions 9

Preliminary grades

Each question can be awarded up to three points: one point for E, two points for C and three points for A. To get an E, you must get at least one point on each question — i.e. no question must be awarded zero points. For a C, you must get two points on at least half of the questions. For an A, you must get three points on at least half of the questions.

Questions

The questions are given below. They are not given in any particular order.

(3p) 1. Explain why it is not possible to *securely* embedd a cryptographic key in a program (e.g. a smartphone app), i.e. why the adversary can steal the key. Also describe the requirements for a solution and possibly some example.

Suggested solution Since the software might run in a hostile environment, the adversary can extract the key.

The only way to prevent an adversary from extracting the key is to store it in special-purpose hardware. If you can ensure the integrity of the operating system, then sandboxing the applications will protect the key from other (malicious) applications which try to steal the key.

(3p) 2. Give a brief overview of the most important aspects of a secure logging system.

Suggested solution The logging system must be stored in a secure location. It must be append only — i.e. no one can read or change the log. There are problems with the administrator of a system, since he or she can modify the logging system and thus "hide the tracks". This must be solved by setting up the logging system with separation of duties, e.g. the logging system of system A is under control of administrator B and the logging system of system B is under control of administrator A.

(3p) 3. Give an example where "data" can be mistaken for "code" and explain what the consequences are.

Suggested solution Shell scripting is an easy example. Here you can store part of the code in variables, the simply substitute them. Consider the following `/bin/echo -e ${1}`. The variable `${1}` will be substituted and the result will be interpreted as actual arguments to the program.

(3p) 4. You've just landed a job as a developer somewhere and now you're having one of your first few days. There is a discussion in the "fika room", the topic is the password policy.

"Well, every respectable website requires at least eight characters, with lower and upper case, numbers and special characters", the head of the team says, "so we have it too".

What would you like to say in this conversation?

Suggested solution The last decades' research in user authentication says that such a policy yields bad security. It forces users to select easy to guess passwords and incentivizes password reuse while more secure passwords are disqualified according to the policy.

A better policy is to have at least 12 characters as the only requirement. Also, no requirement of updating the password at regular intervals — only if a breach has occurred.

(3p) 5. What is attribute-based access control (ABAC) and what are its advantages?

Suggested solution It's an access control model.

It uses attributes in the security policy: e.g. identities, age limits, times. This requires authenticated attributes.

This is the most general access control model.

(3p) 6. The terms “data” and “information” are related but not the same. Discuss how they are related and how this affects the term “security”, as in “data security” and “information security”.

Suggested solution Data is an encoded representation of information. Data can be manipulated by formal rules to infer new information. E.g. the data “$x + 1 = 0$” does not directly reveal the value of x, but we can manipulate the data with formal rules (equation solving) and infer the value of x ($x = -1$).

The same applies for other situations: When sending data over an anonymizing network (e.g. Tor), we only reveal the size and timing of the packets sent. However, these can be statistically correlated to the packets exiting the network, thus the sender and recipient can be inferred.

7. What does it mean to authenticate something? Illustrate your explanations by discussing the following examples and explain why they work or not:

- Alice authenticates her identity to Bob by showing him her ID card.
- Alice authenticates her age to the cinema by showing her ID card.
- Alice authenticates her identity to the web server by sending her password.

Suggested solution To authenticate something means to prove its authenticity.

For example, Alice might claim to Bob that her identity is Alice. However, from Bob’s point of view, she might just as well be Eve trying to fool Bob. Thus Bob needs some compelling evidence from Alice that actually proves that she indeed is Alice, i.e. Alice authenticates her identity.

As another example, Alice might want to prove the authenticity of her age to Bob. In the previous example, Alice could use an ID card to prove that her name is Alice (her identity). In this case she could still use the ID card, but this time her name is not interesting, it’s her age (birthdate).

The method of the ID card only works if Bob *trusts* the issuer; in the case of an ID card, it will be the local government. The principle is that the issuer has verified some attributes (Alice’s name or identity, her birthdate and probably a few more). If the ID card must be easy to verify but difficult to forge, then Bob can trust the validity of the attributes.

Finally, Alice authenticates her identity to a web server using a password. The reason this works is that Alice and the web server has agreed on a secret that only Alice and the web server knows. If this secret is hard to guess, then the web server can be sure that someone indeed is Alice if they know Alice’s password.

(3p) 8. There are numerous alternatives available today for end-to-end secure communication[1], e.g. the apps Signal, WhatsApp and Telegram for instant messaging, media messaging and video calls; PGP and S/MIME for email. They are all based on a combination of public-key and shared-key cryptography.

Discuss the usability challenges facing end-to-end secure communication.

Suggested solution The challenge for these systems is to provide a design which aligns the security with how users work.

The easy part is to provide a tool for securing the communication, i.e. encrypting and providing integrity checks.

The hard part is to do proper key management, specifically to authenticate the owners of the other keys. The currently most used approach is that of Signal, WhatsApp and Telegram. They

[1] Normally this is referred to as end-to-end *encrypted* communication, but we have integrity in addition to confidentiality.

authenticate phone numbers by sending text messages to the phone number. Thus they can be sure that the owner of the phone number is also the owner of the private key. (Well, the phone operator can of course impersonate the owner of the phone number.) Then another user has identified another user by his or her phone number, then the app will ensure the verified key is used.

(3p) 9. What is a covert channel?

Suggested solution A covert channel is a mechanism that was not designed for communication but which can nonetheless be abused to allow information to flow in a way which is not allowed in the security policy. The problem commonly arises when two clearance levels shares resources.