Riverside Enterprise is an aerial ridesharing company that uses various network protocols to support and enhance its operations. Riverside uses two major protocol implementations:

- Open-source CaptainsLog shares user experience feedback with the company.
- Proprietary StarfleetComm allows communications between fleet vehicles.

Select all of the true statements below using the protocol specifications information from Module 02.

Reminder: Canvas auto-grading will reduce the overall score for this problem for incorrectly selected statements. Unselected statements will not alter the score (you won't gain or lose points for not selecting a statement, regardless of whether it is true or false).

- [ ] Reverse engineering StarfleetComm would deter attackers from attacking the protocol.

- [ ] While their name does not suggest it, open protocols, like CaptainsLog, are only accessible to subject experts and are often only considered “open” as more than one company is involved in development.

- [x] CaptainsLog is likely easier for attackers to find security flaws than StarfleetComm.

Correct.

- [x] Proprietary protocols, like StarfleetComm, are often used in Physical and Network layers as vendors often want to protect their protocols for business reasons.

Incorrect.

- [x] Open protocols, like CaptainsLog, are generally reviewed multiple times before being standardized.

Correct.

See Section 2.1 Protocol Specifications on pp. 23-25 in your textbook for more details on open-source vs. proprietary protocols.

CaptainsLog is likely easier for attackers to find security flaws than StarfleetComm.

True.

Open protocols, like CaptainsLog, are generally reviewed multiple times before being standardized.

True.

Proprietary protocols, like StarfleetComm, are often used in Physical and Network layers as vendors often want to protect their protocols for business reasons.

False. The application layer is the most common place for proprietary protocols since there is

not always a requirement for interoperability between vendors.

Reverse engineering StarfleetComm would deter attackers from attacking the protocol.

False. Most proprietary protocols are reverse engineered within a short period of time and do not deter attackers.

While their name does not suggest it, open protocols, like CaptainsLog, are only accessible to subject experts and are often only considered "open" as more than one company is involved in development.

False. With an open protocol, reverse engineering is unnecessary because the protocol details are publicly available.

PartialQuestion 2
3 / 4 pts

Select all of the true statements below using the network address information from Module 02.

Reminder: Canvas auto-grading will reduce the overall score for this problem for incorrectly selected statements. Unselected statements will not alter the score (you won't gain or lose points for not selecting a statement, regardless of whether it is true or false).

- [x] The machine address used at the physical layer is often assigned by the device manufacturer.

Correct.

- [ ] Hostnames are registered using the DNS system.
- [ ] Port numbers have strict authentication requirements and must be registered with a port registrar.
- [ ] IP addresses identify an application running on the Internet.
- [x] Devices use physical layer addresses to determine whether traffic is intended for them or can be ignored.

Correct.

- [x] The TCP layer utilizes application addresses (port numbers) as its primary identifier.

Correct.

- [x] Registration authorities are responsible for assigning host names.

Correct.

- [x] Address servers are used to assign static addresses.

Incorrect.

Address servers are used to assign static addresses.

False. Address servers are used to assign dynamic addresses. Static addresses are typically part of the system configuration. (p. 32)

Application addresses (port numbers) have strict authentication requirements and must be registered with a port registrar.

False. Application addresses can be set to whatever value the administrator wants, but often are set to values that everyone already knows. (p. 34)

Devices use physical layer addresses to determine whether traffic is intended for them or can be ignored.

True. (See p. 31 in the textbook.)

Host names are registered using the DNS system.

False. DNS maps hostnames to IP addresses, while registration authorities assign hostnames. (p. 34)

IP addresses identify an application running on the Internet.

False. IP addresses are used to identify devices, and application addresses (port numbers) are used to identify applications. (pp. 31 & 32)

Registration authorities are responsible for assigning host names.

True. (See p. 34 in the textbook.)

The TCP layer utilizes application addresses (port numbers) as its primary identifier.

True. (See p. 32 in the textbook.)

The machine address used at the physical layer is often assigned by the device manufacturer.

True. (See p. 33 in the textbook.)

Question 3

1.5 / 1.5 pts

Which statement best describes the use of network addresses by attackers to cause security violations?

- Network addresses have no relevance to security violations caused by attackers.

- Attackers rarely target network addresses and focus more on other vulnerabilities in the system.
- All network address types, including Ethernet addresses, can be exploited by attackers.

Correct.

- Attackers primarily target network addresses other than Ethernet addresses for security violations.
- Only Ethernet addresses are vulnerable to security violations caused by attackers.

IncorrectQuestion 4

0 / 1.5 pts

Which statement best describes the primary security concern regarding application addresses or port numbers?

- The biggest security issue lies in assigning port numbers and determining the entity responsible.
- The security of application addresses depends on the network devices' physical location and has no connection to protocol vulnerabilities.
- Security vulnerabilities arise from the improper utilization of application addresses.

Incorrect. The biggest security concern with respect to application addresses (port numbers) is authentication. See p. 34 in the textbook for more information.

- Authentication of applications is the main security concern associated with application addresses.
- The security issue with application addresses is equally attributed to assignment and authentication.

Question 5

1 / 1 pts

Which organization is responsible for maintaining and publishing Request for Comments (RFCs) that contribute to developing standards for the Internet?

- Institute of Electrical and Electronics Engineers (IEEE)
- American National Standards Institute (ANSI)
- International Standards Organization (ISO)
- Internet Engineering Task Force (IETF)

Correct.

- International Telecommunications Union-Telecommunications Standards Sector (ITU-T)

Remember:

Upon submission, you will be able to see your quiz responses after submission until you navigate