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:

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

a. They exploit weaknesses in cryptographic algorithms.
b. They exploit weaknesses in algorithm implementations.
c. They do not require physical access to the device.
d. None of these.

Correct Answer: a, 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.

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

QUESTION 3:

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

a. Time required to carry out some computation.
b. Encrypted ciphertexts for a number of given plaintext messages.
c. Birthday attack of the hash function used.
d. Variation in power consumption during computation.
e. All of these

Correct Answer: a, d

Detail Solution: Timing and power analysis attacks are very common in mounting side-channel attacks. It does not rely on analysis of ciphertexts or mounting birthday attack on hash functions.

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

QUESTION 4:

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 squarings and 2 multiplication operations.

The correct option is (b).

QUESTION 5:

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

a. It requires a single measurement.
b. It requires multiple measurements.
c. It is more effective than simple power analysis.
d. It is less effective than simple power analysis.

Correct Answer: b, c

Detail Solution: Differential power analysis is more sophisticated and effective as compared to simple power analysis. Differential power analysis requires multiple measurements.. The correct options are (b) and (c).

QUESTION 6:

Which of the following can prevent power analysis attacks?

a. The computation times in the different branches of an "if" statement must be unequal.
b. The computation times in the different branches of an "if" statement must be the same.
c. Package the chip in a tamper-proof casing.
d. All of these.

Correct Answer: b

Detail Solution: Power analysis attack can be prevented by making all the branches in conditional statements symmetric with respect to computation. It does not require breaking the casing of the chip. The correct option is (b).

QUESTION 7:

What is the full form of PUF?

a. Perfect Unitary Function
b. Preset Until Fail.
c. Physically Undefined Function.
d. None of these.

Correct Answer: d

Detail Solution: The full form of PUF is Physically Unclonable Function. The correct option is (d).

QUESTION 8:

Which of the following is/are true for a PUF?

a. Physical properties of a device are used to generate a key, which is different from one manufactured device to the next.
b. The key is stored on-chip and is well protected.
c. The key obtained from the PUF can be modified as required.
d. None of these.

Correct Answer: a

Detail Solution: In a PUF, the key is generated exploiting the uniqueness in the challenge-response pairs of a device. The key is not stored anywhere in the device. The key as generated depends on device characteristics and cannot be changed. The correct option is (a).

QUESTION 9:

What is a hardware Trojan?

a. It is a form of PUF that can be used for attacking.
b. It is a malicious modification of the circuitry in a chip.
c. It is a form of PUF that is used for preventing attacks.
d. None of these.

Correct Answer: b

Detail Solution: A hardware Trojan is not a PUF. It refers to some malicious modification to the hardware, such that whenever some triggering condition becomes true, some unintended operation (called payload) is activated. The correct option is (b).

QUESTION 10:

Which of the following types of PUF can be used?

a. Ring oscillator PUF.
b. SRAM PUF.
c. FPGA PUF.
d. Programmable PUF.

Correct Answer: a, b

Detail Solution: Ring oscillator PUF and SRAM PUF are two types of PUF that can be used. The correct options are (a) and (b).

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