M2 CyberSecurity 2017-2018

Physical Security GBX9SY05 - Hardware and Embedded Systems

Paolo MAISTRI, Ioana VATAJELU

No documents allowed

50 minutes

Questions

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 RTL (Register Transfer Level)
3. Describe how you would choose an Error Detecting Code to protect a public-key cryptosystem from fault attacks, and why.
4. Describe the pipeline redundancy technique, used against fault attacks. Which are the advantages/disadvantages of this technique?
5. Explain what is a Physically Unclonable Function and which are its characteristics.
6. Why the “split manufacturing” technique can prevent the insertion of Hardware Trojan Horses?