Universidade do Algarve | Basics on Security | 2024

Lab #5

Nome | PL2 | Número de Aluno

Completely fill the circles as shown: ○○●○

Rúbrica de Avaliação	Pontos
Correct answer selected	1.7
Incorrect answer selected	-1

Q1 You listen to a presentation about a new network protocol for online banking. After the talk, there is a lot of discussion going on. **Check all the remarks** that are relevant under the **Dolev-Yao** model.

- ○ The bank runs Windows on their servers. This will be insecure.
- ○ It looks nice, the NSA (National Security Agency) will break the encryption function and use this to spy on us.
- ○ What happens if someone breaks into the bank's data center? They should use a blockchain instead!
- ● I don't think they properly protect against transaction replay.

Q2 For each network capability, which goal is **directly** violated? **Only check one goal** - the most directly violated one per capability.

Attacker Capability	Confidentiality	Integrity	Availability
Observe packets	●	○	○
Modify packets	○	●	○
Drop packets	○	○	●
Delay packets	○	○	●
Forge packets	●	○	○
Replay packets	○	○	●

Q3 For their new blockchain-based cryptocurrency venture, FooBank's CTO wants to get rind of all that unwanted software code and build revolutionary high-speed banking protocol directly on top of IP pakets. They propose the following protocol for money transfers between two different bank branches:

"I first send you a packet with information of the receiver, then a packet with information of the amount, and then a packet with information of the recipient. Trust me, it's the best protocol we ever had!".

What could possibly go wrong? **Check all the options that are true**.

- ● Some transfers may inexplicably fail.
- ● Instead of sending money from Alice to Bob, FooBank may end up sending money from Bob to Alice.
- ● Mischievous attackers may get rich.
- ● Someone in Russia may get wind of it.

Q4 Check all statements that are true about BGPs.

- ○ The confidentiality of our communications can be asserted by physically protecting all fiber cables (in the world) on the default path.
- ● Securing BGP communications **today** is mostly an **afterthought** due to the fact that threat models have changed from the old Arpanet to the modern Internet.
- ○ When leaving a spouse (home), one should reconfigure their BGP routes to protect her against stalking.