This work is distributed under the CC BY-SA license, unless stated otherwise.

Hardware Security

15. Exam questions (tutorial)

Ján Jančár

Summer 2026

Today

Group activity

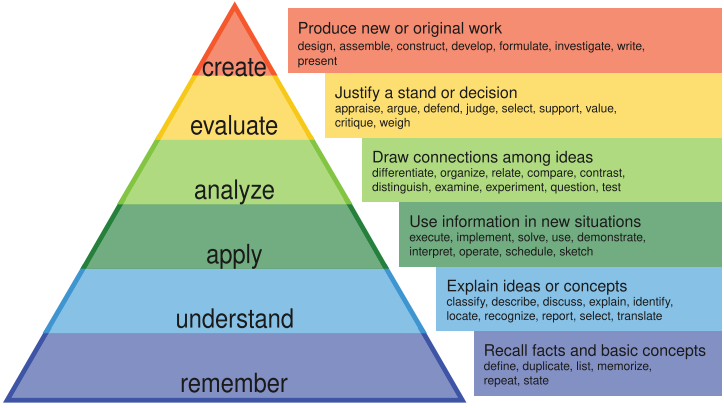
1. Creating questions
   - Each group gets a few topics (lectures)
   - Creates questions and grading rubric
   - Submits to PANDA and writes down
2. Answering questions
   - Groups exchange questions
   - Answers first without materials, then look
   - Submits answers to previous group
   - Previous group grades
     - Correct/Incorrect/Questionnable?
3. Discussing questions & answers
   - We go over questions from PANDA

Creating questions

- There are **good** and **bad** questions
- The questions should be
  - Not too easy (“*What is 2+2?*”)
  - Not too hard (“*Solve the Riemann’s hypothesis.*”)
  - Relevant (“*What did you have for lunch?*”)
  - Gradeable (“*Is a HSM better than a TPM?*”)

Creating questions

Bloom's taxonomy



Creating questions

Good questions

- (**evaluate**) *"A company's IT security team wants to upgrade their employee login system from Time-based One-Time Passwords (TOTP) to hardware FIDO2 authenticators. Justify this upgrade by detailing two distinct security vulnerabilities inherent to TOTP that WebAuthn/FIDO2 actively prevents. "*
- (**analyze**) *"A Hardware Security Module (HSM) detected physical tampering. List at least 2 possible responses and discuss their advantages/disadvantages."*
- (**apply**) *"A user leaves their laptop and U2F hardware token unattended on their desk. An "evil maid" wakes up the laptop, attempts a login to the user's account, and presses the flashing button on the hardware token when prompted. How does the modern CTAP2 protocol mitigate this exact physical attack vector compared to the original U2F standard?"*
- (**understand**) *"Explain how U2F achieves phishing/MiTM resistance. What role does the client have?"*
- (**remember**) *"A Trusted Execution Environment (TEE) provides"*
  - *A: code integrity, B: code confidentiality, C: data integrity, D: data confidentiality*

Creating questions

Bad questions

- "*What year was Kocher's seminal paper on Timing Attacks published?*"
  - Trivial, not-relevant
- "*Is masking or hiding better for side-channel defense?*"
  - Too broad, not answerable
- *"Design a perfectly secure crypto-coprocessor that blocks all power analysis attacks using hiding and masking.*"
  - Not possible

Creating questions

- Question text
- (Options)
- Correct answer
- Grading rubric

Phase 1 - Creating questions

Answering questions

- Now rotate questions between groups
- Keep the correct answers and grading rubric

Phase 2 - Answering questions

Phase 3 - Discussing questions & answers

Takeaways

- What are **you** taking away from this tutorial?
- What surprised you?