ISAE Embedded systems master

Evaluation – Exercices and questions – WITH CORRECTION

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.

Answers are shown in green highlighting or given tentatively in italics, but without any guarantee for applicability for any real life purpose without much further (certainly costly[1]) review.

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.

[1] *Especially with respect to Question 4.*

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).

(hardware/physical) All sensitive RDMBS data storage should reside in room 1234.

(hardware) No american-designed CPU should be used on our ICMBs. (Good luck btw.)

(software) No call to fprintf() should be made without a format string.

(software) All software should rely on the company LDAP system for authenticating its users.

(software) All embedded software should comply to CERT Secure Coding Standards

(organizational) No personal password should be asked or given to a 3rd party (outside of computer security officers ***of course***[2]*).*

(organizational) No executable program should be sent by unsigned email. (Good luck again)

(organizational) All users accessing banking applications should be given explicit nominative delegation from the CFO (Chief Financial Officer).

[2] *After 10 years, still trying to have at least one user trust me on that...*

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 :

No user should be able to drive the shuttle from his/her own smartphone.

Police force should be allowed to move the shuttle by 10m on its path.

It should not be possible to copy the shuttle software source code.

All operation logs for the last 30 days should be available.

No passenger-related logs should be kept longer than permitted by law (except for logs already indefinitely isolated by a specific search warrant).

The bill of the shuttle should be paid.

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

No passenger should be killed by the shuttle.

The shuttle should not charge a transaction illegitimately.

The shuttle logs should not hold logs of the passenger transit if he/she does not want to (unless necessary for transportation).

The shuttle equipment should not allow spying in the vehicle without notice.

No (other) user should be able to drive the shuttle from his/her own smartphone.

Question 3

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

Two users at different security levels may try to communicate information contrarily to the policy mandatory rules using a covert channel.

A low clearance user may produce a lot of high classification (useless) data in order to saturate the system (storage).

You can try generic attacks still applicable to systems applying mandatory policies:

- *eavesdrop on the system using e.g. EM monitoring;*
- *"guess" users passwords to steal their identity or "guess" encryption keys to monitor traffic.*

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.

NB: This question was the most difficult of the entire exam. Applicants should have wisely tried to answer it last.

Opportunity could for example be split among:

- *collusion in flight: pilot, crew, passenger, none.*
- *collusion on ground: manufacturer, supplier, maintenance, airport, airline, none.*

Equipment could be refined more specifically to take into account the domain parts: unaided, domestic equipment, standard aircraft part, special equipment.

If implementing an attack depend on resources associated to software systems, those resources could be split between the various levels defined by DO-178C according to the software criticity level: A, B, C, D or E. (Though this scale is not necessarily linked to security constraints.)

*Expertise may be given more dimensions (not necessarily more levels as the 3 steps division between layman, proficient and expert is not so easy to improve) in the directions of:**

- *aircraft expertise;*
- *traffic control expertise;*
- *airport expertise;*
- *airline operation expertise (including aircraft maintenance).*

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).

Advantages:

You will be officially and indefinitely granted the appropriate fame for discovery.

You will be protected from potential manufacturer abusive actions (especially if the CERT manages the disclosure process).

You will in the end help people being protected from potential abuses.

Your work will be thoroughly checked technically.

You may benefit from corrections very early.

Drawbacks:

You may lose the exclusivity to the vulnerability discovery (if someone else reports it to the CERT network in the same time frame).

You may be asked to delay public disclosure to give some time to the manufacturers or some national bodies to do some things.

You will be only 1 vulnerability among the thousands discovered every year.

You will probably not gain much money from the report.

You will not be able to harm vulnerable systems yourself. (Obviously this is a drawback from a pure material girl/boy point of view – not the moral one.)