Course Name: ETHICAL HACKING

Assignment- Week 10

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following are examples of hardware-based attacks?

a. Side-channel attack.
b. Physical probing.
c. Denial of service stack.
d. SQL injection attack

Correct Answer: a, b

Detail Solution: In side-channel attack, some side channels (like delay, power, etc.) are monitored during some computation using some sophisticated measuring instruments, and as such requires access to the hardware that runs the computation. In comparison, denial-of-service and SQL injection are essentially software-based attacks.

The correct options are (a) and (b).

QUESTION 2:

For modular exponentiation computation of x^{25}, how many squaring and multiplication operations would be required?

a. 4 and 4.
b. 4 and 2.
c. 3 and 4.
d. 5 and 2.
e. 5 and 3.

Correct Answer: b

Detail Solution: The binary representation of 25 is 11001.

Thus, $x^{25} = x^{16} * x^8 * x^1 = (x^8 * x^4)^2 * x^1 = ((x^4 * x^2)^2)^2 * x^1 = (((x^2 * x)^2)^2)^2 * x^1$

This computation requires 4 squaring and 2 multiplication operations.

The correct option is (b).

QUESTION 3:

Which of the following is/are **true** for side-channel attacks?

a. They exploit weakness in cryptographic algorithm.
b. They exploit weakness in algorithm implementation.
c. They do not require physical access to the device.
d. It is used to encrypted ciphertexts for a number of given plaintext messages.

Correct Answer: b

Detail Solution: Side-channel attacks basically exploit weaknesses in the implementation (hardware or software) of an algorithm. It requires physical access to the device for measurement of some parameter.

The correct option is (b).

QUESTION 4:

Which of the following is/are **true** for simple power analysis?

a. In this analysis attacker directly uses power consumption to learn bits of secret key.
b. Using this analysis we can identify features like rounds of DES/AES, multiply in RSA exponentiation.
c. In this analysis the waveform is partitioned into two sets according to selected bits.
d. It relies on the use of a hardware Trojan in the circuit.
e. None of these.

Correct Answer: a, b

Detail Solution: In simple power analysis the waveform is examined to identify the bit stream/key, In this analysis the attacker directly uses the power consumption of bits, using this attack, attacker can identify number of rounds in AES/DES, multiply in RSA exponentiations. It is easy to defend. In counter to this Differential power analysis waveform is portioned according to bit stream and then the difference of the waveform is used for analysis. Power analysis attacks does not use hardware Trojan.

The correct options are (a) and (b).

QUESTION 5:

Which of the following strategies can be used to prevent timing analysis attack?

a. Make the computation independent of the input.
b. Package the chip in a temper proof casing.
c. Use highly secured cryptographic algorithm.
d. None of these.

Correct Answer: a

Detail Solution: Side channel attacks such as power and time analysis attacks exploit the weakness in the algorithm implementation. So if we use highly secure algorithm and do not implement it correctly then it can be exploited using side channel attack.

Side-channel attacks can be prevented by making all the branches in conditional statements symmetric with respect to computation (or in simple word making the computation constant irrespective of input pattern).

The correct option is (a).

QUESTION 6:

Which of the following is **not** a desirable property of PUF?

a. Given a PUF, it is hard to construct a procedure PUF', where PUF != PUF', and PUF'(x) = PUF(x) for all x.
b. Given only y and corresponding PUF instance, it is hard to find x such that PUF(x) = y.
c. Given PUF and x, it should be easy to evaluate y = PUF(x)
d. None of these.

Correct Answer: d

Detail Solution: All the given points are desirable properties of PUF.

The correct option is (b).

QUESTION 7:

PUF can be used for:

a. Security Primitive
b. Identification
c. Private/Public key pair generation.
d. None of these.

Correct Answer: a, b, c

Detail Solution: PUFs can be used for all given applications (refer week 10, lecture 49, slide number 9,10,11).

The correct options are (a), (b) and (c).

QUESTION 8:

Number of possible paths in 8-bit arbiter PUF will be _____.

Correct Answer: 256

Detail Solution: Arbiter PUF is composed of n two-port switching stages. For an n-bit challenge size, number of possible paths will be 2^n**;** for n= 8, number of possible paths will be 256.

The correct answer will be 256.

QUESTION 9:

Consider the following statements:

(i) Hardware Trojans are small modifications in the circuit.

(ii) It is used to reduce power consumption of a circuit.

a. Only (i) is true.
b. Only (ii) is true.
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are true.

Correct Answer: a

Detail Solution: A hardware Trojan is a small malicious circuit integrated with a normal chip which incurs small hardware overhead, and is difficult to detect. It does not lead to reduction in power consumption.

The correct option is (a).

QUESTION 10:

Which of the following statement(s) is/are true about Hardware Trojan?

a. It performs tasks for which it are designed or programmed.
b. It can replicate itself.
c. It does nothing harmful to the user's computer system.
d. None of these.

Correct Answer: a

Detail Solution: A hardware Trojan is a small malicious circuit integrated with a normal chip which incurs small hardware overhead, and triggers in some event; it cannot replicate itself.

The correct option is (a).

**************END*********