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 not an example of hardware-based attack?

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

Correct Answer: c, d

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 (c) and (d).

QUESTION 2:

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

a. Time required to carry out operations
b. Electromagnetic emissions from the device
c. Space complexity of the algorithm
d. Plaintext and Ciphertext
e. Power consumed during computation

Correct Answer: a, b, e

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 plaintext/ciphertext of the algorithm.

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

QUESTION 3:

Which of the following attacks on hardware are invasive in nature?

a. Black-box testing
b. Physical probing
c. Reverse engineering
d. Side-channel attack

Correct Answer: b, c

Detail Solution: Invasive attack → attack that needs direct physical access that alters or opens the chip/package.

Physical probing is invasive, it involves decapping the package or touching internal nodes with probes. Reverse engineering is invasive when it requires removing layers, imaging dies, or destructively extracting the netlist.

Black-box testing is non-invasive (tests only inputs/outputs). Side-channel analysis is typically non-invasive (measures power/timing/EM externally).

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

QUESTION 4:

Which of the following can be used as countermeasures to prevent hardware-based attacks?

a. Obfuscate data in register and buses
b. Add dummy circuit to generate random noise
c. Increase CPU clock frequency to make probing harder
d. Use secure cryptographic algorithm

Correct Answer: a, b

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 is essential for data security but cannot mitigate hardware-based attacks. Increasing the CPU clock frequency cannot prevent attacks like side-channel attack, it may make it easy due to high electromagnetic emission

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

QUESTION 5:

What is hardware Trojan?

a. A virus that infects software
b. A malicious change inside a chip
c. A tool used for testing hardware
d. A feature to make hardware faster

Correct Answer: b

Detail Solution: A hardware Trojan is a hidden malicious modification in a chip that can cause it to leak data or misbehave.

The correct option is (b).

QUESTION 6:

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 7:

Which of the following statement(s) is/are **false**?

a. Detection of hardware Trojans is relatively easy
b. No single method can detect all types of hardware Trojans
c. Hardware Trojan detection often involves high design, testing, or runtime overhead
d. Hardware Trojans are always inserted at the software level

Correct Answer: a, d

Detail Solution: Trojan detection is difficult; no single method can detect all types of Trojan; Trojan detection often adds significant overhead; Trojans are inserted at hardware level hardware.

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

QUESTION 8:

For modular exponentiation computation of x^{25}, 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: d

Detail Solution: The binary representation of 25 is 11001.

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

This computation requires 4 squaring and 2 multiplication operations.

Shortcut rule: Squaring → total bits – 1

: Multiplication → (#of 1's) - 1

The correct option is (d).

QUESTION 9:

What is the main purpose of Physical Unclonable Function (PUF) in hardware security?

a. To increase the clock speed of the processor
b. To provide device-unique authentication
c. To reduce the power consumption of chips
d. To improve signal transmission speed

Correct Answer: b

Detail Solution: PUFs exploit manufacturing variations to generate unique, unpredictable responses for each chip, making them useful for authentication and secure key generation.

The correct option is (b).

QUESTION 10:

Which of the following statements describe the evaluability 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: c

Detail Solution: All the listed points are desirable properties of PUFs. Option (a) describes the unclonable property, option (b) describes the one-wayness property, while option (c) correctly describes the evaluability property.

The correct option is (c).

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