Course Description

Web Trust and Security Project

Contents

The Big Idea

Within the domain of Web Science in general but also in the context of Web Trust and Security in particular, the initiation, definition, development, planning, executing, and evaluation of projects are essential for professional work. In many well-established areas of software development, models as the waterfall model or the V-model stand for the classical (sometimes outdated) approach. In contrast to this the projects in the context of Web Trust and Security are typically characterized by an iterative and more agile approach, like implemented by scrum, and take multiple perspectives into account.

Based on this kind of approach to performing projects special aspects of the other courses of this module will be deepened. The project work is being done in groups, each group working on different topics and consisting of presumably two to five students, depending on the number of participants. Due to the setup of the master programme, the students work from their habitations. As a consequence the work shall be organized based on web tools.

The project main focus is to exemplarily use the methods from the courses Web Security, Web Trust and Risk Management the achieve appropriate results in these parts of the project.

Intended Learning Outcomes

As a result of the course, participating students will become acquainted with the development of web projects with the focus on web trust and security. Especially they should be able to …

- have a deeper understanding of web trust and security
- define goals, identify threats and select appropriate methods to achieve the goals
- exercise appropriate methods to assure web security
- apply suitable methods to assess web trust
- design project specific risk management processes

Structure of the Course

The course ist structured into three phases

Kick-Off

Students develop and design case studies as projects in groups of up to five members. The objectives of the projects will be defined by the students themselves. For remote teamwork, students agree upon a collaboration infrastructure based on current Web 2.0 collaboration tools[1].

The case studies focus on Web based systems and their relevant Trust, Security aspects and Risk Management aspects. **The main activity is to conclusively derive security and trust measures from the overall goals of the project.** In particular this also comprises security and trust goals. Nevertheless security and trust goals also derive from the overall project goals (e.g. business goals). **Students apply the methods introduced in the other courses of this module.** In particular this includes the method of risk analysis introduced in the Web Security course.

Phase One: Group building and project idea

The Students form groups of up to fivemembers. They perform a brainstorming to develop an idea of a web based system to be designed and defined. The groups will develop an **Exposé** for their project idea, based on a detailed research on their topic. In Particular the Exposé contains a **Mission Statement** as a foundation for all following steps.

Phase Two: Concept

The groups develop a **Basic Project Concept**, containing:

- a detailed problem statement
- an outline of project specific challenges
- a detailed set of objectives for their project, in particular a relevant set of functional objectives, security and trust objectives (goals) deriving from the mission statement,
- related works

- an outline, what aspects the project will cover and first conceptualisations of possible problem solutions (definition of the scope)
- an impact analysis of the sketched solutions
- a discussion of project risks and a constructive discussion how the group will manage these risks
- a detailed project schedule.
- a risk analysis and
- a security concept.

The latter two points are the central results, form the principal part of the concept and need to be elaborated extensively according to the methods presented in the Web Security course. The other parts mentioned above are elaborated just briefly. To practice the concepts presented in the Web Trust course and/or the Risk Management course the students also elaborate in a well-detailed manner

- a trust analysis and if necessary a set of trust measures
- a project specific risk management process and a security policy

depending on the courses the group members enrolled in.

The groups continue to refine their solutions. Preferable results might be

- a conceptual model,
- a number of proof-of-concepts in order to evaluate existing software systems as candidates,
- or may lead even to an initial prototype.

Phase Three: Result presentation and discussion

In a third phase the project essence shall be presented on a set of slides, representing the key contents of the project as outlined in the phases above. Additionally students reflect on their findings during execution of the project. Structure and guidelines for slide presentations are result of students research on this topic. The resource for these guidelines is explicitly given before the presentation.

Didactic Concept, Schedule and Assignments

The course concept contains online workshops, online discussions, milestone meetings and audits. In addition there is an introductory and final on site presence.

Introductory lesson on site

Kick-Off: After a short repetition of the relevant course details specific projects concerning current topics in web trust and security will be presented. As a result of this introductory workshop the students will form groups and subsequently choose a project and herewith a relevant perspective. As an additional preparation for the introductory lesson the references given should be read.

Online sessions for the commitment on the project concepts

The online sessions are used by students presenting their intermediate results for the phases mentioned above. For each group at least one intermediate presentation covering Phase One or Phase Two is mandatory. For each Phase corresponding documents are uploaded into the course page as deliverables to be graded. Furthermore time slots for individual advice by the lecturer can be booked by each group. Point for discussion might be explanation of milestones, clarifications and so on. The subsequent performance of the projects depends on the individual project plans. Each group will have to define two milestones, where online status meetings are being held with the relevant course lecturer. The students report their progress related to the milestone definition. The results of each Phase are documented in written form and serve as a basis for grading. **It is the students task to bring forward the project an to generate progress. It is also the students task to identify necessary information and to request and obtain the information during the consultation times of the online sessions.** After the last Online session each group slests another group whose results are subject to a peer review. The allocation of the peer review groups follows the principle known from the Web Security course.

Wrap-up session on site

The projects are finalized by the on-site meeting, where the project groups present their work and discuss it with the course lecturer and the perspective lecturers. The session is performed as a plenary session and it is the purpose to motivate all participants to contribute also their views to the projects. The peer reviews follow each groups presentation.

Examination

Rating of the work performed

The project plan (concept and schedule) and its further development, the presentation document, the presentation during the wrap-up session on site, the contribution via peer review and the participation in the discussion serve as the base for the grade.

Criteria for grading

- The points depicted in the three phases serve as a checklist for quantitave and qualitative completeness
- Not only has the "speaker" of each group but also every member of the group to contribute to the presentation of the groups concept, the schedule and the various discussions.
- Since the project is to be performed by groups, each member of the group has to make a substantial contribution to the presentation, to be reflected in a speaking time of at least 10 minutes. Each member of the project team should spend nearly the same amount of time than the others during the presentation.
- The individual contentual contribution of each group member must be revealed in an overview table in **each** document delivered
- The overall quality of a presentation should withstand professional standards.

- The peer reviews should be well-founded, well-structured and concrete in an appropriate way.

References

↑ "List of collaborative software". Wikipedia. http://en.wikipedia.org/wiki/List_of_collaborative_software. Retrieved 2012-12-10.
[1] ANDREWS, Mike, WITTHAKER, James A.: How to Break Web Software: Functional and Security Testing of Web Applications and Web Services. Addison-Wesley Longman, Amsterdam 2006
[2] BROGAN, Chris; SMITH, Julien: Trust Agents – Using the Web to build Influence, improve Reputation, and earn Trust. John Wiley & Sons Inc., Hoboken, New Jersey 2010
[3] HADNAGY, Christopher: The Art of Human Hacking. Wiley Publishing Inc., Crosspoint Boulevard, Indianapolis 2011
[4] MICROSOFT CORPORATION: When to trust a website. http://windows.microsoft.com/en-us/windows-vista/When-to-trust-a-website (Retrieved 30/05/2012)
[5] O'HARA, Kieron; HALL, Wendy: Web Science. http://eprints.soton.ac.uk/265682/1/OHara-Hall-ALT-N-Web-Science.pdf (Retrieved 09/10/2017)
[6] SCHNEIER, Bruce: Liars and Outliers – Enabling Trust in a Society that needs to thrive. John Wiley & Sons Inc., Crosspoint Boulevard, Indianapolis 2012
[7] SCHNEIER, Bruce: Secrets & Lies – Digital Security in a Networked World. Wiley Publishing Inc., Indianapolis, Indiana 2004

27.02.2019