1. What does IoT security aim to ensure?

- a) Affordability and scalability
- b) Availability, integrity, and confidentiality
- c) Compatibility and speed
- d) Energy efficiency and durability
- **Answer:** b) Availability, integrity, and confidentiality

2. Which is a major challenge in IoT security?

- a) Lack of user manuals
- b) Managing diverse data types and computing power
- c) High development costs
- d) Limited network coverage
- **Answer:** b) Managing diverse data types and computing power

3. What is the most common vulnerability in IoT devices?

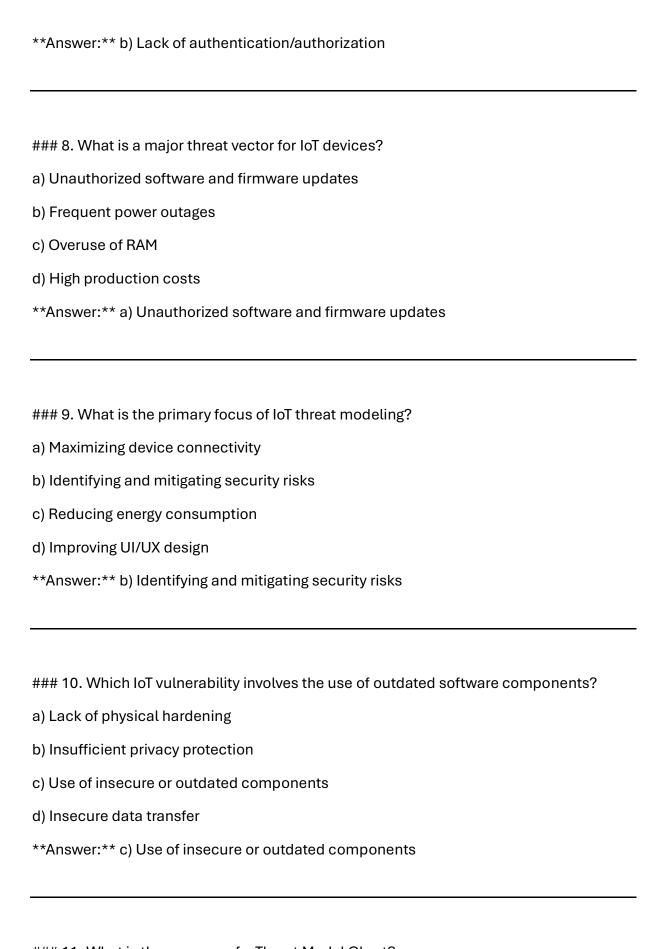
- a) Limited memory capacity
- b) Weak, default, or hardcoded passwords
- c) Poor hardware design
- d) Overuse of encryption
- **Answer:** b) Weak, default, or hardcoded passwords

4. Which attack is associated with capturing sensitive information between IoT devices?

a) Man-in-the-Middle (MITM) attack b) SQL injection attack c) Buffer overflow attack d) Cross-site scripting attack **Answer:** a) Man-in-the-Middle (MITM) attack ### 5. What should be the first step for any IoT business regarding security? a) Implementing encryption protocols b) Conducting a thorough security risk assessment c) Designing a user-friendly interface d) Using open-source software **Answer:** b) Conducting a thorough security risk assessment ### 6. Which of the following is NOT a key IoT security requirement? a) Ensuring data integrity b) Providing device identity c) Supporting unlimited device connections d) Meeting compliance regulations **Answer:** c) Supporting unlimited device connections

7. What is a common issue with insecure ecosystem interfaces?

- a) Overheating of devices
- b) Lack of authentication/authorization
- c) Excessive use of bandwidth
- d) Limited device lifespan



a) To enhance user experience b) To document and prioritize identified threats c) To visualize data analytics d) To track IoT device sales **Answer:** b) To document and prioritize identified threats ### 12. What scoring model is used to qualify threats in IoT systems? a) DREAD model b) SWOT analysis c) PERT model d) Gantt model **Answer:** a) DREAD model ### 13. Which of these is a best practice for IoT security? a) Using default passwords b) Avoiding software updates c) Enabling multi-factor authentication d) Disabling encryption **Answer:** c) Enabling multi-factor authentication

14. What kind of attack is the Mirai botnet associated with?

- a) Distributed Denial of Service (DDoS)
- b) Phishing
- c) Ransomware
- d) Social engineering

15. What was a vulnerability exploited in the 2020 Tesla Model X hack?

- a) Bluetooth
- b) Wi-Fi encryption
- c) Overheating sensors
- d) Weak processor
- **Answer:** a) Bluetooth