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 can be used as countermeasures to prevent hardware-based attacks?

a. Encrypt data stored in register and buses.
b. Add dummy circuit to generate random noise.
c. Provide authentication using PUF.
d. Use secure cryptographic algorithm

Correct Answer: a, b, c

Detail Solution: Typical Countermeasures to Prevent Hardware Attacks are: Obfuscate data in registers, generate random noise generator to prevent side-channel attacks, add metal mesh on top of the circuit, secret hiding, PUF. Use of cryptographic algorithms cannot protect against hardware base attacks.

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

QUESTION 2:

Which of the following statement(s) is/are ***false*** for side channel attacks?

a. They exploit some weakness in the algorithm.
b. They exploit some weakness in the implementation of the algorithm.
c. They require physical access to the device.
d. They only require the set of inputs/outputs to the algorithm.

Correct Answer: a, d

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. They are not dependent on the weaknesses of the algorithm. Moreover, they do not rely on applying inputs and observing the outputs only.

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

QUESTION 3:

Which of the following is/are typically exploited in side-channel attacks?

a. Electromagnetic emissions.
b. Timing analysis of an operation.
c. Space complexity of an algorithm.
d. Power consumed during computation.
e. All of these.

Correct Answer: a, b, d

Detail Solution: Timing analysis, power analysis, and EM emission analysis are very common in mounting side-channel attacks. It does not rely on the space complexity of the algorithm.

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

QUESTION 4:

For modular exponentiation computation of x^{13}, how many squaring and multiplication operations would be required?

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

Correct Answer: a

Detail Solution: The binary representation of 13 is 1101.

Thus, $x^{13} = x^8 * x^4 * x^1 = (x^4 * x^2)^2 * x = ((x^2)^2 * x^2)^2 * x = ((x^2 * x)^2)^2 * x$

This computation requires 3 squaring and 2 multiplication operations.

The correct option is (a).

QUESTION 5:

What does power analysis do?

a. It measures variation in power consumption during a computation.
b. It attacks the power supply and feeds new power supply to the circuit.
c. It relies on the use of a hardware Trojan in the circuit.
d. All of these.

Correct Answer: a

Detail Solution: Power analysis attack relies on measuring the variations in power consumption during execution of an algorithm. It neither tries to attack the power supply, nor it uses a hardware Trojan.

The correct option is (a).

QUESTION 6:

Which of the following statements describes the *unclonable* 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: a

Detail Solution: All the given points are desirable properties of PUF. The Unclonable property of PUF states that, given a PUF it is hard to construct a procedure PUF', where PUF ≠ PUF', and PUF'(x) = PUF(x) for all x.

The correct option is (a).

QUESTION 7:

Which of the following is/are applications of PUF?

a. Identification.
b. Key generation.

c. Side channel analysis.
d. Power analysis.
e. None of these.

Correct Answer: a, b

Detail Solution: PUFs can be used for enhancing security, authentication, Identification and key generation (refer week 10, lecture 49, slide number 9, 10, 11).

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

QUESTION 8:

Consider the following statements:

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

(ii) Hardware Trojans can be used for defensive purpose.

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

Correct Answer: c

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. Trojans can also be used for defensive purposes such as copyright protection.

The correct option is (c).

QUESTION 9:

In which of the following lifecycle stage(s) of an IC, insertion of the Hardware Trojan is not possible?

a. Specification.
b. Deployment.
c. Fabrication.

d. None of these.

Correct Answer: a, b

Detail Solution: The stage on which the Trojans cannot be inserted are specification, testing and deployment.

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

QUESTION 10:

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

a. It cannot replicate itself.
b. It is difficult to detect.
c. It does nothing harmful to the user's computer system.
d. None of these.

Correct Answer: a, b

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 is very difficult to detect hardware Trojans. Also, the hardware Trojans cannot replicate itself.

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

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