Software and Security Engineering: Supervision 2

Lectures covered by the supervision:

https://www.cl.cam.ac.uk/teaching/2324/SWSecEng/

- Lecture 4: Security protocols.
- Lecture 5: Attacks on TLS, from rogue CAs through side channels to Heartbleed.
- Lecture 6: The software crisis.

Past exam questions:
https://www.cl.cam.ac.uk/teaching/exams/pastpapers/t-SoftwareandSecurityEngineering.html

Supervision questions:

1. What are universal issues with proving your identity and access privileges? How are those mitigated or enhanced in digital systems?
2. Discuss and compare the following attacks:
   a. "Man in the middle" attacks.
   b. "No PIN" attack.
   c. "Preplay" attack.
3. Discuss with examples and compare the following security protocols (focus on ways for getting around these protocols, be creative):
   a. 2 factor authentication
   b. Kerberos security protocol
   c. EMV security protocol
   d. Public key encryption scheme
   e. TLS
4. Discuss the example of exchange of messages between Brutus and Anthony (lecture 5), in terms of authenticity and secrecy.
5. Discuss different types of bugs mentioned in the course. Sketch one example per discussed bug type.
6. Discuss what went wrong with NHS National Programme for IT. What kind of steps one could take to avoid these issues? How would you conduct such a project?
7. 2017p2q5 - https://www.cl.cam.ac.uk/teaching/exams/pastpapers/y2017p2q5.pdf
8. 2020p2q6 -https://www.cl.cam.ac.uk/teaching/exams/pastpapers/y2020p2q6.pdf (***ONLY*** c and d).
9. 2014p3q9 - https://www.cl.cam.ac.uk/teaching/exams/pastpapers/y2014p3q9.pdf (***ONLY*** a)
10. Summarize the main message from lecture 4 in 1-3 sentences?
11. Summarize the main message from lecture 5 in 1-3 sentences?
12. Summarize the main message from lecture 6 in 1-3 sentences?

Bonus task:

1. For the previously established project, create a script that is able to trigger build process and that is able to run all the tests. If you are working in Java, I suggest to use Maven. If you are working in C++, I suggest CMake. If the tests are successful, the script should create a binary and "deploy" it in a folder. Provide a link to the script. Provide the link to the script and instructions how to download it and run it.
2. Create a GitHub page for your project: https://docs.github.com/en/pages/quickstart Provide the link to the page.
3. Discuss quality requirements for your project.

Save your answers into MS Teams or email them to me. Please use the following naming pattern:

SASE_Supervision_2_Answers_<last name>_<first name>_Easter_2024

Send your answers as a pdf, doc, image, or any other format of a document for which there exists an easily available software to open.

Jasmin JAHIĆ
jj542@cam.ac.uk
https://www.cl.cam.ac.uk/~jj542/
https://www.cl.cam.ac.uk/~jj542/teaching.html