ISAE Embedded systems master

**Evaluation – Exercises and questions**

4 mars 2019

# 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 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** Which of the following faults is related to those considered in **safety**?

□ 2019 superball finals playback failure on in-flight entertainment system.

□ Car robbery.

□ Exam results tampering.

□ Non functioning plane fuel gauge.

□ Car flat tire.

**Q2** Which of the following data destruction technique is seriously **unsecure** (for conventional hard drive storage) ? NB: Do not try any of those without adequate protection.

- □ 64 passes Mersenne twister overwrite.
- □ Plasma torch melting (~10000°K).
- □ Insertion into a tree cutter (<4 cm$^3$ grid).
- □ Low level logical repartitioning.
- □ Compression by a steam roller (25 to 27 t) on hard floor.

**Q3** Which type of security vulnerability is *not* a bug?

- □ Buffer overflow.
- □ User-defined permissive access rights.
- □ SQL injection via user names.
- □ Arithmetic overflow.
- □ Format string incorrect parsing.

**Q4** What is the best moment to define the security requirements of an application?

- □ Before the project is even thought of.
- □ At system shut down.
- □ Just before integration testing.
- □ During the functional system requirements elicitation phase.
- □ Before system operational start-up.

**Q5** Which of the following is not a risk reduction strategy?

- □ Additional testing effort.
- □ Project closure.
- □ N-version programming.
- □ Integration of fault-tolerant components.
- □ Code reviews.

**Q6** Why do recent CPUs reveal annoying hardware design faults allowing for side-channel oriented attacks ?

- □ Because of CPU manufacturers lack of control on their fab suppliers.
- □ Because of electromagnetic emissions and the lack of TEMPEST protection.
- □ Because of hardware density and sensitivity to voltage/intensity current surges.
- □ Because it is possible to read the content of CPU internal memories by fast substrate deconstruction near 0°K.
- □ Because multiple levels of caches necessitate the introduction of complex memory barriers instructions that developers do not use.
- □ Because of temporal correlation between speculative execution decision, data loaded by the CPU and threads unauthorized to access the data.

**Q7** What is the typical activity set as an exception in the prologue of *Regulation (EU) 2016/679 on the protection of naturals persons with regard to the processing of personal data and on the free movement of such data* – and thus, informally, exempt of respecting GDPR :

- □ Apple and watermelon culture
- □ Triple redundant rocket launch
- □ Big data monetization
- □ Health management statistics
- □ National security

**Q8** Which habilitation is needed to access a document of security classication (TOP SECRET, {NAVY, LOGISTICS, BUDGET, FUEL}) under the Bell-La Padula security policy (and the natural ordering of labels) :

- □ (TOP SECRET, { AIR FORCE, SAC, NAVY, BUDGET, NUCLEAR})
- □ (TOP SECRET, { NAVY, LOGISTICS, FUEL, SALARIES, BANKING, BUDGET})
- □ (PUBLIC, {NAVY})
- □ (SECRET, { HEADQUARTERS, SALARIES })
- □ (CONFIDENTIAL, { SPACE, TECHNICAL, ENGINE})

**Q9** What is the security assurance needed to reach the most secure level of the evaluation in normalized evaluation criteria :

□ The ability to select between a discretionary or mandatory security policy at login

□ A formal proof of (a model) of the security kernel functions and its implementation

□ A mandatory security policy based on security levels (associated to objects)

□ A trusted execution path (SysRq).

□ Presidential signature of the certificate.

**Q10** What are you avoiding with a prepared SQL query which has most impact with respect to security?

□ Performance issues.

□ The need to manage runtime execution errors due to malformed query.

□ Potential side effects of user input.

□ Difficulty with application of SQL quality rules (in embedded SQL).

□ The possibility to talk directly with the RDBMS engine via TCP.

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

- a portable music player

*Do not allow end customer uncontrolled copyrighted music redistribution.*

*Control accessible music stores (if local laws permit).*

*Allow low quality free music download.*

*Prevent personal recordings upload.*

*Never, ever, allow teenagers to backslash old music hits. (Oh, no… that one is hard!)*

- a (piece of) rocket landing computer

*Only act on appropriately authenticated self-destruction request(s).*

*Do not accept random landing sites updates.*

*Only accept signed software updates*

*Do not accept software updates in the field.*

*Take appropriate evasive maneuvers against foe missiles and planes (Ouch.*

*Do not try to recover Starman's roadster.*

- an insulin pump

*Never accept out-of-bounds medicine injection quantities. (NB: both safety and security)*

*Do not allow remote monitoring (of one patient private prescriptions).*

*Only accept appropriately signed firmware updates.*

*Do not deliver unidentified medecine.*

*Do not stop pump in case of network unavailability.*

*Do not systematically double Cinderella stepmother somnifere.*

**Question 2**

Consider an imaginary *automatic* software download system for all the systems of a modern plane, using a single VPN tunnel with the manufacturer.

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

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

*Only install and activate a field loadable software associated to a manufacturer-generated signature.*

*Shutdown the system when the plane is out any flying phase.*

*Only setup VPN tunnel encryption with endpoints authentificated with this chief-engineer generated certificate.*

*Perform trafic shaping of VPN content with prioritization of flight-control units over all other units.*

*Record all violations of maintenance access during flight and send them back to the manufacturer.*

*Distribute YouFavoriteDesktopOS security patches to passengers systems of business and first class.*

And the 2 others to the needs of the airports hosting the plane :

*Provide a software download cache with 24 hours period update with local manufacturer signature checking. (Note how such a nice bandwidth saving service could be used as an attack intermediate.)*

*Only accept VPN tunnels data transports originating from airport-controlled enpoints. (Note how this security rule may conflict with one of those above.)*

*Enforce maintenance laptops OS updates to originate from plane manufacturer networks.*

*Only allow plane / manufacturer traffic to function in physically controlled area of the airport and via wired connections.*

*Provide FAA-approved network security guidelines and training to all maintenance personnel.*

**Question 3**

Imagine a regular PC desktop system which boot sequence is protected by a TPM. (This is the single major security measure.) Identify and explain 2 advantages and 2 drawbacks of this kind of protection (setup naturally for this kind of mechanism).

*Advantages:*

*Direct hard disk tampering is impossible (TPM boot signature checking would detect it).*

*Firmware (BIOS) tampering is detected similarly.*

*It is usually possible to enforce integrity checks of logging functions (and traces).*

*Cryptographic key protection can be done using TPM mediation.*

*Standardized solution.*

*Drawbacks:*

*All system updates necessitate re-signing of TPM controlled modified files before reboot (or risk reboot failure).*

*User-downloaded programs are out of the scope of TPM protection.*

*TP-based crypto may be less flexible (esp. from the point of view of a developer).*

*Master TPM key loss leads to full OS software freeze.*

*Core security root was generated at TPM manufacturer location.*

*Necessitate a TPM-aware boot loader*

*Necessitate a TPM-aware operating system.*

**Question 4**

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

*Only use dynamic memory allocation in the system start-up phase. (Define program start-up phase).*

*Perform WCET analysis of all functions.*

*Throttle specific input buffer usage depending on the number of input errors (spend less time on erroneous channels).*

*Check function termination.*

**Question 5**

Explain the advantages and drawbacks of a company organization with IT auditors totally independent from the operational IT department.

*Advantages:*

*Fully transparent audit/assessment procedures and results.*

*Totally independent (externally receivable) opinion.*

*Less manipulable from the IT side.*

*Drawback:*

*Unable to participate to solutions implementations.*

*Intrusive and potentially infrequent diagnosis.*

*More manipulable from the out-of-IT side.*