ISAE Embedded systems master

Evaluation – Exercices and questions

27 february 2018

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 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 right one.

Attention, the following notation system will be used :

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

Q1 Which of the following properties is ***not*** related to computer security?

- ☐ Confidentiality.
- ☐ Reliability.
- ☐ Availability.
- ☐ Accountability.

Q2 Which of the following faults is specifically related to the type considered in security?

- ☐ Lightning strike.
- ☐ Solar eruption EM burst.
- ☐ Dog bite.
- ☐ Car robbery.
- ☐ Programming bug.

Q3 Which of these algorithms is a symetric encryption algorithm?

- ☐ Quicksort
- ☐ RSA
- ☐ SHA-3
- ☐ DES

Q4 Which of these algorithms is useless to implement a secure communication protocol?

- ☐ AES
- ☐ RC4
- ☐ SHA-256
- ☐ 3DES

Q5 Which attack class is associated to power analysis?

- ☐ covert channel usage
- ☐ buffer overflow exploitation
- ☐ auxiliary channel monitoring
- ☐ substrate deconstruction
- ☐ eavesdropping

Q6 What is the key advantage of security software updates?

- ☐ They allow to remove attackers from compromised systems.
- ☐ Their deployment is inexpensive.
- ☐ They are totally inocous when done as fast as possible.
- ☐ They discharge the manufacturer from most visible liability.
- ☐ They avoid the headaches of security programming rules definition.

Q7 What is the best way to add conditional parameters (like #define, #if/#else, etc.) to a configuration file?

- ☐ Implement a parser capable of analysis a full Turing-machine capable language.
- ☐ Carefully isolate the lines containing #labeled keywords.
- ☐ Pre-backslash all special characters in the configuration file prior to analysis.
- ☐ Delegate the preprocessing management to the C preprocessor and treat the result as a configuration file.

Q8 At which step of the application development phase is it most cheap to consider the integration of security functions:

- ☐ In the application design phase.
- ☐ At system disposal.
- ☐ During executives summer holidays.
- ☐ At the validation phase (just before production go).
- ☐ Via operating system updates.

Q9 Which area of the stack is especially useful for an attacker to overwrite when implementing a buffer overflow?

- ☐ FP the frame pointer
- ☐ SP the stack pointer
- ☐ sfp the saved frame pointer
- ☐ retval : the CPU return address
- ☐ argX : the arguments of the called function

Q10 Which habilitation is allowed to access a document of security classication (SECRET, {SPACE, LOGISTICS, PRICE}) under the Bell-La Padula security policy (and the natural ordering of labels) :

- ☐ (TOP SECRET, { GOVERNEMENT, SALARIES })
- ☐ (CONFIDENTIAL, { SPACE, TECHNICAL, ENGINE})
- ☐ (PUBLIC, {AIR FORCE})
- ☐ (SECRET, { GOVERNMENT, AIR FORCE, LOGISTICS, PRICE})
- ☐ (SECRET, { SPACE, LOGISTICS, LOX, FUEL, GAS, ROADSTER, BOWIE'S CD, PRICE})

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.

Advice : do not hesitate to use draft papers to prepare your answer(s) separately.

Question 1

Give 4 examples of security rules applicable to informations systems (*at least* one in each of the hardware, software and organizational category).

Question 2

Consider an automatic autonomous driverless shuttle designed to cover short distances on predefined routes (at rather low speeds) in an urban environment and transport up to 8 passengers.

Propose 4 security objectives for this system (among all the imaginable ones).

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

And the 2 others to the needs of the passengers of the shuttle :

Question 3

Describe 2 different ways of abusing the security of a system providing a mandatory multilevel confidentiality security policy (BLP).

Question 4

In the spirit of the ITSEM guidelines, propose *tentatively* several scales and levels to evaluate the strength of a security mechanism in the aeronautical domain.

Question 5

Explain the advantages and drawbacks of reporting a technical vulnerability to a national CERT (as opposed to, for example, Twitter, your boss, the local mafia, the local lawyers or the manufacturer).