정보보호입문 문제은행 (컴퓨터학과)

1. There have been numerous news reports on cyber crimes and incidents, and there are too many to list.
   A. What is the most notorious computer security incident you know of in which **confidentiality** was compromised? Briefly summarize the incident by a couple of sentences. You must also provide a persuasive argument as to why this incident is primarily a confidentiality issue.
   B. What is the most notorious computer security incident you know of in which **integrity** was compromised? Briefly summarize (e.g., a couple of sentences) the incident. You must also provide a persuasive argument as to why this incident is primarily an integrity issue.
   C. What is the most notorious computer security incident you know of in which **availability** was compromised? Briefly summarize (e.g., a couple of sentences) the incident. You must also provide a persuasive argument as to why this incident is primarily an availability issue.

2. Please explain each of the following terms briefly.
   A. Return to libc
   B. Integer overflow
   C. Inference problems
   D. Zero trust security model
   E. IP spoofing
   F. Homomorphic encryption
   G. Rate limiting
   H. Key stretching
   I. Fuzzing
   J. STRIDE threat modeling
   K. Return-oriented programming

3. Explain security vulnerabilities in software. Then, discuss how we can reduce s ecurity vulnerabilities during the development of software.

4. Explain malware obfuscation techniques as many as possible. Then, discuss how to detect obfuscated malware.

5. The SolarWinds cyber attack first announced at December 2020 is a massive attack on software supply chain. Explain the vulnerabilities being involved in this attack as many as possible, which made the attack successful against 18,000 companies and organizations. Explain each vulnerability according to the violation of one or more of the eight design principles for security enhancement. Then, suggest your opinion how we can protect from the future supply chain attacks.

6. Replay attacks are simple but powerful, which can exploit time invariants in remote user authentication. Describe two different approaches for protecting password-based user authentication from replay attacks.

7. Two main problems of intrusion detection technologies are false positives and false negatives. Explain false positives and false negatives, respectively. Discuss which one is more important than the other, and how to minimize them.

8. Discuss the differences between ACLs and capabilities. Explain the cases when ACLs are better than capabilities.

9. How can we verify the received messages are authentic? Discuss how we can do message authentication without message encryption.

10. Explain how Dirty COW vulnerability works. Then, discuss how to prevent such a vulnerability during the development of software.

11. Provide one case of "security through obscurity" and explain the security problems of the case. Then, discuss how to improve the security in the case, rather than relying on the implementation secrecy.

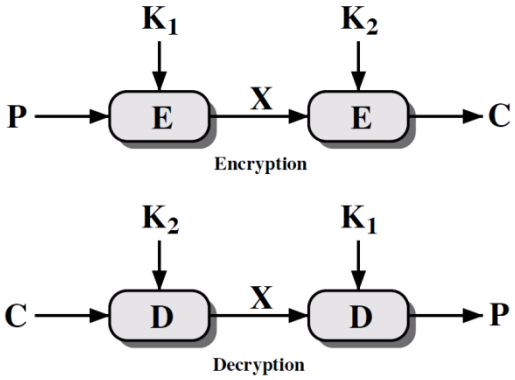
12. Describe the vulnerability of Intel AMT bug which was found at 2017 and allo ws an attacker to control any Intel machine remotely. Then, discuss how to fi nd and fix such a problem through "security by design".

13. Choose one example of the environment variables which can be a security vul nerability. Then, suggest how to prevent from exploiting such a vulnerability i n advance.

14. Explain the importance of OS hardening for preventing attacks. List the possib le tasks for OS hardening as many as possible.

15. Explain the eight principles for secure system design. Discuss how to develop an Android application with the eight principles.

16. In the following double-DES using two different keys 56-bit K1 and K2, securi ty level is $O(2^{56})$ rather than $O(2^{112})$. Explain why.



17. Describe the man-in-the-middle attack on the Diffie-Hellman key exchange protocol.

18. Consider secure hash function requirements.

    A. Describe the following definitions

i. Pre-image resistance

ii. Second pre-image resistance

iii. Collision resistance

B. For an m-bit hash value, what value determines the security of hash code against brute-force attack?

i. Pre-image resistance:

ii. Second pre-image resistance:

iii. Collision resistance:

19. Explain why MAC cannot be used as a signature.

20. None of the cipher algorithms in the real world cannot guarantee perfect (or unconditional) security, except one-time pad.

A. Explain what conditions are needed for the unconditional security of one-time pad.

B. Explain why all of the other cipher algorithms except one-time pad cannot support it in practice.