

CSCI 283 and CSCI 172 - Computer Security - Fall 2006
Test 1 Solutions

1. (5 points) Circle one of True or False for each of the following. No explanations required. **You will get -1 for an incorrect answer, and +1 for a correct one. So, for example, if you get 3 correct and 2 incorrect answers, you will get one point.**

- i. (1 point) Abbreviated Access Control Lists (ACLs) are more storage-efficient than are Access Control Matrices **True**
- ii. (1 point) Abbreviated ACLs can express more combinations of rights, subjects and objects than can Access Control Matrices **False**
- iii. (1 point) The principle of attenuation of privilege says that officers lower in the hierarchy of an organization should have fewer privileges **False**
- iv. (1 point) The principle of fail-safe defaults says that, unless specifically restricted, a subject is assumed to have a right over an object. **False**
- v. (1 point) The temporary elevation of privileges presents a security loophole. **True**

2. (5 points) Consider a computer system with three users: Alice, Bob and Cyndy. Alice owns the file *alicerc*, and Bob and Cyndy can read it. Cyndy can read and write Bob's file *bobrc*, but Alice can only read it. Only Cyndy can read and write her file *cyndyrc*. Assume that the owner of each file can read, write and execute it. Using rights read, write and execute, denoted r,w,x respectively, create the access control matrix.

Solution: The ACM is:

Table 1: Problem 1a: Chapter 2 from text, exercise 1a

| | <i>alicerc</i> | <i>bobrc</i> | <i>cyndyrc</i> |
|-------|----------------|--------------|----------------|
| Alice | rwX | r | |
| Bob | r | rwX | |
| Cyndy | r | rw | rwX |

For the above problem, also create the access control lists, and the capability lists.

Solution: ACLs are columns of the above matrix, and capability lists are rows.

ACLS are:

$$\text{ACL}(\textit{alicerc}) = \{(\text{Alice}, \text{rwX}), (\text{Bob}, \text{r}), (\text{Cyndy}, \text{r})\}$$

$ACL(bobrc) = \{(Alice, r), (Bob, rwx), (Cyndy, rw)\}$

$ACL(cyndyrc) = \{(Alice,), (Bob,), (Cyndy, rwx)\}$

Capability lists are:

$cap(Alice) = \{(alicerc, rwx), (bobrc, r)\}$

$cap(Bob) = \{(alicerc, r), (bobrc, rwx)\}$

$cap(Cyndy) = \{(alicerc, r), (bobrc, rw), (cyndyrc, rwx)\}$

3. (5 points) The state of Indiana has a new law requiring voters to produce photo identification. Proponents of the law claim that it will prevent voter impersonation. Its opponents claim that the law prevents low-income voters, who cannot easily obtain photo IDs, from voting. This law enhances one of the three qualities of integrity, confidentiality and availability of the voting system. Which one? In the process, it also reduces one of the qualities. Which one? Explain your answers.

Solution: This law improves the integrity properties of the system, because it makes it more difficult for an illegible voter to vote. It reduces the availability properties of the system, because it prevents those eligible voters, who are unable to get photo IDs, from voting.

4. (5 points) Consider a security policy of a voting system: only registered voters are allowed to vote, and only once. Consider a state where voters provide their names at a polling booth, the polling officer checks if they have already voted, and lets them in if they haven't. Is this enforcement secure? Broad? Precise? Briefly explain your answers.

i. Is it secure?

No. There is no way to detect if a voter is impersonating another voter who has not voted yet.

ii. Is it broad?

Yes. Because it is not secure.

iii. Is it precise?

No, because it is not secure, there is no question of it being precise.

5. (5 points) Consider RSA encryption with primes $p = 29$ and $q = 43$. The modulus is $n = pq = 1247$. (These numbers are, of course, too small to be used in a secure instantiation of RSA; however, they will do for the purpose of this test). A string of length 110 bits is encrypted. How long will the ciphertext be? Explain your answer.

Solution: The message can be at most 10 bits long, as the encryption can handle at most 1247 distinct messages, and an 11-bit message can take as many as 2048 distinct values, but a 10-bit message takes only 1024 values. The ciphertext for a 10-bit message string can be as large as 11 bits, because the ciphertext needs to be able to handle as many as 1247 distinct messages. Thus the plaintext consists of 11 messages of ten bits each, resulting in ciphertext of 11 messages of eleven bits each, hence the ciphertext is 121 bits long.

6. (5 points) Consider RSA encryption, **not** necessarily with the parameters of Problem 1. Suppose a string of n bits is divided into three substrings of size m each, and each substring is encrypted using Alice's private key. Suppose each substring corresponds to a sentence in English, and that the original message is $m = m_1m_2m_3$, consisting of the sentences: "Do the following in order. Enter your password. Enter your date of birth". Suppose the ciphertext is $c = c_1c_2c_3$, such that $c_i = E_a(m_i)$ where a represents Alice's private key. c is sent to Bob, but intercepted by an adversary before it gets to him. Describe an attack by the adversary to change the message sent to Bob so that he cannot detect the change in the message. How can this attack be prevented?

Solution: The adversary can send $c_1c_3c_2$. Decryption of each of the c_i will give the corresponding value of m_i but the original order will be changed. This attack can be prevented by hashing the entire message and encrypting it; that is, with a digital signature of the entire message, not individual blocks. See text, section 11.1.2.

7. (5 points) Consider the function f which takes n -bit strings to four-bit strings. Let $x = x_1x_2\dots x_n$ where x_i is the i^{th} bit of x . Let $f(x) = y = y_1y_2y_3y_4$ where y_i is the i^{th} bit of y . $f(x)$ is such that $y_1 = x_1 \oplus x_2 \oplus \dots \oplus x_n$, which is the XOR of all bits of x . $y_2 = x_1 \oplus x_3 \oplus x_5 \oplus \dots$ is the XOR of the odd-numbered bits of x , $y_3 = x_2 \oplus x_4 \oplus x_6 \oplus \dots$ that of the even-numbered bits of x , and $y_4 = x_3 \oplus x_6 \oplus x_9 \oplus \dots$ that of every third bit. Is f a secure hash function? Explain your answer.

Solution: No, f is not a secure hash function. Consider any value of $f(x) = y_1y_2y_3y_4$. Let $z_1 = y_2$, $z_2 = y_3$, $z_3 = y_4$, $z_5 = y_4$. Let $z = z_1z_2z_30z_5$. Note that $f(z) = f(x)$. Thus, one can efficiently obtain a pre-image.

8. Suppose you are to design a secure protocol for a sales transaction for an ecommerce website. You are required to assume that:

1. The buyer and seller have never met before and do not have a shared secret/key.
2. The buyer does not have a public/private key pair.

i. (3 points) What else do you need to know before you design the protocol?

Solution: Whether the seller has a public/private key pair. Note: just having a public/private key pair without a certificate does not help during communication, so it is always assumed that an entity with a public/private key pair has a corresponding certificate from a trusted authority.

ii. (9 points) Assume some reasonable answers for Part a and provide a protocol design. (you may use some space from the next page)

Solution: If the seller is assumed to have a public/private key pair: the buyer requests the certificate from the seller, checks the digital signature of the trusted authority, uses the public key to encrypt the sales request, the seller responds with a confirmation signed using his public key, this is checked by the buyer.

If the seller is assumed not to have the public/private key pair, the buyer initiates a Diffie-Hellman key agreement protocol; the key is then used to encrypt the sales request from buyer to seller, and

to encrypt the sellers' confirmation to the buyer.

iii. (**3 points**) What are the vulnerabilities of your design?

Solution: Vulnerability of the first protocol is variants of the replay attack; a nonce will address that. If the nonce is used, and example vulnerability is the compromise of the private key. Vulnerability of the Diffie Hellman key agreement is a man in the middle attack.