Course Description

Web Security

Contents

The Big Idea

Besides the obvious benefits of the Internet for our economy and our social life, fraud, cheating misuse and identity theft are terms often and easily associated with the internet. The discipline of Information Security, i. e. Internet Security, typically addresses this with classical security concepts which combine mostly technical security measures with additional physical and organizational measures. Despite of this, the number of computer crime cases still is rising[1]. The currently emerging discipline of web science intends to broaden the view on the internet. The web allows and generates a still growing interconnection of humans, services and information. Web science addresses the technical aspects of the web as well as the social and economic aspects [2]. This trend opens the door for the topics Web Trust and Web Security with a broadened view too. Web Security must address the technical aspects of secure web interaction und usage as well as the social and economic aspects of security in the web. Major fields of web security are the perception of security and risk by service and infrastructure providers i. e. the designers of web infrastructures. Furthermore the perception of security and risk by the interacting individuals is worth paying attention to. A better understanding of these aspects should result in more suitable systems as well as in more efficient and more effective security concepts. Another basic question is the general societal correlation between security and trust and the application of this correlation to the web. These topics are addressed in the first part of the course. The second part deals with secure web architectures and secure web applications in the classic way.

Intended Learning Outcomes

Students will become familiar with the social and technical aspects of Web Security. After passing the course students will be capable of

- analysing motivations and mechanisms for designing web security
- understanding the problems of perceiving Web Security and Web Trust
- understand and explain relevant aspects of the correlation between Web Trust and Web Security
- analyse and describe the motivation of attackers
- analyse and describe security requirements for typical web application scenarios
- select appropriate security measures and combine them into a scenario specific security concept
- finding the sources for current information on web security
- understanding of the most prevalent web attacks In-depth.

Structure of the Course

The course is divided into three parts. The first and introductory part addresses the Basics of IT-Security and Web Security by defining the terminology and describing the general approach of classical security analysis. The second part takes a closer view on some social and perceptional aspects of Web Security. In the third part, two exemplary web attacks are examined regarding their possible outcomes. Additionally applicable protective measures against these attacks are considered.

Introduction: Basics of IT-Security and Web Security

The general goal of IT Security is to reduce the risks of IT scenarios to a sustainable and manageable level by designing appropriate security concepts consisting of a combination of effective and efficient security measures on a technical, physical and organisational level. Web Security pursues this objective in designing secure web architectures and secure web applications. This objective can only be accomplished by describing scenario-specific protection goals, a structured analysis of vulnerabilities and the associated threats and risks. Profound knowledge of this structured approach and the necessary terminology are essential prerequisites for dealing with Web Security. This first part introduces the basic terminology and the general approach to security analysis.

Web Security and Web Trust

Perception of Security

Security analysis is amongst others based on threat and risk estimations of people performing the analysis. Individuals interacting inside the web have to rely on their security impressions of the systems they employ for interaction. Most users do not even recognize the security architecture of the systems they use. Security analysts as well as users must rely on their

subjective perception of the risks they are dealing with[3], [4]. Ongoing discussions on security and privacy in social networking platforms show the urgent need for a structured approach towards web security estimated from different views.

Correlation between Web Security an Web Trust

The web has become the infrastructure for an important part of human interaction and delivers plenty of benefits to its participants. On the other hand all negative aspects of human misbehavior automatically are transferred and become part of web culture e. g. fraud, cheating and misuse. The potential threat induced by this, is amplified by apparent or real anonymity of attackers as well as by national limitations in legislation enforcement across borders and national differences in law. These limitations reduce the possibility of trust relationships to be established across the web. Trust enabling measures known from our common social life must be replaced by other measures like security. There is a strong but complex correlation between Trust and Security in our societies [5]. This is true for the web as a societal subsystem too. The lessons learned from society in general can partially be transferred to the correlation between Web Trust and Web Security.

Attacks on Web Applications and Design of Secure Web Architectures

Considered from a security perspective the technical basis of the web, namely URLs, HTTP, HTML, CSS, JavaScript, and vendor specific plug-ins is full of loopholes. Only careful employment of the available elements can ensure a basic level of security. This part of the course gives a brief overview on two of the most prevalent attacks [6] and makes their results visible via live hacking a vulnerable web server [7]. Details on these exemplary attacks called Cross Site Scripting and SQL injection as well as protective measures are discussed in [8] .

Didactic Concept, Schedule and Assignments

The learning concept combines on site lessons, online workshops and home working. An introductory on site workshop provides basic knowledge and serves as a starting point for discussions during later online workshops. The online workshops are structured in a highly interactive matter, hypotheses are constructed, open questions will be discussed inside the learning group. Three online workshops are organized on three evenings as synchronous events with a duration of three hours each. Preliminary asynchronous work is performed through discussions and clarifications via E-mail, discussion forums and other tools in the learning platform. The referenced resources build up the foundation for professional discourse during the online sessions. Depending on the number of participants 1 to 5 students each form a learning group to prepare the required readings and to evaluate the findings of the online sessions afterwards.

Introductory On Site Session

Initially the first on site session starts with organizational course details and a lecture introducing the basic terms and definitions of IT security and web security. Especially the concepts of

security objective, vulnerability, threat and risk are introduced. The basic concepts are illustrated by examples familiar to the students. Practical usage of new terms is performed during a small case study on security analysis. The key data of the case study is presented by the lecturer. The on site sessions ends with the assignment of readings and tasks to perform based on the readings.

1st Online Workshop

Prerequisite for the 1st Online Workshop are the contents of [3], [4] and selected chapters of [5]. For the on line workshop the students prepared hypotheses which outline the contents of the required readings from their perspective. The results become subject of a peer review and are discussed inside the learning group under sufficient assistance of the lecturer.

2nd Online Workshop

The 2nd Online Workshop deals with the technical aspects of web security. As a preparation for this workshop the students read a selected chapter of [8]. The skills gained by this are applied to a case study for a secure web application. Selected students present their results. Selected questions, assumptions and hypotheses will be discussed and clarified.

3rd Online Workshop

The third workshop is designed as an interactive live hacking event. Selected students present their attacks prepared on the basis of [6] and [8]. The WebGoat server [7] is prepared by the students inside a local virtual machine. In case of severe technical obstacles, a server reachable via the internet provided by the lecturer can be used for demonstration.

Wrap-up session on site

This on site workshop is dedicated to summarizing the students impressions and findings of the course. Especially potential outcomes for attack victims of the 3rd online workshop are discussed, as well as possible countermeasures from the system architects point of view and the users view. The session ends with a written examination of 45 minutes duration.

Examination

During the concluding on site appointment a written examination for the module is to be passed. This course contributes tasks corresponding to 45 minutes working time.

References

↑ ""German Cybercrime Statistics". https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html. Retrieved (08.10.2017).

↑ "[O'Hara, K., Hall W., Web Science, http://eprints.soton.ac.uk/265682/1/OHara-Hall-ALT-N-Web-Science.pdf "Web Science"]. O'Hara, K., Hall W., Web Science, http://eprints.soton.ac.uk/265682/1/OHara-Hall-ALT-N-Web-Science.pdf. Retrieved (09.10.2017).

↑ ""Schneier, B., The Psychology of Security". April 08, 2012. http://www.schneier.com/essay-155.html. Retrieved (Retrieved 08.04.2012).

↑ "[Schneier, B., How the Human Brain Buys Security, 2008, http://www.schneier.com/essay-232.html "Web Science"]. April 09, 2012. Schneier, B., How the Human Brain Buys Security, 2008, http://www.schneier.com/essay-232.html. Retrieved (Retrieved 09.04.2012).

↑ Schneier, Liars and Outliers, B. (2012). Enabling Trust in a Society that needs to thrive. Wiley & Sons, Indianapolis, 2012.

↑ "OWASP Top Ten Project,". https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Retrieved April 12, 2010.

↑ "OWASP WebGoat Project,". https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project. Retrieved April 12, 2010.

↑ Witthaker, and Andrews, M., J.A. (2006). How to Break Web Software: Functional and Security Testing of Web Applications and Web Services. Addison-Wesley Longman, Amsterdam.

27.02.2019