ISAE Embedded systems master

Evaluation – Exercices and questions

7 february 2017

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 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 What are currently the most efficient incentives for top level management with respect to security?

- ☐ Legal or regulatory constraints.
- ☐ Consumer demand.
- ☐ Economical constraints.
- ☐ Company reputation.

Q2 Which of these algorithms may benefit from a public key directory ?

- ☐ AES
- ☐ RSA
- ☐ SHA-3
- ☐ DES

Q3 What is the security development method needed to reach the highest evaluation levels in normalized evaluation criteria :

- ☐ A trusted execution path (SysRq).
- ☐ The abilitiy to select between a discretionay or mandatory security policy at login
- ☐ A formal proof of (a model) of the security kernel functions and its implementation
- ☐ Presidential signature on the certificate.

Q4 Error codes must always be checked after calling a library function because :

- ☐ most programming books recommend them ;
- ☐ all software developpers do that all the time ;
- ☐ it will prevent the program from crashing ;
- ☐ it is the only way of preventing abuse of API misuse interactions.

Q5 Which step of the application development phase is quasi systematically omitted even from security-oriented computer software development :

- ☐ Test funding.
- ☐ End-user security need.
- ☐ Data disposal.
- ☐ Developper holiday.
- ☐ Authentication delegation.

Q6 What is the methodological information provided by a CERT/CC (Computer Emergency Response Team) ?

- ☐ Examples of awareness raising documents for internal communication toward employees
- ☐ Career development guidelines for computer security officers
- ☐ Secure software development rules for various programming languages
- ☐ Secure contract rules for export control conformance

Q7 Given that the total number of atoms in the universe is usually estimated around 10^82, what is the incentive for selecting a 2^256 bit key length instead of a 2^128 bits key length for AES :

- ☐ Because, you never know, your adversary may have access to several universes to attack you.
- ☐ Because someone may already have broken the 2^128 bit key length version but not the extended one.
- ☐ Because you can and the additional energy cost is marginal.
- ☐ Because it will cost more and motivate the development of commercial encryption devices.

Q8 Which habilitation is allowed to access a document of security classication (CONFIDENTIAL, {NAVY, TECHNICAL, RADAR}) under the Bell-La Padula security policy (and the natural ordering of labels) :

- ☐ (TOP SECRET, { AIR FORCE, SALARIES })
- ☐ (SECRET, { NAVY, TECHNICAL, ENGINE})
- ☐ (PUBLIC, {NAVY})
- ☐ (CONFIDENTIAL, { NAVY, AIR FORCE, TECHNICAL, LOGISTICS, RADAR, SONAR})
- ☐ (CONFIDENTIAL, { NAVY, AIR FORCE, LOGISTICS, RADAR, SONAR})

Q9 Before a competitive exam, the computer on which all results are to be consolidated and sorted is locked in a glass walled room visible by everyone, the programs to run are audited and checked and the official publication place of the results is decided and announced to the candidates. This kind of procedure is related to :

- ☐ confidentiality
- ☐ integrity
- ☐ availability
- ☐ or *survivability*

Q10 In the above configuration, the easiest avenue for an attacker (the residual vulnerability) to disrupt and discredit the whole exam is :

- ☐ by intercepting and altering the commmunication channel between the computer and the publication medium to display funny results.
- ☐ by studying very hard to rank first in the competitive exam and then publicly despising how « easy it was ».
- ☐ by breaking into the computer room and stealing the computer.
- ☐ by intercepting and altering correction reports from professors.
- ☐ by intercepting exam questions and selectively leaking them to a significant fraction (e.g. 15%) of the candidates (but not all).

Q11 In a networked sensors system relying on the Biba multilevel mandatory integrity policy, is it possible that a low integrity level CPU uses a high integrity sensor output in order to perform a computation ?

- ☐ YES
- ☐ NO

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

Consider an automatic drone delivery system (for conventional goods). Propose 4 security objectives of this system.

2 of them corresponding to the needs of the distributor using the delivery system :

And the 2 others to the needs of the end customer of the delivery system :

Question 2

Propose 4 programming rules for enhancing the security of a C software development project.

Question 3

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

Question 4

Give examples of the 4 different approaches to risk management :

Risk avoidance

Risk reduction

Risk acceptance

Risk transfer

Question 5

Here are several ideas for entirely removing buffer overflow problems. Discuss their adequacy (do they work) and applicability (do they sound realistic).

Do not use function calls, but only coroutines (aka. jumps).

Change the CPU architecture to have a (second) separate stack for storing return adresses.

Make the stack non-executable and more generally prohibits self-modifying code.