Video 5: Cyber Arms Race

Alexandre Bartel

The report should consist of a single pdf file. Send the report to

alexandre.bartel@uni.lu

with the following subject:

`MICS2019SVEM Video 5 FIRSTNAME_LASTNAME`

The deadline is the 7^{th} of April 2019 at 23:59.

Maximum 3 sentences per answer. Total points: 50 P.

1 Video 1 : Brain

Watch the video *"Brain: Searching for the first PC virus in Pakistan"* available here. Duration: ≈ 10 minutes.

Question 1.1 Who is Mikko Hypponen? 2 P.

Question 1.2 Who did he visit in 2011? 2 P.

Question 1.3 For which operating system was the virus writen? 2 P.

Question 1.4 How did the virus propagate? 2 P.

Question 1.5 Why did they wrote the virus? 2 P.

2 Video 2 : Cyber Arms Race

Watch the video *"Mikko Hypponen - 'Cyber Arms Race' at Les Assises de la Sécurité et des Systèmes d'Information 2018"* available here. Duration: ≈ 45 minutes.

Question 2.1 What is Stuxnet? 2 P.

Question 2.2 Why is there a before and an after Stuxnet? 2 P.

Question 2.3 When was Stuxnet discovered and analyzed? 2 P.

Question 2.4 How many zero-days did Stuxnet contain? 2 P.

Question 2.5 How did Stuxnet know it is running in the ”target” environment? 2 P.

Question 2.6 Why are governments, intelligence agencies and the militaries interested in offensive use of cyber power? 2 P.

Question 2.7 How could one know the configuration of the nuclear power plant? 2 P.

Question 2.8 Is using Stuxnet a cyber-war? Why or why not? 2 P.

Question 2.9 How was Petya propagated to infect computers? 2 P.

Question 2.10 Why have non-ukranian companies also been affected by Petya? 2 P.

Question 2.11 How did Maersk recovered from the lost of the authentication servers? 2 P.

Question 2.12 What is the most expensive computer incident in history? 2 P.

Question 2.13 What is the average time for a company to detect is has been breached? 2 P.

Question 2.14 What to do when the network (the safe) has been breached? 2 P.

Question 2.15 What is Hypponen's Law? 2 P.

Question 2.16 How did the attackers get access to the credit card terminals? 2 P.

Question 2.17 Why do recent botnets such as Mirai infect IoT devices? 2 P.

Question 2.18 We know how to patch computer systems. But how can we ”patch” people? 2 P.

Question 2.19 Why is there job security in security? 2 P.

Question 2.20 Do you agree with the pessimistic view that all smart devices are vulnerable? 2 P.

Note on plagiarism

Plagiarism is the misrepresentation of the work of another as your own. It is a serious infraction. Instances of plagiarism or any other cheating will at the very least result in failure of this course. To avoid plagiarism, always cite the source from which you obtained the text.