Feedback — Quiz_week6

Help Center

You submitted this quiz on **Sun 22 Feb 2015 7:52 AM PST**. You got a score of **15.00** out of **15.00**.

Question 1

True of false: the endorsement key in TPM is a non-migratable key.

Your Answer		Score	Explanation
(•) True	✔	0.50	
( ) False			
Total		0.50 / 0.50	

Question 2

True of false: if the user provides the same password to different TPM chips, the same storage root key will be created.

Your Answer		Score	Explanation
(•) False	✔	0.50	SRK also depends on EK, which will be different for different TPM chips.
( ) True			
Total		0.50 / 0.50	

Question 3

True of false: all the TPM migratable keys are generated outside the TPM and thus they cannot be trusted.

Your Answer		Score	Explanation
(•) False	✔	0.50	MK can be generated both inside and outside of a TPM. It will be considered trusted by its creator.
( ) True			
Total		0.50 / 0.50	

Question 4

Which of the followings are functions of TPM? Check all that apply.

Your Answer		Score	Explanation
☑ generate pseudo-random numbers	✔	0.50	
☑ generate and store cryptographic keys	✔	0.50	
☑ store user passwords, encryption keys and digital certificates	✔	0.50	
☐ detect virus	✔	0.50	
Total		2.00 / 2.00	

Question 5

Which of the following PUFs are memory based. Check all that apply.

Your Answer		Score	Explanation
☐ Paper PUF	✔	0.50	

☑ Butterfly PUF	✔	0.50
☑ SRAM PUF	✔	0.50
☐ Ring Oscillator PUF	✔	0.50
Total		2.00 / 2.00

Question 6

Which of the following methods can make the RO PUF more reliable? Check all that apply.

Your Answer		Score	Explanation
☐ Use better methods or equipment to measure the delay gap more precisely.	✔	0.50	The precision of measurement does not matter, it is the delay gap that matters.
☑ Run the RO pairs for a longer time.	✔	0.50	Yes, running the ROs longer will increase the delay gap and thus make the RO PUF more reliable.
☑ Use error correction coding to correct the PUF bit flips.	✔	0.50	
☐ Use a small threshold for RO pair selection.	✔	0.50	should be using a large threshold

Total	2.00 / 2.00

Question 7

Which of the following features make the configurable RO PUF reliable? Check all that apply.

Your Answer		Score	Explanation
☑ Inverters that are sensitive to temperature or supply voltage can be excluded.	✔	0.50	Yes, at post silicon, we can test this and not select these "sensitive" inverters so the PUF will be more reliable under different environment.
☑ The configuration vector is selected after the chip is fabricated.	✔	0.50	Choosing the configuration vector in post-silicon phase will ensure that only the inverters that can increase the delay gap will be selected
☐ It includes all the inverters so the maximal delay gap can be achieved.	✔	0.50	Including all the inverters does not necessary maximize the delay gap. See the example in the lecture.
☐ One RO can use more inverters than the other to increase the delay gap.	✔	0.50	If two ROs do not have the same number of inverters, the one with more inverters will have longer delay, this will make it easier for an attacker to guess the PUF data. (This might be more of a security issue than reliability

	issue. But it is important to know this.)	
Total	2.00 / 2.00	

Question 8

Which of the followings need to be considered when a true random number generator (TRNG) is evaluated? Check all that apply.

Your Answer		Score	Explanation
☑ power efficiency of the TRNG	✔	0.50	
☑ the source of entropy for the TRNG	✔	0.50	
☑ complexity of implementing the TRNG	✔	0.50	
Total		1.50 / 1.50	

Question 9

When an FPGA system developer detects a hardware Trojan from the FPGA chip he has purchased, where the hardware Trojan may come from? Check all that apply.

Your Answer		Score	Explanation
☑ FPGA vendor who designed the FPGA chip	✔	0.50	
☑ Foundry that fabricates the FPGA chip	✔	0.50	
☑ EDA tool vendor whose design tool is integrated in the FPGA design environment	✔	0.50	
☑ IP vendor whose IP is included in the FPGA chip	✔	0.50	
Total		2.00 / 2.00	

Question 10

When Bob purchases an FPGA-based system, which of the following security vulnerabilities and attacks he should consider. Check all that apply.

Your Answer		Score	Explanation
☐ Reverse engineering that attempts to reveal the design information of the system	✔	0.50	

☐ Whether the FPGA configuration bitstream file is encrypted or protected	✔	0.50
☑ Hardware Trojan inside the FPGA-based system	✔	0.50
☑ User's sensitive information leaking from the system	✔	0.50
Total		2.00 / 2.00