ISAE Embedded systems master

Evaluation – Exercises and questions

30 march 2023

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 What is the moment in a software development project to consider intrusion testing?

- ☐ Before emergence of the project idea.
- ☐ After each project sprint.
- ☐ After the first payment.
- ☐ At any time during operational life.
- ☐ After your country governmental agency informs you that they have done one.

Q2 CRC codes are sometimes associated to transmitted data in order to allow detection of accidental alteration of binary data. Why cannot they be used for securing the integrity of the same data?

- ☐ Because they are too short and cannot be extended easily in size.
- ☐ Because their security has not been validated.
- ☐ Because they are linear codes and hence amenable to inversion.
- ☐ Because you would have to transmit the CRC separately from data to prevent the attacker from also tampering the checksum.

Q3 Which case is an example of a logical backdoor?

- ☐ The rear garden door.
- ☐ A malicious program sent by mail mimicking a small fun tic tac toe game
- ☐ A magical test keys sequence that lets an ATM expel one bank note.
- ☐ An SQL script destroying the company databases if a specific employee contract is terminated (UNLESS current_year > BIRTH_DATE+42).

Q4 Which attribute (of dependability) can be associated to security main attributes?

- ☐ Maintainability.
- ☐ Availability.
- ☐ Anonymity.
- ☐ Price.
- ☐ Security updates.

Q8 Here is a small snippet of C code, where variables have their natural meaning (`buf` is some buffer space, `src` some internal safe data and `val` some external not-trusted value).

```
if (val * 4 > sizeof(buf) ||
    val > UINT_MAX / 4)
        return -EINVAL;
memcpy(buf, src, val * 4);
```

The above piece of C code is :

- ☐ Incorrect.
- ☐ Inefficient because untrusted values checking should be done at the call site.
- ☐ Correct.
- ☐ Correct but written in the wrong order.

Q5 What is the main limitation of using a symmetric encryption algorithm in a digital signature scheme ?

- ☐ It is mandatory to encrypt the document in order to get a signature.
- ☐ Signatures are not useful in front of a third party as both parties can sign whatever version of the document they claim to be original.
- ☐ You cannot detach the signature from the document.
- ☐ It could be much slower than a public/private key signing system.

Q6 Why is it impossible to trust a single private key to provide adequate integrity protection?

- ☐ Because prime numbers factorization is gonna improve a lot with quantum computers.
- ☐ Because perfect security does not exist and you can always guess the key.
- ☐ Because you cannot be sure that the public key associated to the private key is actually associated to the good recipient (unless you trust the public key directory).
- ☐ Because you only have the public key to check the integrity verification and can only encrypt with it.

Q7 Which of these parts of system hardware is most vulnerable to blunt magnetic reads?

- ☐ The CPU fan.
- ☐ The motherboard .
- ☐ The hard disk.
- ☐ The FDDI channel.

Q9 Which one is a secure hash algorithm ?

- ☐ Diffie-Hellman
- ☐ Rijndael
- ☐ SHA-3
- ☐ UDP
- ☐ HTTP

Q10 How can you realistically protect a component from electromagnetic monitoring?

- ☐ By eliminating covert channels.
- ☐ By heavy shielding (of memory and logic) with 20mm strainless steel.
- ☐ With a Faraday cage.
- ☐ By a strong electromagnetic field.

Part II (10 pts)

This part is composed of four open questions (2.5 pts each). Please write down your answer *on this document* in the appropriate space.

Question 1

Consider an embedded web server inside the computer of an automotive. We assume this computer is not associated directly to any critical function of the vehicle (like speed or attitude control); but otherwise participates to any other function used by the vehicles users (navigation, entertainment, route planning, maintenance, networking, etc.) Wireless communication systems allow this computer to be connected to the Internet but with typical perturbations of a moving car (temporary loss of connectivity, limited bandwidth, etc.).

Propose 2 security objectives for this system (among all the imaginable ones), from the point of view of the car manufacturer.

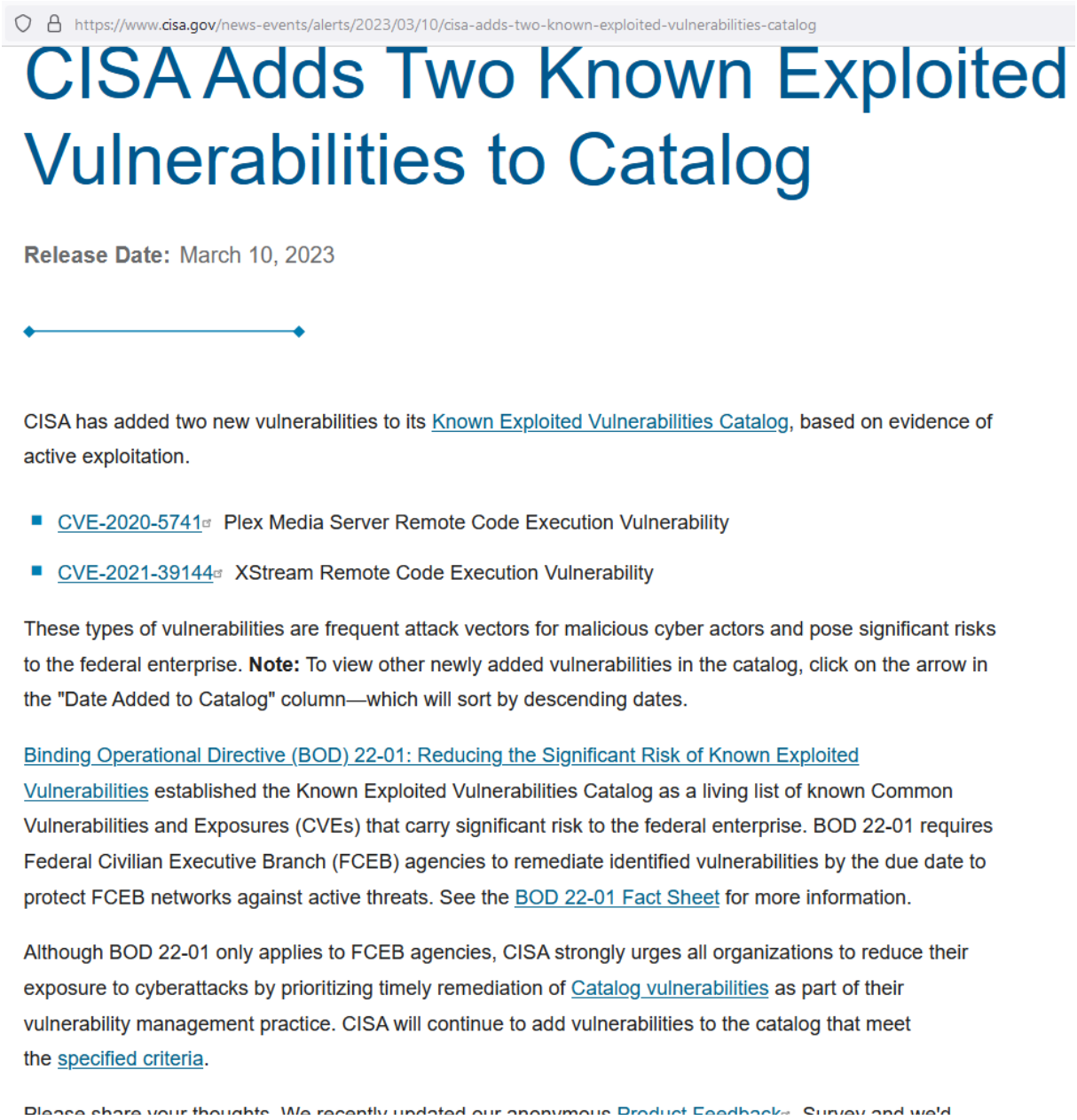
Identify two additional security objectives for this system (among all the imaginable ones), from the point of view of the car *owner.*

Try to imagine a situation where the car owner and the car manufacturer would have contradictory security expectations.

Question 2

Propose 4 security requirements associated to the development environment (editor, compiler, testing framework, version management system, software distribution) of a software company.

Question 3



https://www.cisa.gov/news-events/alerts/2023/03/10/cisa-adds-two-known-exploited-vulnerabilities-catalog

CISA Adds Two Known Exploited Vulnerabilities to Catalog

Release Date: March 10, 2023

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

- CVE-2020-5741 Plex Media Server Remote Code Execution Vulnerability
- CVE-2021-39144 XStream Remote Code Execution Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. **Note:** To view other newly added vulnerabilities in the catalog, click on the arrow in the "Date Added to Catalog" column—which will sort by descending dates.

Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the Known Exploited Vulnerabilities Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for more information.

Although BOD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria.

Please share your thoughts. We recently updated our anonymous Product Feedback Survey and we'd

Study the above news alert published on an official web site of the US government, the one of the Cybersecurity & Infrastructure Security Agency (CISA, "America's Cyber Defense Agency").

1) How do you know (simply) this is an official website of the US government ?

2) Which procedure and computer security management approach can you infer for the organization of US governmental agencies from the analysis of this alert ?

3) As private company *contractor* of the US government, how would you organize security management in your organization with respect to this policy (both from the cost-efficiency and customer satisfaction point of views) ?

Question 4

You are tasked with proposing a secure software distribution mechanism for an experimental Unix-like operating system by a research & education academic project. Propose an overall system for such a task by outlining the design principles and the target properties.

In a second step, you are hired by a high profile aerospace civilian manufacturer that would like to reuse your system for onboard software updates of embedded systems on operational planes.

Discuss the difficulties in reusing your system in this context ? Do you think some workarounds are feasible (or some weaknesses acceptable) ?