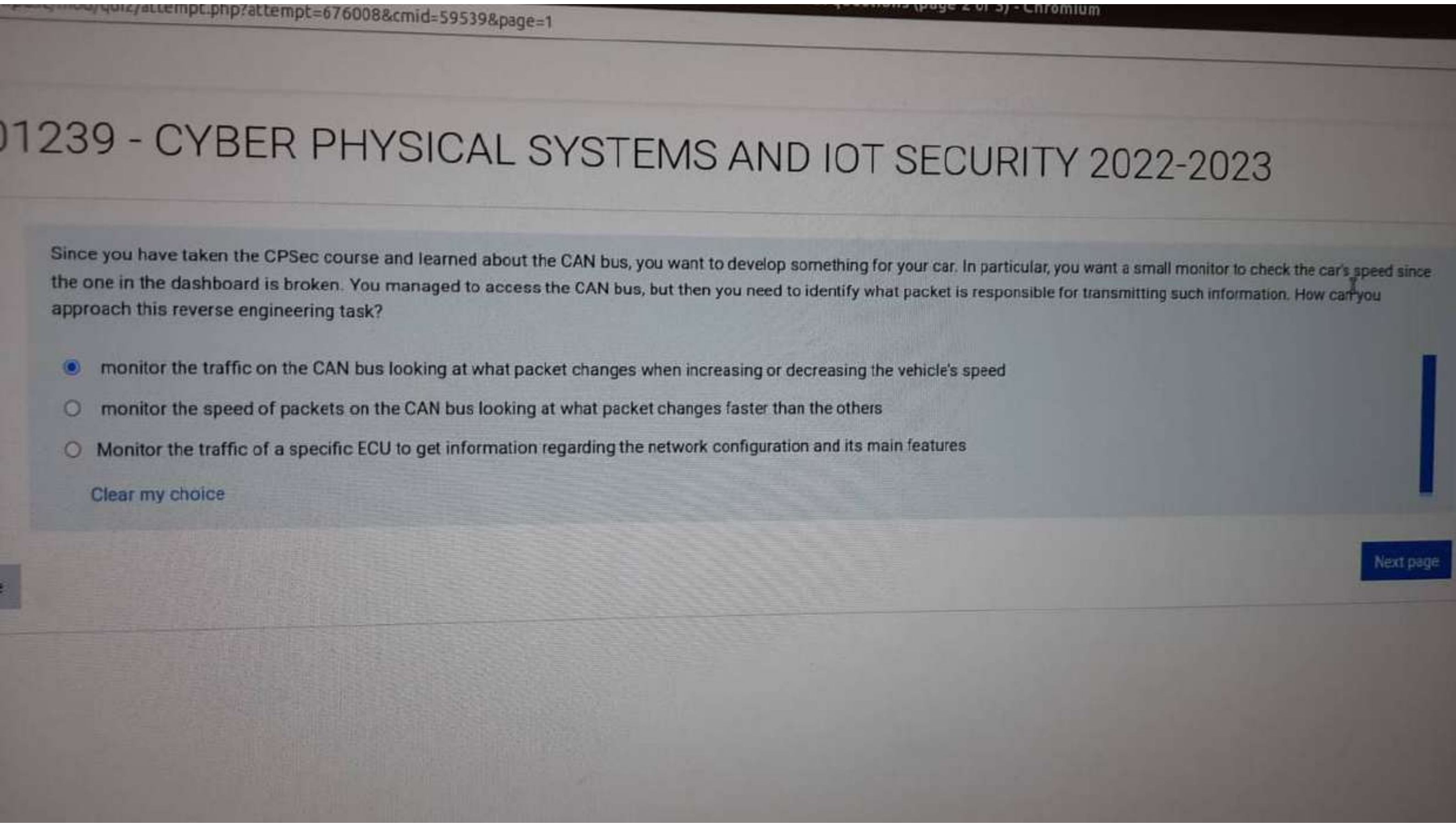


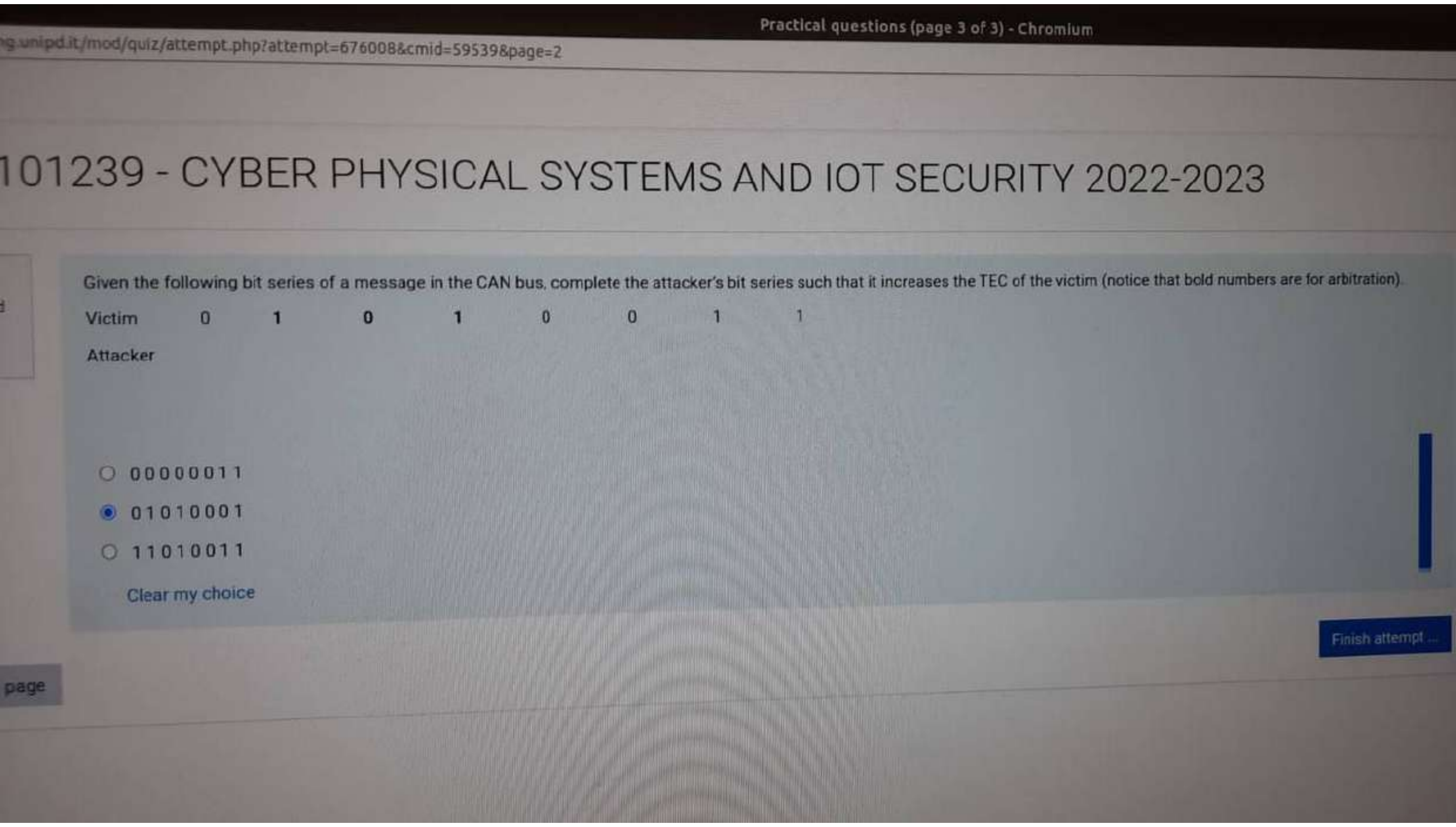
quiz/attempt.php?attempt=676008&cmid=59539&page=1

(page 2 of 3) - Chromium

1239 - CYBER PHYSICAL SYSTEMS AND IOT SECURITY 2022-2023

Since you have taken the CPSec course and learned about the CAN bus, you want to develop something for your car. In particular, you want a small monitor to check the car's speed since the one in the dashboard is broken. You managed to access the CAN bus, but then you need to identify what packet is responsible for transmitting such information. How can you approach this reverse engineering task?

- ● monitor the traffic on the CAN bus looking at what packet changes when increasing or decreasing the vehicle's speed
- ○ monitor the speed of packets on the CAN bus looking at what packet changes faster than the others
- ○ Monitor the traffic of a specific ECU to get information regarding the network configuration and its main features



Practical questions (page 3 of 3) - Chromium
ng.unipd.it/mod/quiz/attempt.php?attempt=676008&cmid=59539&page=2
Clear my choice
Finish attempt ...
page

101239 - CYBER PHYSICAL SYSTEMS AND IOT SECURITY 2022-2023

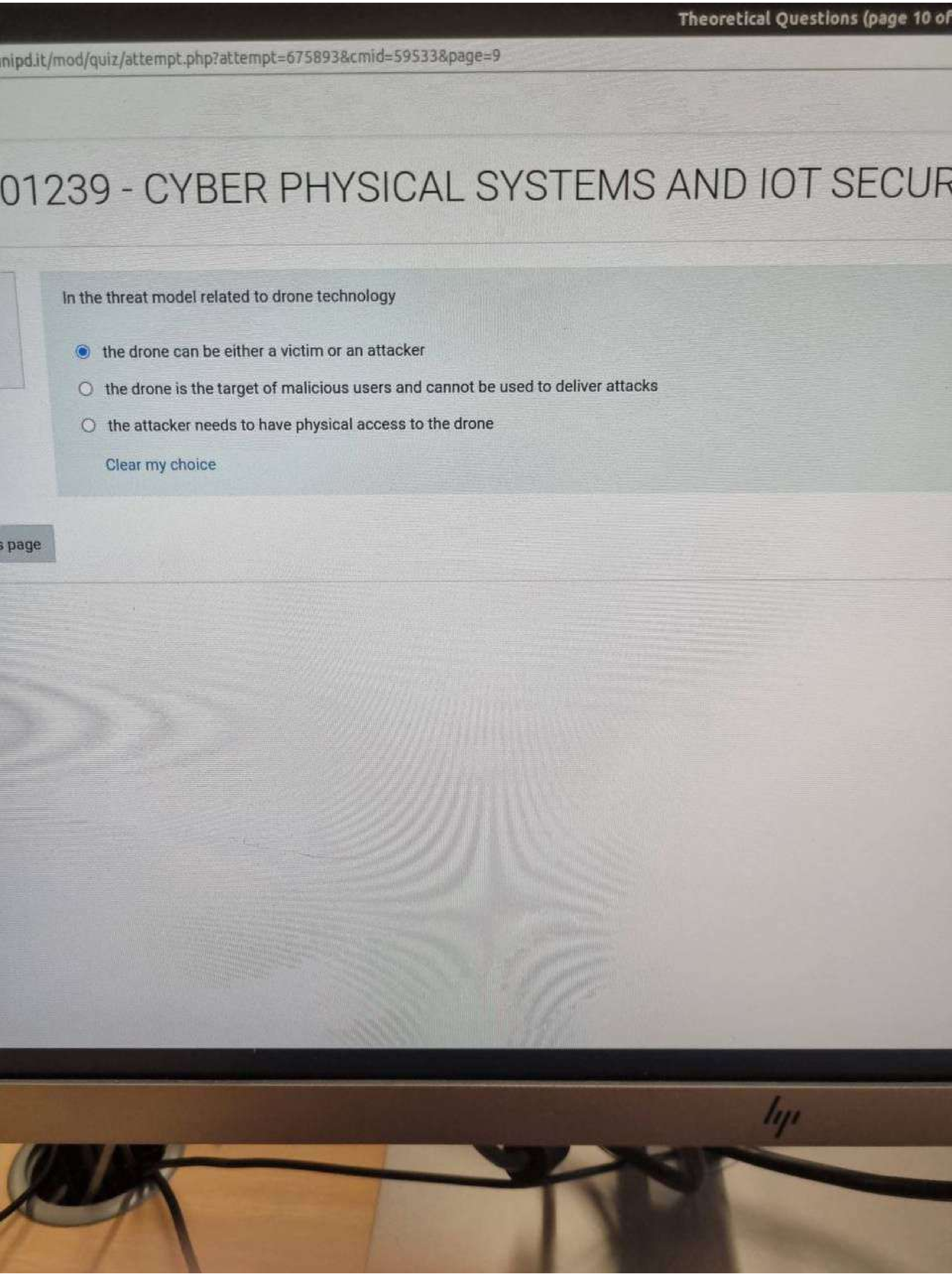
Given the following bit series of a message in the CAN bus, complete the attacker's bit series such that it increases the TEC of the victim (notice that bold numbers are for arbitration).

Victim	0	**1**	**0**	**1**	0	0	1	1
Attacker								

○ 00000011

● 01010001

○ 11010011



Theoretical Questions (page 10 of

nipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=9

01239 - CYBER PHYSICAL SYSTEMS AND IOT SECUR

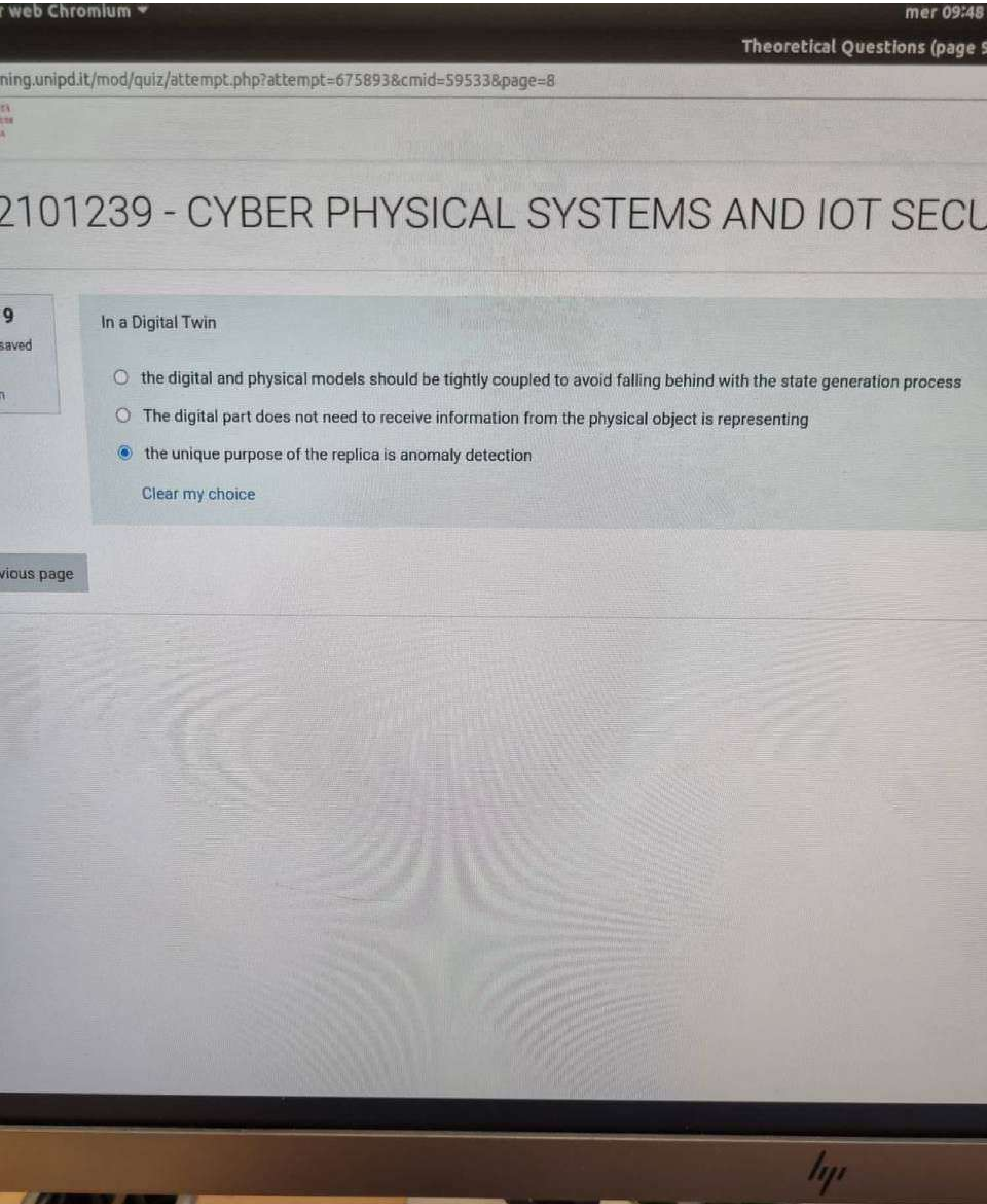
In the threat model related to drone technology

● the drone can be either a victim or an attacker

○ the drone is the target of malicious users and cannot be used to deliver attacks

○ the attacker needs to have physical access to the drone

Clear my choice



web Chromium ▾
mer 09:48
Theoretical Questions (page 9
ning.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=8

2101239 - CYBER PHYSICAL SYSTEMS AND IOT SECU

9

saved

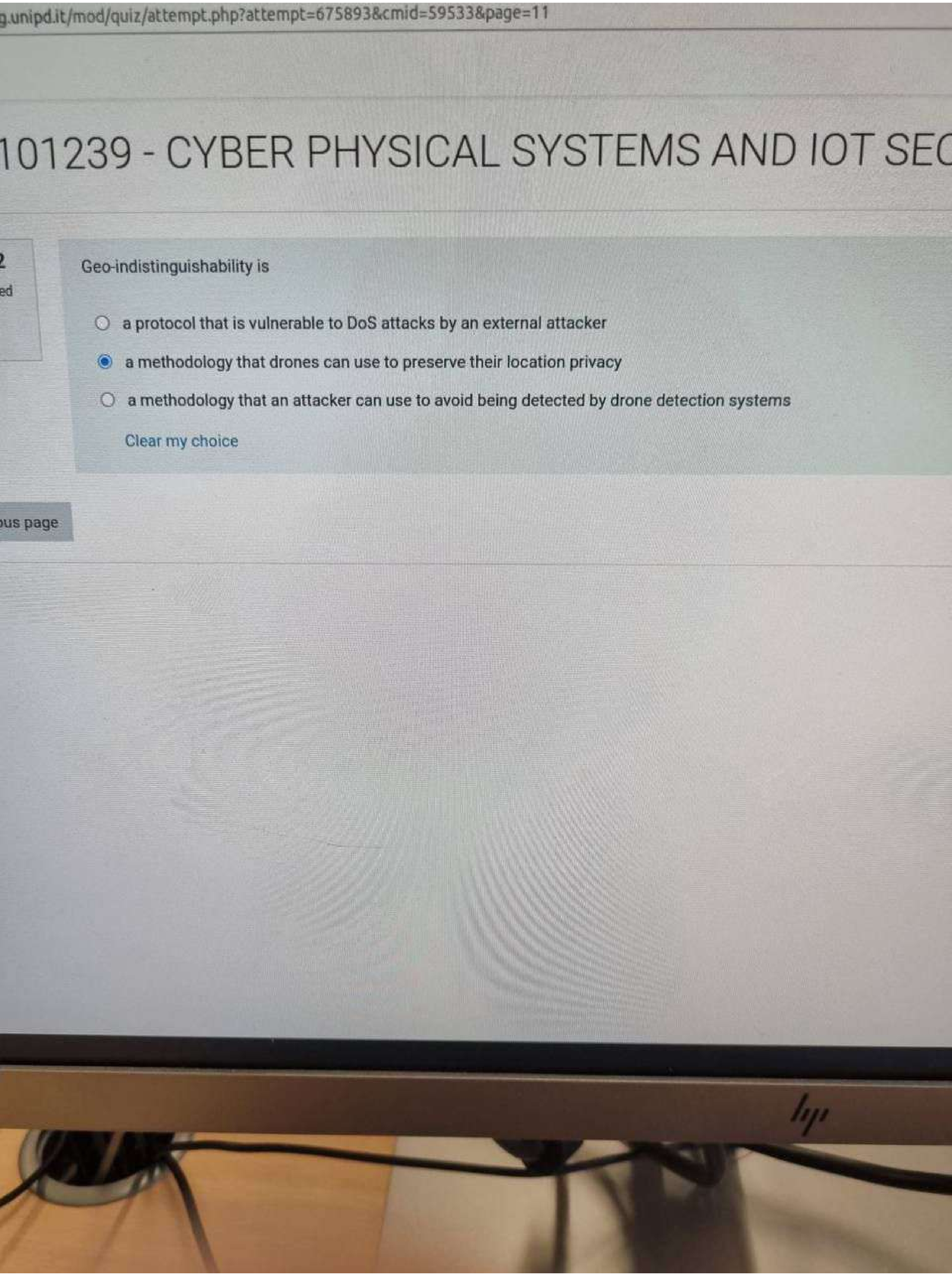
In a Digital Twin

○ the digital and physical models should be tightly coupled to avoid falling behind with the state generation process

○ The digital part does not need to receive information from the physical object is representing

● the unique purpose of the replica is anomaly detection

Clear my choice



g.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=11

101239 - CYBER PHYSICAL SYSTEMS AND IOT SEC

2

ed

Geo-indistinguishability is

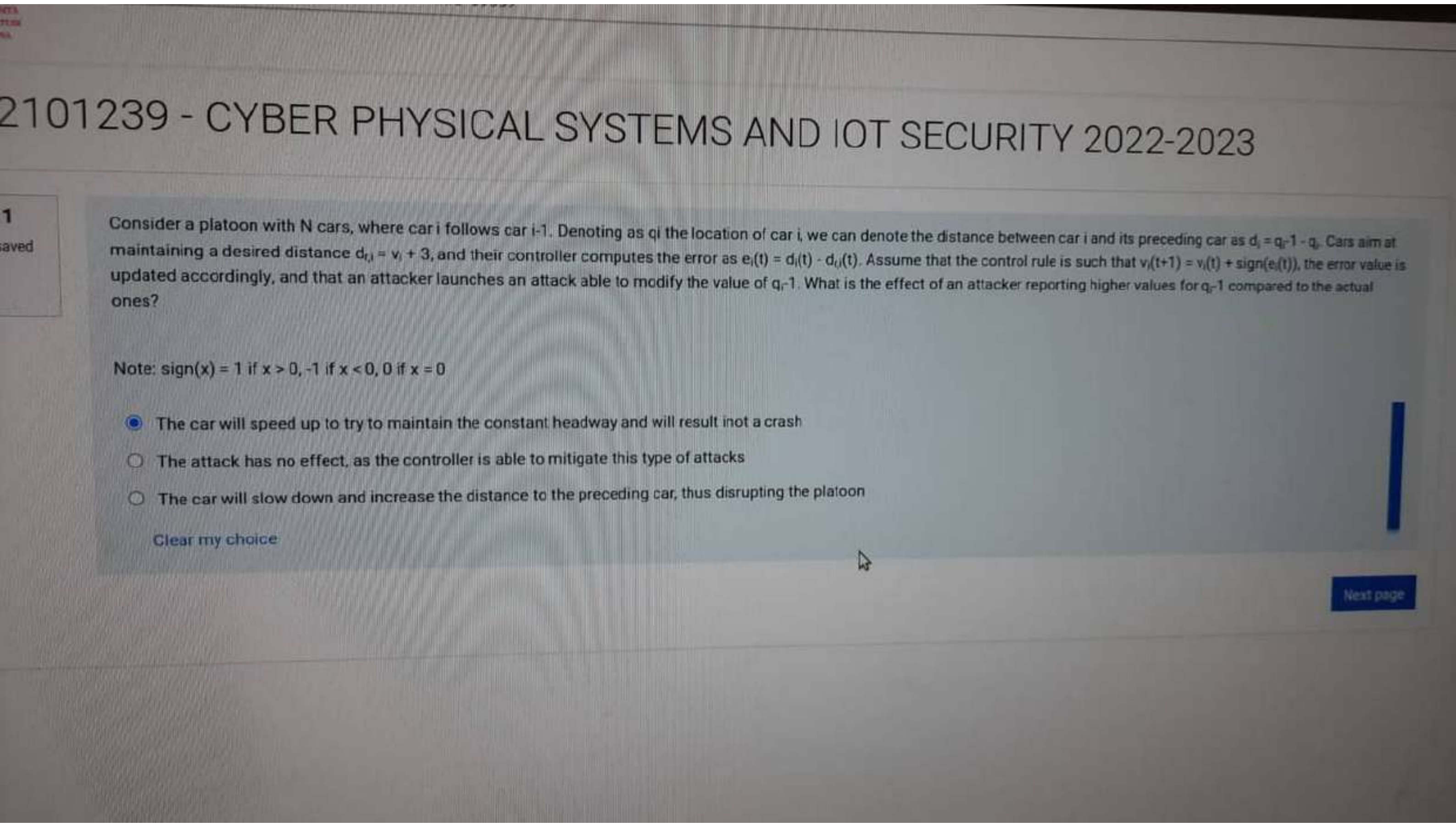
○ a protocol that is vulnerable to DoS attacks by an external attacker

● a methodology that drones can use to preserve their location privacy

○ a methodology that an attacker can use to avoid being detected by drone detection systems

Clear my choice

ous page



2101239 - CYBER PHYSICAL SYSTEMS AND IOT SECURITY 2022-2023

1

aved

Consider a platoon with N cars, where car i follows car i-1. Denoting as qi the location of car i, we can denote the distance between car i and its preceding car as $d_i = q_i$-1 - q_i. Cars aim at maintaining a desired distance $d_{r,i} = v_i + 3$, and their controller computes the error as $e_i(t) = d_i(t) - d_{r,i}(t)$. Assume that the control rule is such that $v_i(t+1) = v_i(t) + \text{sign}(e_i(t))$, the error value is updated accordingly, and that an attacker launches an attack able to modify the value of q_i-1. What is the effect of an attacker reporting higher values for q_i-1 compared to the actual ones?

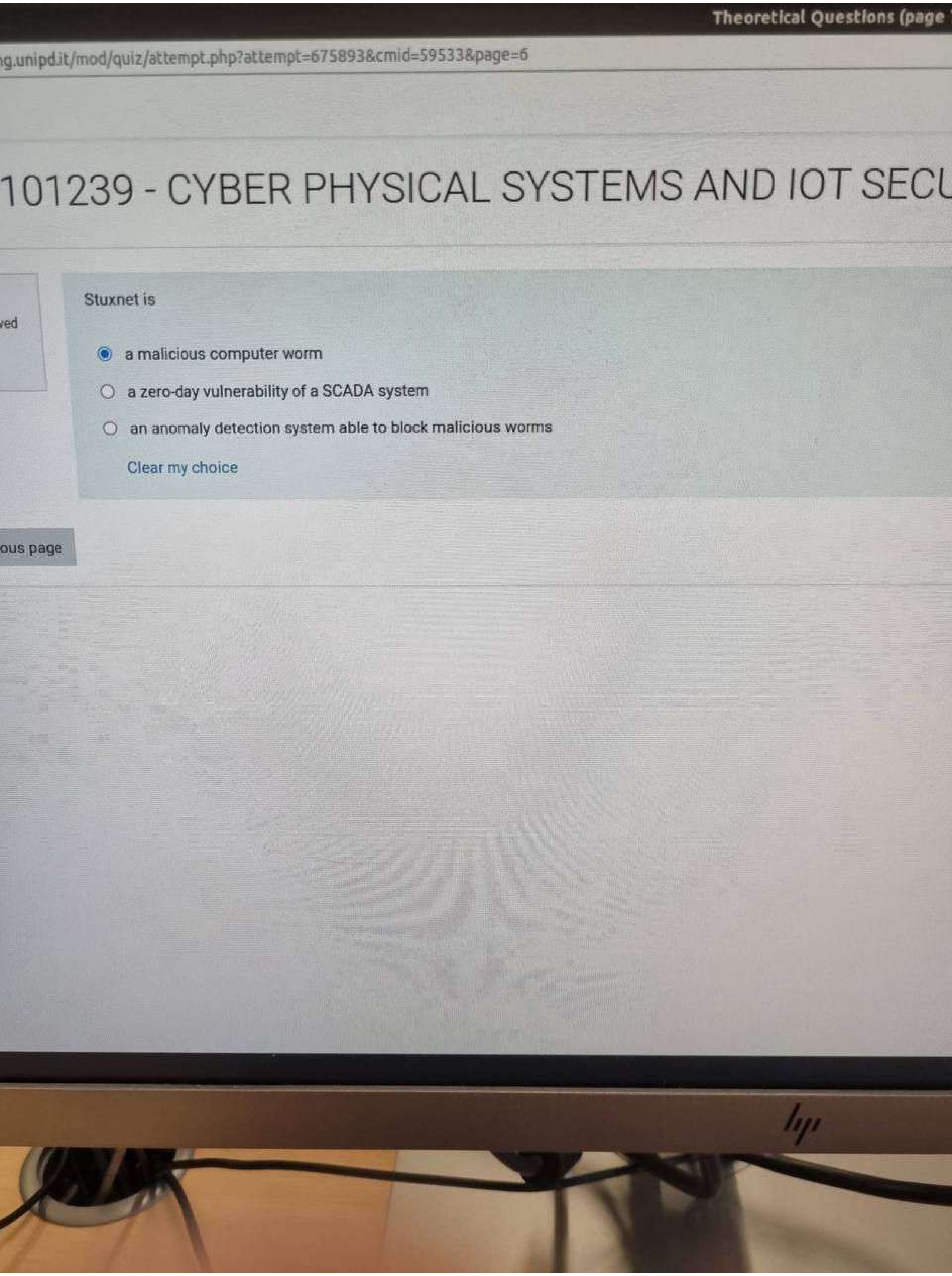
Note: sign(x) = 1 if x > 0, -1 if x < 0, 0 if x = 0

● The car will speed up to try to maintain the constant headway and will result inot a crash

○ The attack has no effect, as the controller is able to mitigate this type of attacks

○ The car will slow down and increase the distance to the preceding car, thus disrupting the platoon

Clear my choice



Theoretical Questions (page

ng.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=6

101239 - CYBER PHYSICAL SYSTEMS AND IOT SECU

ved

Stuxnet is

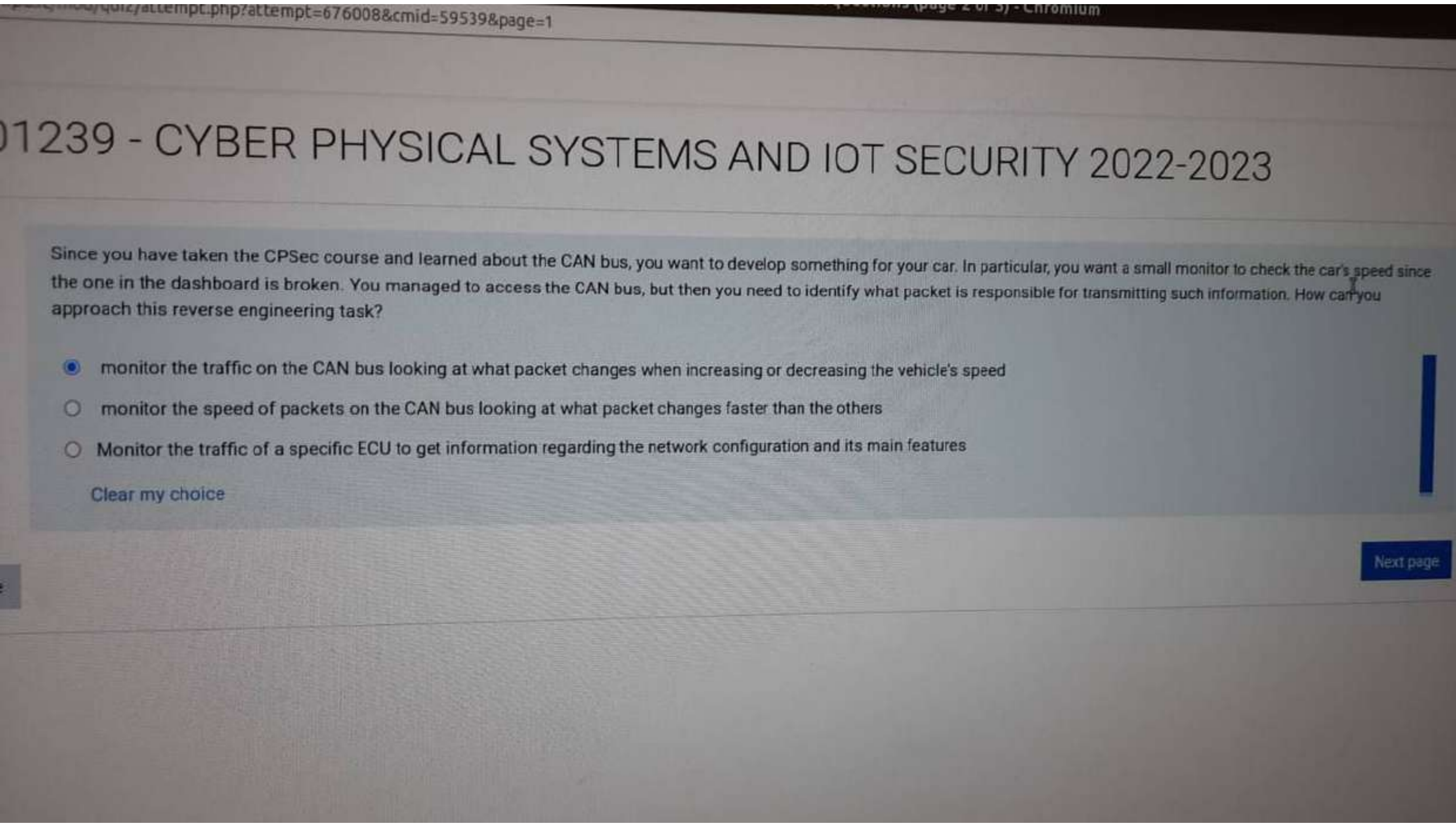
● a malicious computer worm

○ a zero-day vulnerability of a SCADA system

○ an anomaly detection system able to block malicious worms

Clear my choice

ous page



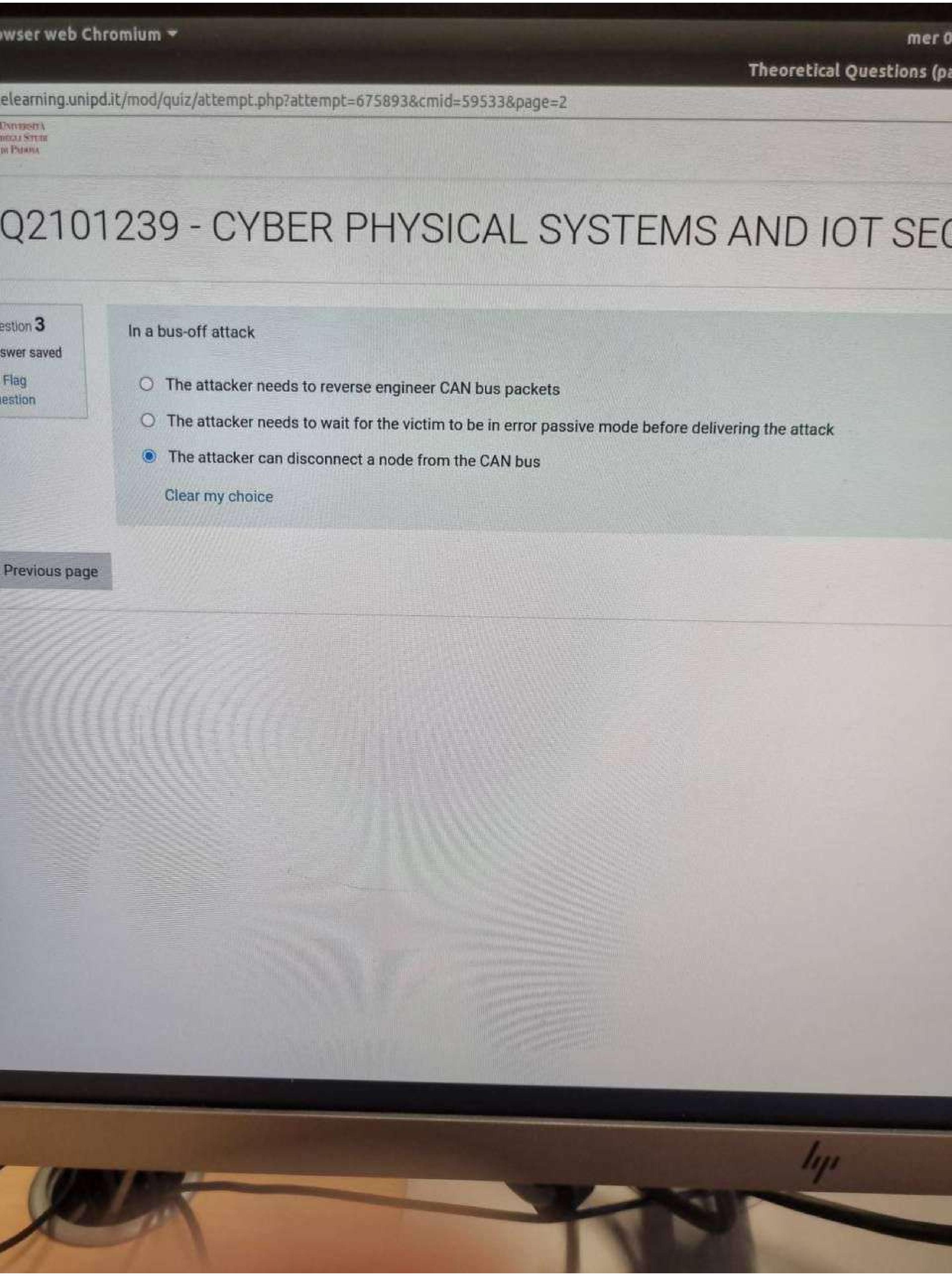
1239 - CYBER PHYSICAL SYSTEMS AND IOT SECURITY 2022-2023

Since you have taken the CPSec course and learned about the CAN bus, you want to develop something for your car. In particular, you want a small monitor to check the car's speed since the one in the dashboard is broken. You managed to access the CAN bus, but then you need to identify what packet is responsible for transmitting such information. How can you approach this reverse engineering task?

● monitor the traffic on the CAN bus looking at what packet changes when increasing or decreasing the vehicle's speed

○ monitor the speed of packets on the CAN bus looking at what packet changes faster than the others

○ Monitor the traffic of a specific ECU to get information regarding the network configuration and its main features


wser web Chromium ▾
mer 0
Theoretical Questions (pa
elearning.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=2
estion 3
swer saved
Flag
estion
Clear my choice
Previous page

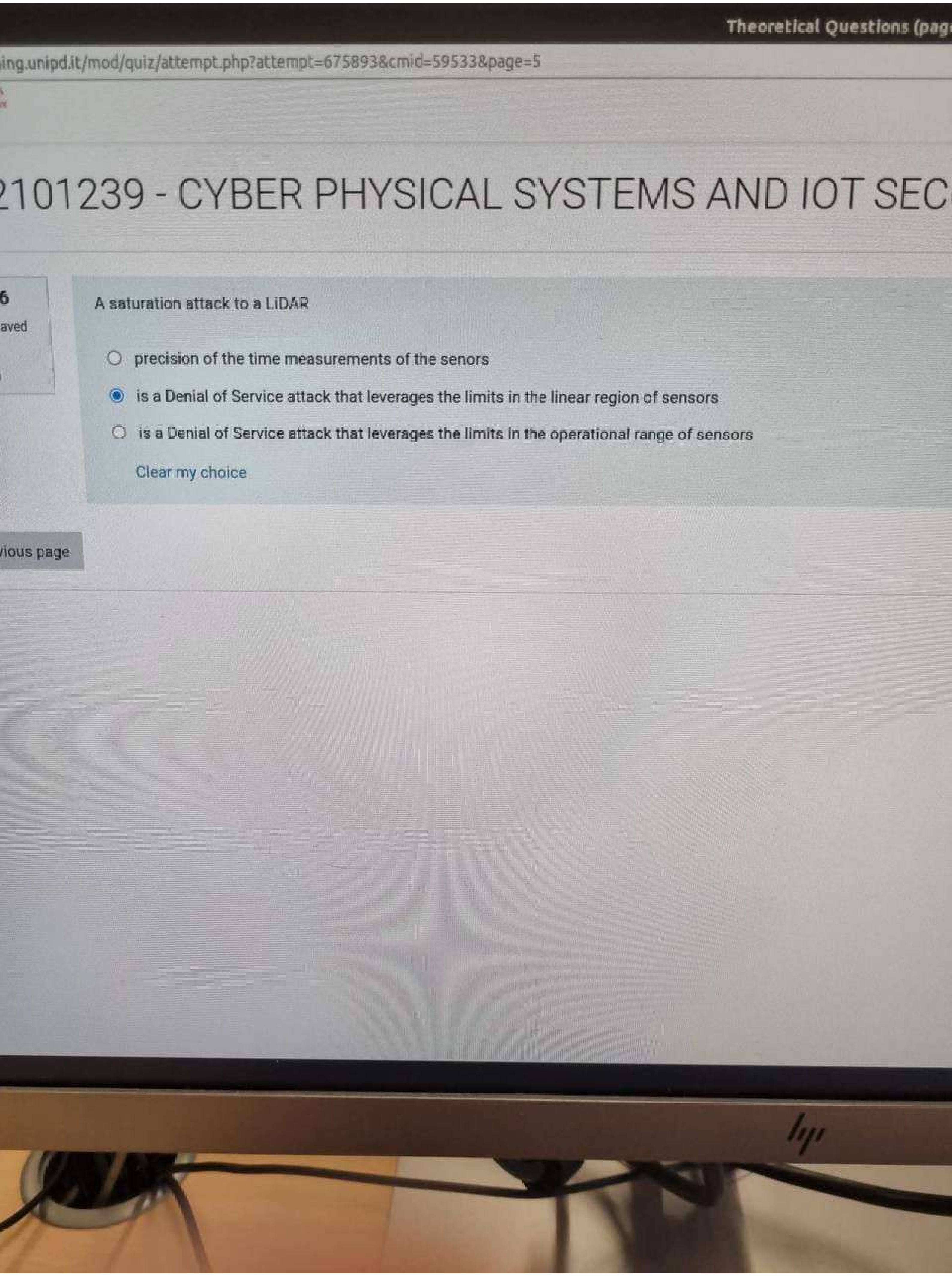
Q2101239 - CYBER PHYSICAL SYSTEMS AND IOT SEC

In a bus-off attack

○ The attacker needs to reverse engineer CAN bus packets

○ The attacker needs to wait for the victim to be in error passive mode before delivering the attack

● The attacker can disconnect a node from the CAN bus


Theoretical Questions (pag
ing.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=5
6
aved
Clear my choice
ious page

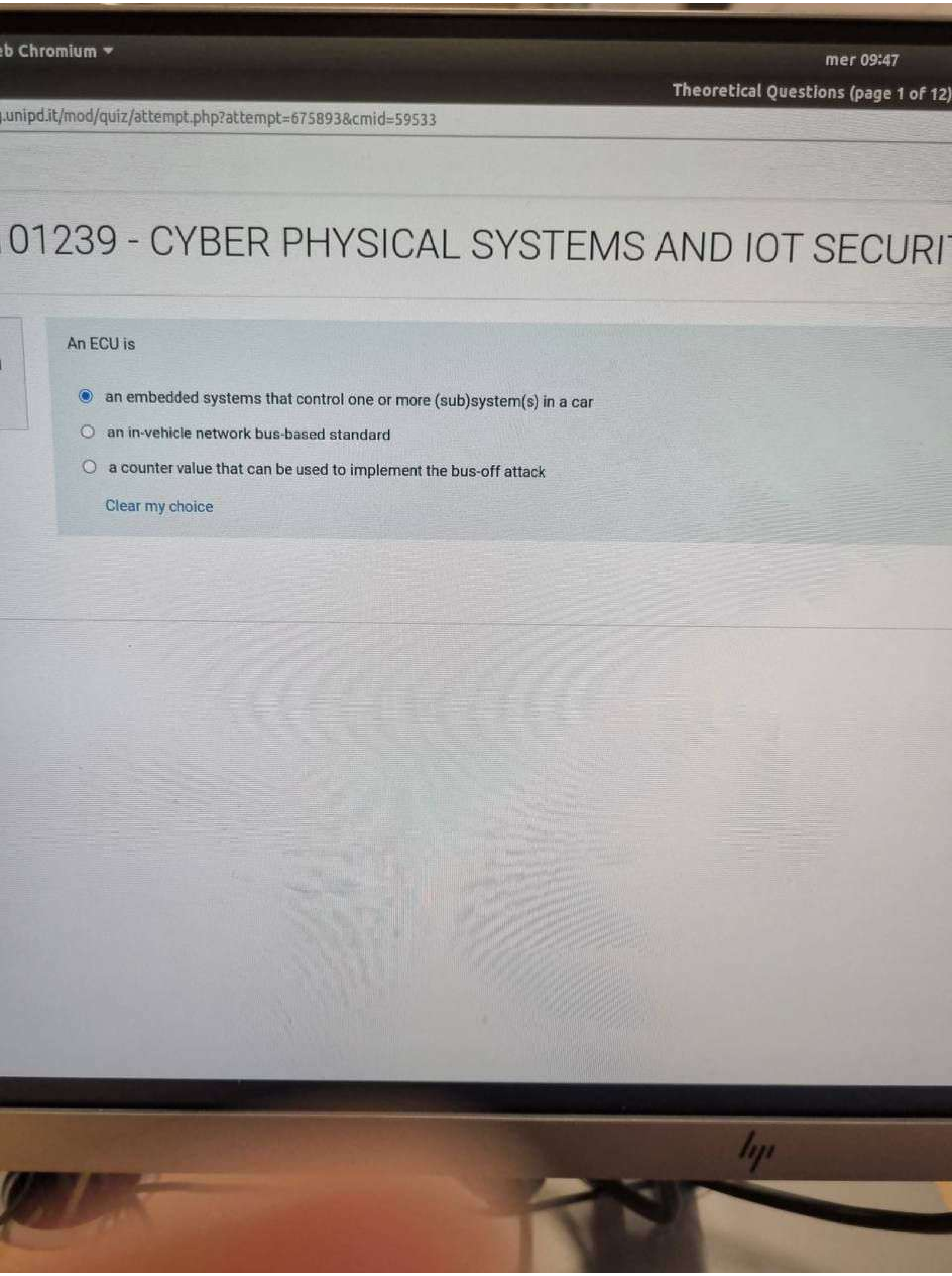
2101239 - CYBER PHYSICAL SYSTEMS AND IOT SEC

A saturation attack to a LiDAR

○ precision of the time measurements of the senors

● is a Denial of Service attack that leverages the limits in the linear region of sensors

○ is a Denial of Service attack that leverages the limits in the operational range of sensors

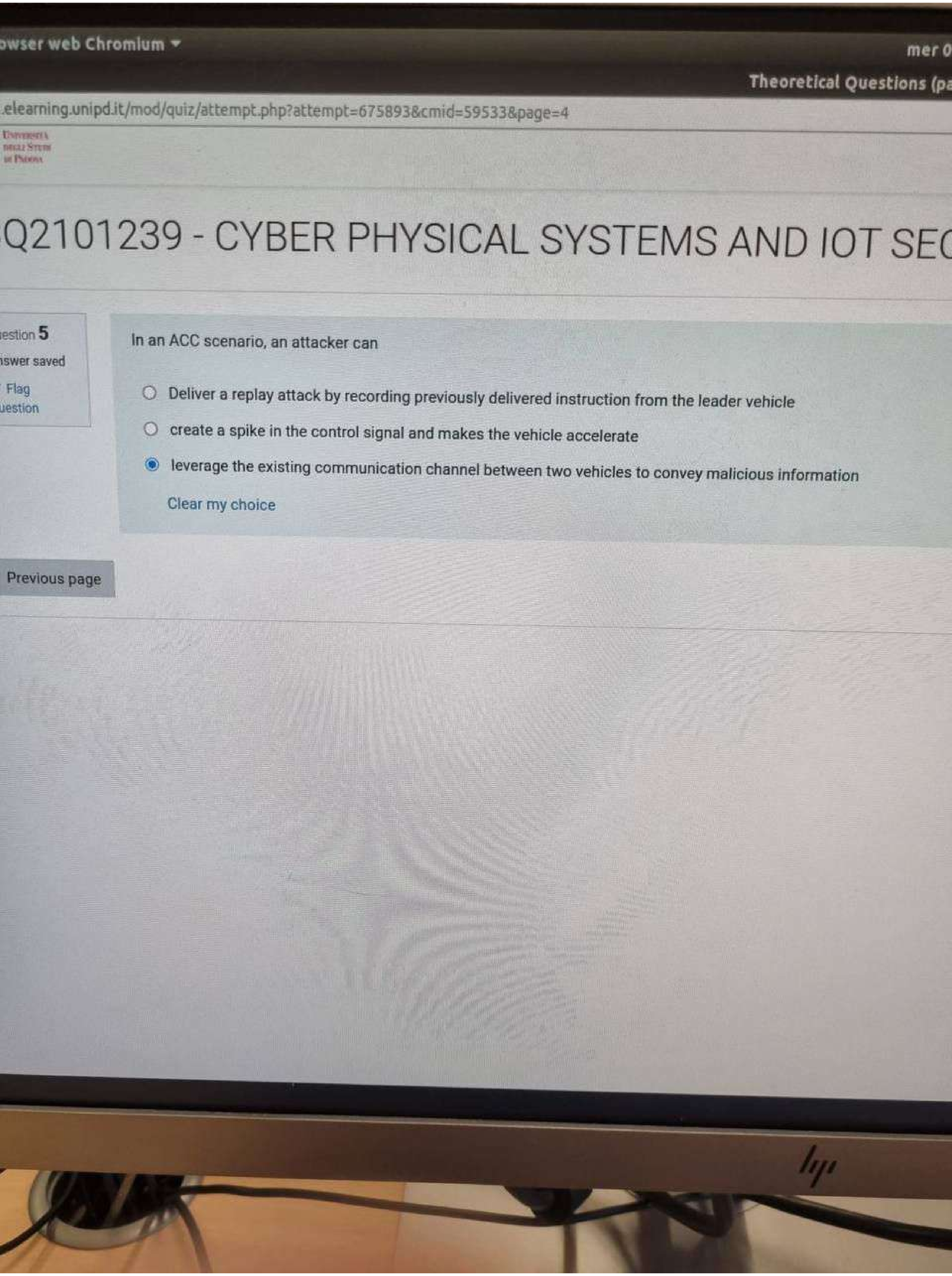

b Chromium ▾
mer 09:47
Theoretical Questions (page 1 of 12)
.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533

01239 - CYBER PHYSICAL SYSTEMS AND IOT SECURI

An ECU is

- ● an embedded systems that control one or more (sub)system(s) in a car
- ○ an in-vehicle network bus-based standard
- ○ a counter value that can be used to implement the bus-off attack

Clear my choice



owser web Chromium ▾
mer 0
Theoretical Questions (pa
.elearning.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=4
Università degli Studi di Padova

Q2101239 - CYBER PHYSICAL SYSTEMS AND IOT SEC

estion 5

nswer saved

Flag uestion

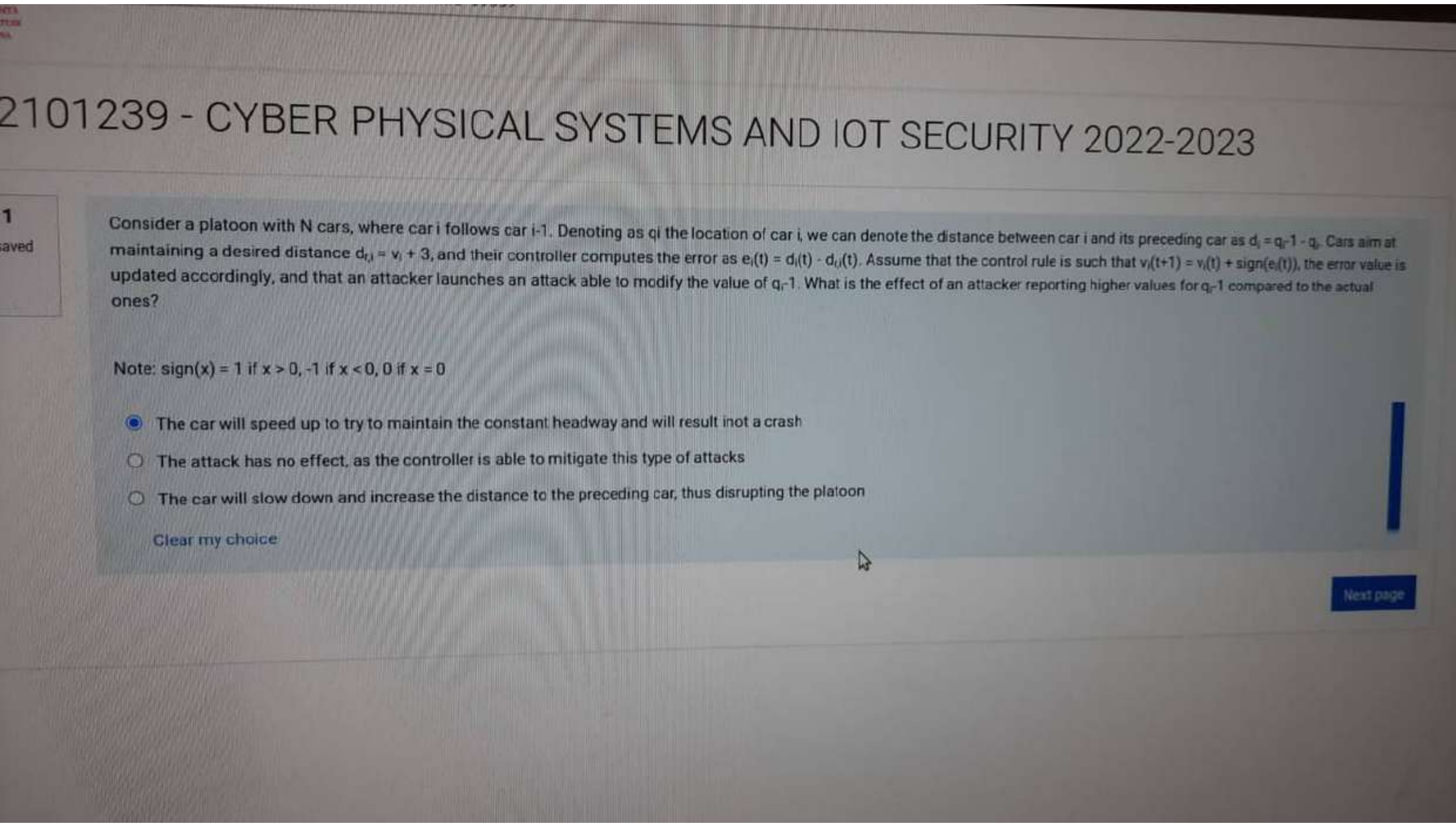
In an ACC scenario, an attacker can

○ Deliver a replay attack by recording previously delivered instruction from the leader vehicle

○ create a spike in the control signal and makes the vehicle accelerate

● leverage the existing communication channel between two vehicles to convey malicious information

Clear my choice



2101239 - CYBER PHYSICAL SYSTEMS AND IOT SECURITY 2022-2023

1

aved

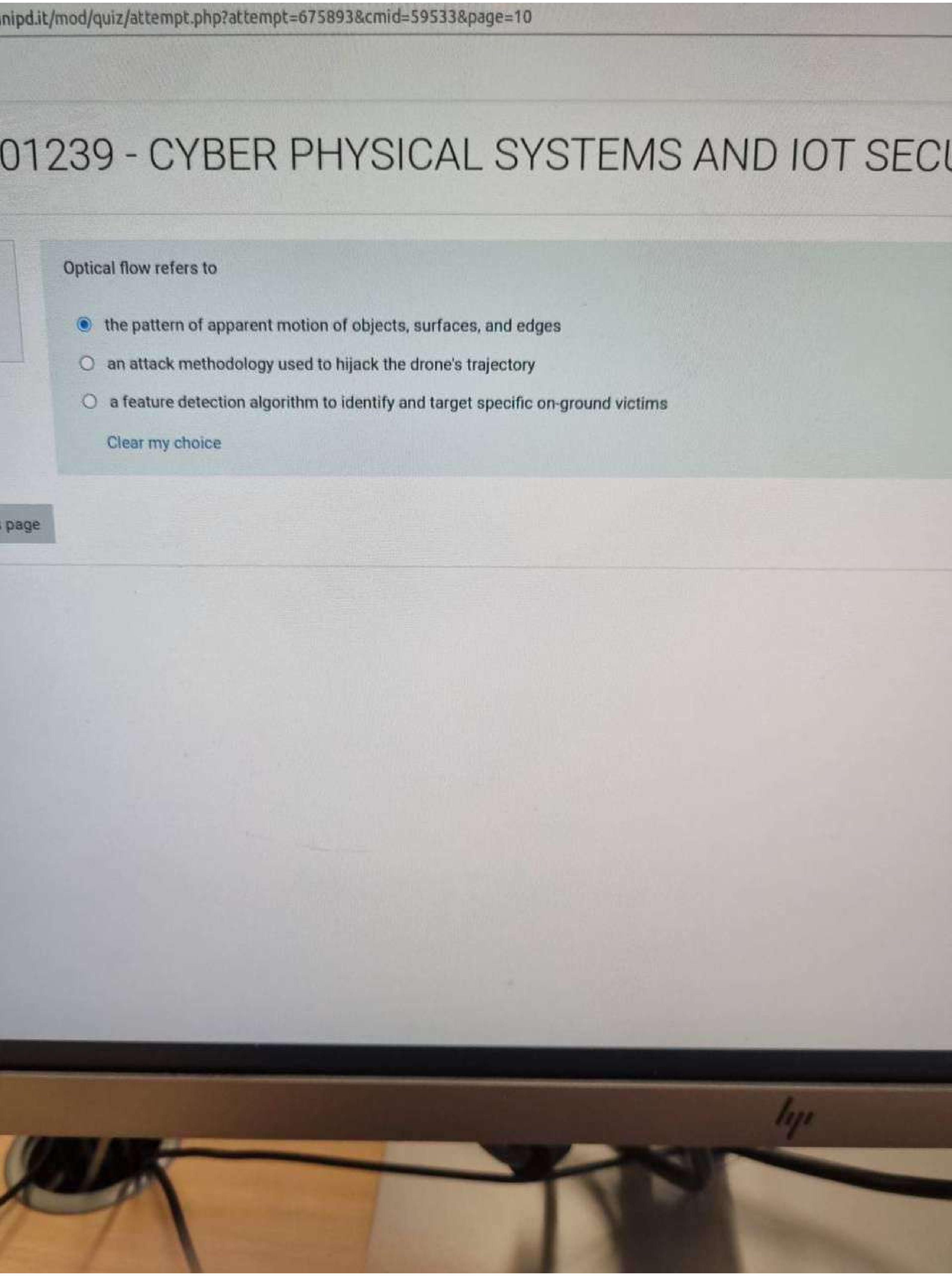
Consider a platoon with N cars, where car i follows car i-1. Denoting as qi the location of car i, we can denote the distance between car i and its preceding car as $d_i = q_i$-1 - q_i. Cars aim at maintaining a desired distance $d_{r,i} = v_i + 3$, and their controller computes the error as $e_i(t) = d_i(t) - d_{r,i}(t)$. Assume that the control rule is such that $v_i(t+1) = v_i(t) + \text{sign}(e_i(t))$, the error value is updated accordingly, and that an attacker launches an attack able to modify the value of q_i-1. What is the effect of an attacker reporting higher values for q_i-1 compared to the actual ones?

Note: sign(x) = 1 if x > 0, -1 if x < 0, 0 if x = 0

● The car will speed up to try to maintain the constant headway and will result inot a crash

○ The attack has no effect, as the controller is able to mitigate this type of attacks

○ The car will slow down and increase the distance to the preceding car, thus disrupting the platoon



nipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=10

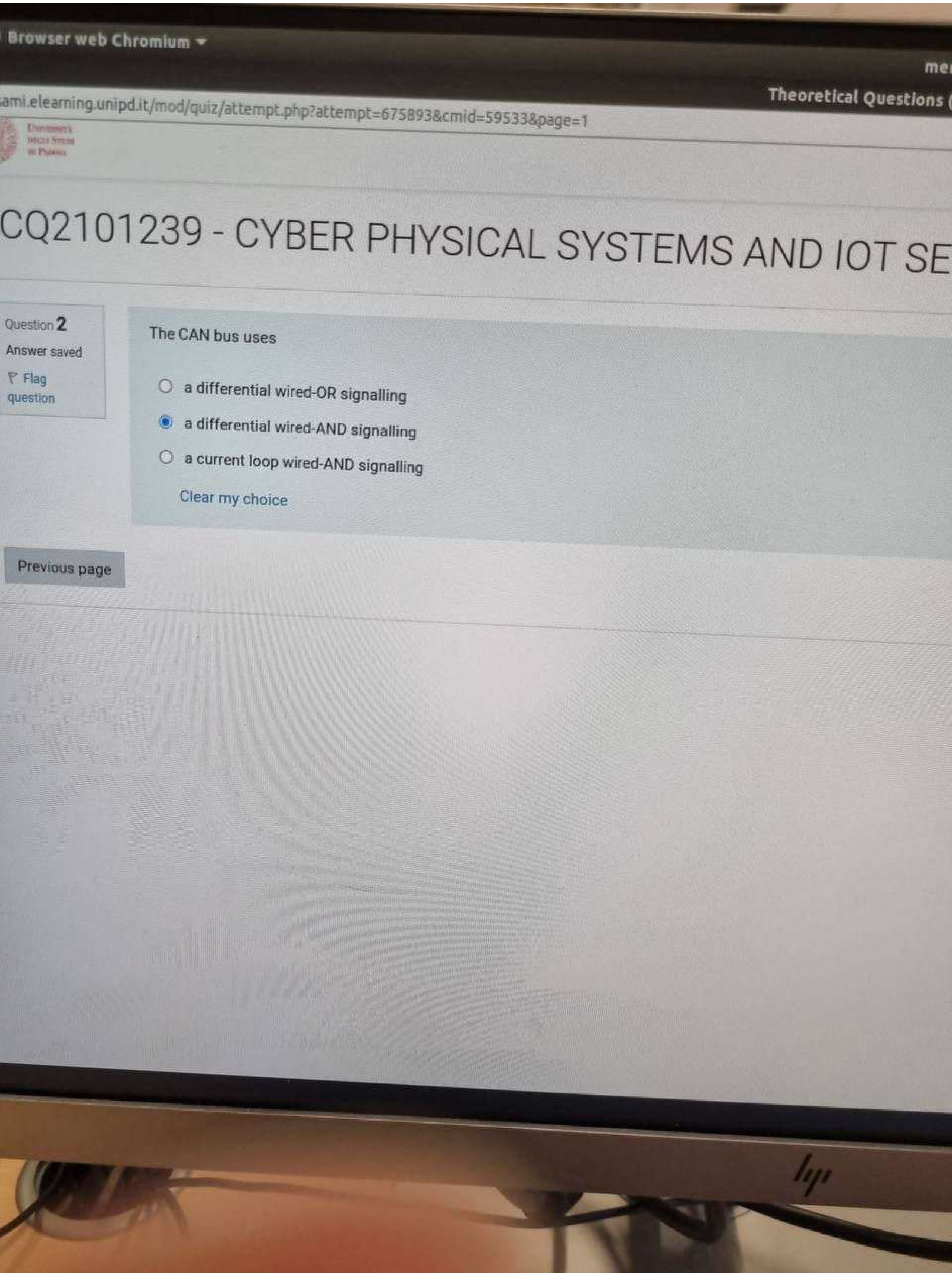
01239 - CYBER PHYSICAL SYSTEMS AND IOT SECU

Optical flow refers to

● the pattern of apparent motion of objects, surfaces, and edges

○ an attack methodology used to hijack the drone's trajectory

○ a feature detection algorithm to identify and target specific on-ground victims



Browser web Chromium ▾
me
Theoretical Questions (
ami.elearning.unipd.it/mod/quiz/attempt.php?attempt=675893&cmid=59533&page=1

CQ2101239 - CYBER PHYSICAL SYSTEMS AND IOT SE

Question **2**

Answer saved

The CAN bus uses

○ a differential wired-OR signalling

● a differential wired-AND signalling

○ a current loop wired-AND signalling