M2 CyberSecurity 2018-2019

Physical Security (WMM9SY05)

Hardware and Embedded Systems

Paolo MAISTRI, Ioana VATAJELU, David Hély

No documents allowed

About 50 minutes

LAST NAME / NOM :

FIRST NAME / PRENOM :

1. Why is security in embedded system important? Cite a few domains where embedded systems should be secured, and describe at least an example of an embedded system that was compromised.

2. Describe a countermeasure against side channel attacks that can be applied at architectural level

3. AES can be vulnerable to fault attacks. Describe briefly how Differential Fault Analysis can allow recovering the secret key, and suggest a (few) countermeasure(s) that could be adopted. Which are the pros and againsts of the solution you proposed?

4. What is the purpose of Built-In Self Test (BIST) techniques? How can they be useful in a secure cryptographic hardware implementation?

5. Please describe the untrusted electronic device supply chain and explain which are the main device counterfeiting types. Please provide a brief description (definition) of each counterfeit method.

6. Give two hardware features which can thwart return oriented programming attacks. Justify your answer.

7. What are the limitations of debug access protection based on Trustzone? Justify your answer.