Josh Keahey

1. According to the National Institute of Standards and Technology (NIST), computer security is defined as: The protection given to an automated information system in order to keep the objectives of the confidentiality, availability and integrity of the system resources, such as hardware, software, information/data, telecommunications and firmware. [1]

2. An active attack is where the threat agent attempts to alter a system's resources or affects their operation from working correctly, whereas a passive attack has the adversary trying to learn information or use it, but will not actually affect the system itself.

3. For passive attacks, there are the releasing of messages, where confidential emails or files being sent were intercepted, read and given to the public. Another is called traffic analysis. Even if an attacker couldn't read files being sent, they could figure out what host's sent them, and how often. As for active attacks, there are four major ones. Replay, which retransmits messages obtained passively for an undesired effect. Masquerade, where the adversary poses as an authorized user, and usually uses another active attack to create chaos. Modifications of messages is another that could change a message to say 'trust so-and-so' with this information. The last is denial of service, which stops or significantly slows down communication of the system. This can disrupt the entire network by overloading it with messages, making it unable to be used.

4. The fundamental security design principles are as follows [2]:
    1. Economy of Mechanism - Essentially this means that the design of security implementation in hardware and software should be as small and simple as possible.
    2. Fail-Safe Defaults - This means that access decisions to the system information should be based on permission rather than exclusion, like when deciding permissions for roles.
    3. Complete Mediation - When info is accessed, checks with the access control mechanism must be done every time, making sure permissions have not been changed.
    4. Open Design - The design itself should be open for public review and advice, and not kept secret.
    5. Separation of Privilege - This is the practice of requiring multiple privilege attributes for somebody to obtain access to a restricted resource in the system.
    6. Least Privilege - To help keep protection as high as necessary, every process and every user of the system should operate using the least amount of privileges possible to perform each task.
    7. Least Common Mechanism - The security design should keep functions shared by different users as small as possible, providing mutual security to the system.
    8. Psychological Acceptability - The security mechanisms in place should not impede the work of the users, while still being accessible to those who have authorization.
    9. Isolation - Items in the system should be separated, such as public access systems and critical resources, processes and files from different users, and security mechanisms.
    10. Encapsulation - This is a form of isolation based on object-oriented functionality by encapsulating a collection of objects in a domain of its own so that object is only accessible to the procedures of the protected subsystem.
    11. Modularity - Not only keep secure functions separate, but also use a modular architecture for mechanism design and implementation.
    12. Layering - Multiple layers of protection should be used, in case one is compromised.
    13. Least Astonishment - The UI should be transparent and not surprise the user.

5. An attack surface are exploitable vulnerabilities in a system that can be categorized as coming from a network, other software, or a human attack. This could be from code on a host listening on ports, to a user with access to sensitive information.

An attack tree can be described as a hierarchical data structure that shows security vulnerabilities for a system. The root node is the security breach that is the goal of the attack, and the leaves of the tree indicate different ways to initiate the attack.

Citations
[1] 2014, Computer Science: Principles and Practice, Stallings and Brown, Chapter 1, Sec. 1.1
[2] 2014, Computer Science: Principles and Practice, Stallings and Brown, Chapter 1, Sec. 1.4