ISAE Embedded systems master

Evaluation – Exercises and questions

4 april 2022

Embedded systems and computer security

Advice to students and supervisors : course documents (either furnished by the school or hand-written during oral courses by the student himself) are allowed during the examination, a standard calculator too (for calculation purposes only) and blank paper sheets for draft.

All other documents, communication devices or media access (like Internet) are not allowed, unless direct explicit authorization from the session supervisor.

Please, write your answers on the document itself in the place reserved.

Student name and surname :

Part I (10 pts)

This first part consists of ten questions (1 pt per question) with multiple answers proposed among which you must select the appropriate one. Unless explicitly indicated, only one answer is the correct one.

Attention, the following notation system will be used :

Correct answer : 1 point added False/no answer : 0 point

Q1 What could be a good moment in a software development project to consider security requirements?

- ☐ Before the project idea emerges.
- ☐ After server shutdown but before actual hardware disposal.
- ☐ During the qualification of the new service.
- ☐ During the 100th customer celebration.
- ☐ During costing evaluation at project definition.

Q2 The HR policy of the company stated that wages would not see any general augmentation in 2021. Furthermore, the specific salary of any individual is kept strictly confidential by the company. However, by querying statistics, unions observe that a few people indeed were given significant benefits with respect to others. Which confidentiality defeating techniques was used to obtain such information ?

- ☐ Bribery.
- ☐ Inference.
- ☐ Cryptanalysis
- ☐ Seduction.
- ☐ Eavesdropping.

Q3 Which case is an example of a Trojan horse?

- ☐ A fake login script recording passwords.
- ☐ A data destruction program triggering at employee departure.
- ☐ A program abusing a remotely exploitable buffer overflow in the company web server.
- ☐ A malicious script scanning accessible filesystems and deleting files randomly.
- ☐ A spy stealing backup tapes.

Q4 What is most characteristic of the security field ?

- ☐ The three attributes: confidentiality, integrity and availability.
- ☐ The relationship with legal constraints.
- ☐ The integration of procedural and organizational aspects.
- ☐ Malicious actions.
- ☐ The historical advance of military work.

Q5 Why is it annoying in the long term that subjects habilitated at a given level can write objects classified at a higher level under the Bell-LaPadula multilevel confidentiality policy ?

- ☐ Highly confidential data may be corrupted by the insertion of false data.
- ☐ Intermediate level data can be more easily compromised than high level data
- ☐ Unclassified information can also be labeled at the secret level.
- ☐ Secret agents will have access access to the cantine menu, but only top secret agents will know which meal is poisoned.
- ☐ Declassification procedures are necessary to keep secret information from growing too much.

Q6 Why is it impossible to trust a single public key to provide adequate confidentiality protection?

- ☐ Because prime numbers factorization is going to improve a lot with quantum computers.
- ☐ Because perfect security does not exist and you can always guess the key.
- ☐ Because the associated private key may be under control of an attacker impersonating the recipient.
- ☐ Because public/private key pairs are mostly useful for signature and integrity protection.

Q7 Which of these aspects of system hardware is associated to an *auxiliary* channel ?

- ☐ The noise of CPU fan.
- ☐ The motherboard price.
- ☐ The VGA monitor cable.
- ☐ The peripheral communication bus arbitration protocol.

Q8 The following piece of C code is *incorrect*.

```
#include <stddef.h>

enum { SIZE = 32 };

void func(void) {
  int nums[SIZE];
  int end;
  int *next_num_ptr = nums;
  size_t free_elements;

  /* Increment next_num_ptr as array fills */
  free_elements = &end - next_num_ptr;
}
```

Why ?

- ☐ It is strange to use an enum to declare the size of an array.
- ☐ It is incorrect to assume that the `nums` array is adjacent to the `end` variable in memory.
- ☐ Pointer arithmetic is always forbidden in C.
- ☐ There is no return statement in the function.

Q9 Which one is an encryption algorithm ?

- ☐ Diffie-Hellman
- ☐ RSA
- ☐ SHA3
- ☐ TCP
- ☐ SMTP

Q10 How can you realistically protect a component from nuclear radiation ?

- ☐ By eliminating covert channels.
- ☐ By heavy shielding and redundancy (of memory and logic).
- ☐ With a Faraday cage.
- ☐ By a strong electromagnetic field.

Part II (10 pts)

This part is composed of five open questions (2 pts each). Please write down your answer *on this document* in the appropriate space.

Question 1

Propose some programming security rules for the development of an embedded computer (in a general purpose land vehicle) :

- 2 rules to enforce in the context of programming in the C language:

- and then 2 rules that you would like to see adopted for program development, *independently* of the programming language.

Question 2

Consider a merchant website for a shop of clothes.

Propose 2 security objectives for this system (among all the imaginable ones).

Now propose practical security mechanisms that you want to integrate in the website to address (fully or partially) those objectives :

Question 3

Consider the files stored on your own typical personal laptop (portable computer). Give one example of the files most important to *you* with respect of all the three attributes of security (confidentiality, integrity, availability).

Justify this importance (one of the highest of the entire computer for you !).

- integrity

- confidentiality

- availability

Question 4

Propose at least 2 programming rules for the development of an encryption library (or the encryption component of some piece of software).

Question 5

NB: Given its evident difficulty, this last question is certainly to be addressed last and will be corrected with indulgence. But write something sensible !

Imagine a space station in low earth orbit composed of several modules provided by different nations over a multiple years construction period. All these interconnected modules are equipped with independently designed and built embedded computers controlling each module systems. Each module has its own autonomous communication system with ground based control stations in the country it is originating from. Outside of life habitat and on-site maintenance access which all modules provide/allow to passengers, each module can perform a single station-wide function: like (maneuvering) propulsion, energy supply, science laboratory, docking, life support, etc. The computers of each module can communicate with each other on a shared local wired network ; for example to share external communication means or sensors data.

1) Can you formulate some security requirements for the core security components of one of those computers ?

2) Now, imagine one of the home nations of the station modules *intends* to become belligerent with an ally of the others. What part of those security requirements would become obsolete ? Which *new* security objectives may appear ?

3) When conflict starts, what can the passengers (those whose nations are not directly involved in the conflict) try to do in order to mitigate the impact of the bellicose country controls ?

4) Now that you have a better intuition with respect to future proof security requirements, if a new (most probably different) international cooperation were to lead to the construction of a second (secure) international space station : can you propose security mechanisms that would allow new control computers of such modules to continue to trust each other and cooperate in such a complex situation ?

Question 5 (*cont*.)