11210/IIS500200 Network Security, Fall 2023

Homework 1

111061548 游鎮遠

1.

I. Confidentiality:
   i. **High Level:** Student grade should be available only to students, parents, and relevant employees.
   ii. **Moderate Level:** Students enrolment.
   iii. **Low Level:** Directory info (list of departments, faculties, and students).

II. Integrity:
   i. **High Level:** Patient information stored in a database – inaccurate information could result in serious harm or death to a patient.
   ii. **Moderate Level:** A entertainment Web site that offers a forum. A user/hacker falsify some info.
   iii. **Low Level:** Anonymous online poll with weak authentication.

III. Availability:
   i. **High Level:** Authentication provider services.
   ii. **Moderate Level:** University's website.
   iii. **Low Level:** An online telephone directory.

High Level:

- The loss have a severe or catastrophic adverse effect on organizational operations.
- Organization cannot do one or more of its primary functions.

Moderate Level:

- The loss could have a serious adverse effect on organizational operations.
- Significant degradation on organization functionality.

Low Level:

- The loss could have a limited effect on organizational operations.
- Organization can still perform its normal functions.

2. Consider a desktop publishing system used to produce documents for various organizations, here are examples for each of the requirements:
   （a） Confidentiality:
   Government Security Briefings, unauthorized access to government security documents such as security briefings, classified documents or diplomatic correspondence, could have serious implications for national security, so confidentiality is a top priority.
   （b） Data Integrity:
   Medical Patient Records, in the context of healthcare, maintaining the integrity of patient records, medical reports, and treatment plans is crucial. Any form of data corruption or tampering could lead to incorrect diagnoses, treatment errors, or even patient harm.
   （c） Availability:
   News Websites, for organizations that operate news websites, ensuring high system availability is critical. These websites need to be accessible to users 24/7, especially during breaking news events, downtime can result in a loss of credibility.

3. Anybody can generate and append a hash to any message. A malicious adversary can easily modify the message and append the recomputed hash value, this modification goes undetected at the receiving end, such us Length Extension Attack.

4. Use a key of length 255 bytes. The first two bytes are zero; that is K[0] = K[1] = 0. Thereafter, we have: K[2] = 255, K[3] = 254, . . . , K[255] = 2.

5. No. The output block P3 depends only on the input blocks C_2 C_3.
   $P_1 = IV \oplus \mathrm{D}[K, \mathrm{C}_1]$,
   $P_2 = C_1 \oplus \mathrm{D}[\mathrm{K}, \mathrm{C}_2]$,
   $P_3 = C_2 \oplus \mathrm{D}[\mathrm{K}, \mathrm{C}_3]$,
   $P_{N+1} = C_N \oplus \mathrm{D}[\mathrm{K}, \mathrm{C}_{\mathrm{N}+1}]$

6. In CBC encryption, the input block to each forward cipher operation (except the first) depends on the result of the previous forward cipher operation, so the forward cipher operations cannot be performed in parallel. In CBC decryption, however, the input blocks for the inverse cipher function (i.e., the ciphertext blocks) are immediately available, so that multiple inverse cipher operations can be performed in parallel.

7. That not true. Collision resistant just means the chance is really low, but not 0, there is still a chance to find a message whose hash is already in the list.

8. It is possible, by using Feistel structure.

9. $n = 667,\ e = 3,\ d = \ ?$
   $n = p * q$
   Choose two different parameters p and q :
   $667 = 23 * 29$
   Where $ed = 1\ mod\ \Phi(n)$, and $\Phi(n) = (p-1)(q-1) = 22 * 28 = 616$
   Use Euclidean algorithm,
   So, $3d = 1\ mod\ (616),\ d = 411.$