Feedback — Quiz_week4

Help Center

You submitted this quiz on **Tue 10 Feb 2015 4:28 PM PST**. You got a score of **12.00** out of **15.00**. You can attempt again, if you'd like.

Question 1

True or false: In all side channel attacks, the attacker must have physical access to the system under attack to collect side channel information.

Your Answer		Score	Explanation
○ True			
● False	✓	0.50	
Total		0.50 / 0.50	

Question 2

True or false: Side channel attacks are passive, but they can be combined with active attacking methods to become more effective in breaking the system.

Your Answer		Score	Explanation
● True	✓	0.50	
○ False			
Total		0.50 / 0.50	

Question 3

True or false: The power and delay of different instructions are normally different.

Your Answer		Score	Explanation
● True	✓	0.50	
○ False			
Total		0.50 / 0.50	

Question 4

True or false: The power and delay of the same instruction on different oprands can also be different.

Your Answer		Score	Explanation
● True	✓	0.50	
○ False			
Total		0.50 / 0.50	

Question 5

True or false: The optical side channel attacks are rare because they require expensive equipment.

Your Answer		Score	Explanation
○ True			
● False	✓	0.50	
Total		0.50 / 0.50	

Question 6

True or false: Hitting different keys or key combinations on the keyboard will generate different acoustic traces. This can leak side channel information.

Your Answer		Score	Explanation
● True	✓	0.50	
○ False			
Total		0.50 / 0.50	

Question 7

True or false: When the secret data stored in cache or register is overwritten by other data, this memory load (or data overwriting) operation will not leak any information about the secret data.

Your Answer		Score	Explanation
○ True			
● False	✓	0.50	

Total		0.50 / 0.50	

Question Explanation

Overwriting a 0 with 0 and with 1 will take different amount of power.

Question 8

True or false: When the cache storing secret data is shared by other processes, it may introduce security vulnerabilities.

Your Answer		Score	Explanation
● True	✓	0.50	
○ False			
Total		0.50 / 0.50	

Question 9

Which of the followings, according to Kocher's 1996 paper, are necessary to launch a successful timing attack? Check all that apply.

Your Answer		Score	Explanation
☑ The execution time variations on the operations are measureable.	✓	0.50	
☑ The execution time variations on the operations are caused by different key values.	✓	0.50	
☑ A way to precisely identify the start and completion of the operation.	✓	0.50	
☑ The algorithm used in the crypto-system and some design details.	✓	0.50	
Total		2.00 / 2.00	

Question 10

Which of the following statements about differential power analysis (DPA) are true? Check all that apply.

Your Answer		Score	Explanation
☑ DPA does not require accurate power traces.	✓	0.50	
□ DPA needs to know the detailed implementation of the crypto algorithm under attack.	✓	0.50	
☑ DPA needs tools or skills to analyze the power traces.	✓	0.50	

□ DPA needs only a small amount of power traces when the crypto algorithm is running.	✓	0.50	
Total		2.00 / 2.00	

Question 11

Both Kocher's and Schindler's timing attacks can break RSA algorithm. Which of the following statements are true? Check all that apply.

Your Answer		Score	Explanation
☑ Kocher's timing attack targets the RSA decryption key.	✓	0.25	
□ Kocher's timing attack tries to factor n.	✓	0.25	
□ Schindler's timing attack targets the RSA decryption key.	✓	0.25	
☑ Schindler's timing attack tries to factor n.	✓	0.25	
Total		1.00 / 1.00	

Question 12

The following actions are needed to launch a scan chain based attack on a system with 5 flip flops. What is the correct order of the attack?

A. set TC=0, let the system run for one clock cycle.

B. set TC=1, read the output from scan out for 5 cycles.

C. set TC=1, send state information to the system via scan in for 5 cycles.

D. set TC=0, apply the input value at the system's primary input ports.

Your Answer		Score	Explanation
● C,A,D,B	✗	0.00	
○ C,D,A,B			
○ A,B,C,D			
○ D,A,C,B			
Total		0.00 / 1.00	

Question 13

Which of the followings can help to prevent side channel attacks? Check all that apply.

Your Answer		Score	Explanation
☑ Use dedicated power supply for the crypto units on the chip.	✓	0.50	this will make attacks that need to measure power and current trace harder.
□ Use sensor mesh at the top metal layer and continuously monitor all paths in the mesh.	✓	0.50	this is the countermeasure for invasive and semi-invasive attacks.
□ Add a digital watermark into the design.	✓	0.50	Most likely this will not affect side channel attacks. However, depending where on the chip, when during the design process, and how you insert your digital watermark, some characteristics of the chip and program execution such as power and delay may change. Point is given no matter you answer yes or no on this one.
☑ Restrict the physical access to the system (e.g., no entry within a certain distance, say 300 meters, of the system)	✓	0.50	
Total		2.00 / 2.00	

Question 14

$\phi(2015) =$ _____ (hint: factor 2015 to primes)

You entered:

5 * 13 * 31

Your Answer		Score	Explanation
5 * 13 * 31	✗	0.00	
Total		0.00 / 2.00	

Question 15

Which of the following statements about the randomized modular exponentiation (ME) are true? Check all that apply.

Your Answer		Score	Explanation
□ The three random numbers r_1, r_2, r_3 cannot have the same value.	✓	0.25	
☑ The random number r_2 cannot be 0.	✓	0.25	

□	The three random numbers r_1, r_2, r_3 must be primes.	✓	0.25
□	The randomized ME method avoids the modular exponentiation computation	✓	0.25
Total			1.00 / 1.00