NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

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 is/are true for black box testing kind of attack?

a. It is an invasive type of attack.
b. It is a non-invasive type of attack.
c. The attacker has information about the implementation details.
d. It relies on weakness of implementation

Correct Answer: b

Detail Solution: In black box testing, the attacker sends an input to the circuit and receives an output. Based on the input/output behavior, the attacker decides what kind of algorithm is used inside. It is a non-invasive type of attack.

The correct option is (b).

QUESTION 2:

What are the typical countermeasures to prevent hardware-based attacks?

a. We obfuscate data in registers and buses.
b. We add preventive measures against side-channel attacks.
c. We provide authentication using physical unclonable functions.
d. We use a very secure cryptographic algorithm.

Correct Answer: a, b, c

Detail Solution: All of (a), (b) and (c) constitute countermeasures for the prevention of hardware-based attacks. Use of a secure cryptographic algorithm cannot prevent hardware-based attacks.

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

QUESTION 3:

Which of the following statement(s) is/are true 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: b, c

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 (b) and (c).

QUESTION 4:

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

a. Electromagnetic emissions.
b. Time taken to execute an algorithm.
c. The time and space complexities 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 time or space complexity of the algorithm.

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

QUESTION 5:

For modular exponentiation computation of x^{17}, how many squaring and multiplication operations would be required?

a. 4 and 4.
b. 4 and 2.

c. 3 and 2.
d. 3 and 1.
e. None of these.

Correct Answer: e

Detail Solution: The binary representation of 17 is 10001.

Thus, $x^{17} = x^{16} * x^1 = (x^8)^2 * x^1 = ((x^4)^2)^2 * x^1 = (((x^2)^2)^2)^2 * x^1$

This computation requires 4 squaring and 1 multiplication operations.

The correct option is (e).

QUESTION 6:

What does power analysis do?

a. It measures variation in power consumption during a computation.
b. It attacks the power supply and feeds power 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 7:

Which of the following strategies can help to prevent power analysis attacks?

a. The computation times in the different branches of conditional statements must be unequal.
b. The computation times in the different branches of conditional statements must be the same.
c. We can use a random noise generator in the circuit.
d. We obfuscate the scan chains in the circuit.

Correct Answer: b, c

Detail Solution: Power analysis attack can be prevented by making all the branches in conditional statements symmetric with respect to computation. It can also be prevented by using a random noise generator. It does not depend on the scan chains in the circuit.

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

QUESTION 8:

What is the meaning of PUF?

a. Perfect Universal Function
b. Physically Unclonable Function
c. Polynomially Unclonable Function
d. None of these.

Correct Answer: b

Detail Solution: The full form of PUF is Physically Unclonable Function.

The correct option is (b).

QUESTION 9:

Which of the following is/are true for hardware Trojan?

a. It incurs small hardware overhead.
b. It is stealthy and usually difficult to detect.
c. It relies on a number of malicious nodes to mount attacks.
d. It is used to reduce power consumption.

Correct Answer: a, b

Detail Solution: A hardware Trojan incurs small hardware overhead, and is difficult to detect. It does not lead to reduction in power consumption. Also, it is not used to mount attacks.

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

QUESTION 10:

What are some of the software-based countermeasures to prevent timing-based side-channel attack?

a. Use a structured programming language for implementation.

b. Mask the data representation.

c. Introduce redundant computations as required.

d. All of these.

Correct Answer: b, c

Detail Solution: To prevent timing attacks, we can use masking and also introduce redundant computations to make all the branches of conditional statements symmetrical.

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

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