ISAE Embedded systems master

Evaluation – Exercises and questions

25 february 2020

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 Why is it annoying to initialize the private key of a hardware security module at the factory ?

- ☐ Donald gets mad at the idea that Jinping may have tampered the motherboard.
- ☐ It is not. In fact, due to latest attack techniques based on silicium doping alterations, one needs to have its own semiconductor factory anyway for decent security.
- ☐ It raises doubts on the fact that the key might have been recorded.
- ☐ It costs a lot of energy.
- ☐ It prevents later module reuse.

Q2 What is the advantage of knowing the source code with respect to security ?

- ☐ Developers cannot hide backdoors easily.
- ☐ Managers cannot enforce dumb source obfuscation rules for intellectual property reasons.
- ☐ Everyone knows where to find the maintenance password easily: in the code. And they proofread the C code at the same time. (BTW, security paranoiacs can even change it.)
- ☐ The final user can double check alleged properties himself (and even find new ones).
- ☐ You can recompile the program with different security or optimization options.

Q3 Which one is not a security requirement ?

- ☐ User authentication.
- ☐ Production cost evaluation.
- ☐ Network compartmentalization.
- ☐ Delayed precise location disclosure.
- ☐ Contract digital signature.

Q4 What is the best way to check user input?

- ☐ Sanitize it by removing jargon words.
- ☐ Remove special characters.
- ☐ Ensure that numeric variables are within a given interval.
- ☐ Parse the input completely.
- ☐ Only offer 6-buttons user interfaces like in the NASA designs.

Q5 What is one of the main problem point between CI/CD (continuous integration / continuous development) and classical security deployment procedures ?

- ☐ Only chaotic white panthers can manage the resulting chaos.
- ☐ Security updates occur all the time, nearly continuously.
- ☐ The security level changes all the time.
- ☐ Classical security validation procedures at delivery cannot be used effectively.
- ☐ The security kernel responsible for security updates needs to be developed first.

Q6 What CPU/hardware feature does *not* help with respect to security ?

- ☐ Memory protection.
- ☐ Branch prediction.
- ☐ NX (no-execute) access right.
- ☐ Memory barriers.

Q7 Which of these aspects of system hardware is associated to a *covert* channel (NB: different from an auxiliary channel)?

- ☐ The noise of CPU fan.
- ☐ The energy consumption.
- ☐ Branch prediction logic.
- ☐ A shared communication bus with shared storage.

Q8 Which physical random number generator sounds secure to you?

- ☐ A 5 years old child smashing the keyboard.
- ☐ Low level bits of audio recording samples.
- ☐ Low level bits of a thermal sensor measurements.
- ☐ Low level bits of a Geiger sensor monitoring artificial radioactivity.
- ☐ A whole class of students trying to answer to a negatively formulated questionnaire.

Q9 Which one is an authentication protocol ?

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

Q10 How can you protect a component from EM interference (in the real world) ?

- ☐ By introducing thermal noise.
- ☐ By shielding with lots of lead (Pb).
- ☐ Using a 1Tesla protection field.
- ☐ With a Faraday cage.

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

Give an example of a security objective (i.e. a requirement) corresponding to several types of embedded systems:

- a military plane flight control computer

- a bike for rent

- a pace maker (heart stimulator)

Question 2

Consider a live videoconferencing application allowing the passengers of cars *of a given manufacturer only* to communicate freely with each others (via a manufacturer controlled infrastructure) while traveling on roads.

Consider the manufacturer is based in Borduria, which country seems dominated by a semi totalitarian and belligerent government.

Propose 6 security objectives for this system (among all the imaginable ones).

2 of them corresponding to the needs of the passengers of the cars:

2 of them corresponding to the needs of the manufacturer of the cars:

And the 2 others to the needs of the government of Syldavia (Borduria historical rival) :

Question 3

Propose a comparison of CBC and ECB modes of operation for an encrypted communication channel (at least 2 advantages and 2 drawbacks of each option).

Question 4

Propose 3 basic programming rules in C with the objective of protecting primarily system *integrity,* against malicious faults of course.

Question 5

Explain the advantages and drawbacks of enforcing a company acquisition policy where only ISO15408 (common criteria) certified IT systems can be bought.