Week 3 exercise: The role of security tools in software projects

This week it won’t be a technical hacking exercise, but instead an essay on a topic that is fairly important in real life: What role do various security tools have in a real-life software project?

Software projects have multiple different activities and do not only concentrate on development and testing. There are customer and regulatory requirements that affect the functional and non-functional requirements, and may have security impact. Deployment and operational phases are also a part of software development. In modern software engineering, “DevOps” teams that are responsible for both development and operations further blur the area between software security and “IT security”.

The essay should look at what niche a software security tool would fill in a project, and which aspects are not helped by tools. It is easy for a company to spend a lot of money on a tool that is under-utilised or does not help in the big picture; on the other hand, not using automation may make some software security activities nearly impossible.

The reading list in this week’s course notes has several useful pointers, but in order for you to be successful in writing this essay, you should look at the following:

- Have a look at the BSIMM software security activity list at http://bsimm.com/online/. This is a list of software security activities that many companies have been observed as performing. Under each activity, there are a number of examples of how companies have actually done this.
- Have a look at Microsoft’s SDL process guidance at https://www.microsoft.com/security/sdl/default.aspx. You can click on the various phases of the SDL to see what sort of activities Microsoft would mandate in their development.

By the way, not everything in these sources is necessarily a good idea to do in your specific situation. Don’t interpret these as being the “truth” for all software projects. These are views and examples, some of the activities having more experience backing them up than others.

When reading, try to see the big picture by thinking about the following questions while you read.

1. Is there a specific type of software security activity that seems to be usually facilitated by use of tools or automation? Why do you think this happens?
2. Are there types of security activities that do not seem to be using any sort of tools or automation? Is there anything in common with these activities?

3. Would you expect some types of software projects to need less or more tools, or different kinds of tools? Examples of different projects would be:
   a. An agile (e.g., Scrum) project that develops a lot of entirely new code for Node.js;
   b. A maintenance project with a gigantic C++ codebase mainly written in 1992;
   c. A safety-critical project in Java for medical devices;
   d. An open-source project in C creating GNU GPL code on Github,
   e. A classified non-U.S. military project using Erlang.

The essay does not have to answer these questions directly, but they should help you to frame the essay question properly. Your essay should reflect on the complete software project (including requirements, design, deployment and operation) and not just the implementation and testing.

**Task:** Choose a commercial or non-commercial tool that is primarily marketed for increasing software security. The following is a short list of tools; you may select one of these, or something else (although it needs to be a tool that has a direct impact on software development; do not select a product such as a firewall, a VPN, an IDS or antivirus software, which are primarily used to purely support operations).

Example tools (or companies that provide tools) are provided below. Many of the companies make several tools and bundle them under various names. You can select the one you want.

Note that the University, or the lecturer, do not imply that any of the tools would be somehow bad or not useful. Listing a tool here also is not an endorsement. All trademarks are property of their respective owners.

Once you have selected a tool, read some of its marketing material. Things like feature lists, white papers, user guides, and demo videos would be useful resources. Make note of the arguments that it is being sold on, what it exactly does ("scanning" is a bit too high level description) and what is the tool expected to deliver.

Then, write an essay about where the tool would fit in increasing security in a software project. The essay should answer the questions:

- What does the tool, technically speaking, do? Is it clear from the vendor material? What questions are left unanswered that you would pose to the vendor’s sales representative if your company would be considering this tool?
- What types of risks does the tool mitigate? Do you think those specific risks would still have to be addressed in some other way, in addition to the tool?
- What is the tool useful for in a software project? What is it not useful for? What sort of image does the vendor convey for the usefulness in a project?
- What aspects of secure development are not addressed by introducing the tool?
- What sort of difficulties would you foresee when introducing the tool into a real-world software project? Do not restrict yourself to the technical ones - also think about business and human aspects, e.g., does it need security professionals to run, does it scale, etc.

To return:

- The essay.
- The essay should not cut-and-paste text from any vendor material. Use an academic quotation style if you need to refer to a specific statement found in the material. Do not include copyrighted material except through the normal fair use quotation exceptions. Otherwise let your own voice and opinion show through. **You are not judged for your opinion, but how well you make your case.**
- Avoid writing the essay in bullet points. Use complete sentences and think of it as prose and essay, not a list of responses to a list of questions. If you claim something, remember to back your claim up with either a reference to the material or at least your well-founded opinion based on your experience.
- Maximum length of an essay is 3 pages at 12pt font. Minimum length is when you think you’ve answered the questions sufficiently.
- Completed essays may be shared as examples between course participants.