Towards a Practical Approach for Teaching IT-Security

Florian Barth
University of Mannheim
Mannheim, Germany

and

Matthias Luft
ERNW GmbH
Heidelberg, Germany

Abstract

Research and teaching IT-Security is getting more and more attention in the light of an increasing number of incidents. As the practical application of knowledge and techniques in this area necessitates creative ways of solving complex problems, special attentions has to be payed to the modus operandi of teaching. The teaching efforts of the student IT-Security team of the University of Mannheim - squareroots - will be the focus of this paper. Results and experience from teaching a course in IT-Security will be analysed regarding the efficiency of the applied teaching methodology.

Keywords: Hacking, Capture-The-Flag, IT-Security, Teaching, Challenge-based Learning

1 Introduction

IT-Security, specifically Information Security, is getting more and more attention in industry [1]. With recent events, such as hacking groups breaking into corporate networks and exposing private information of customers and the company itself [2, 3], as well as, recent attacks on federal networks (e.g. FBI and Department of Justice), IT-Security is gaining even more attention. Due to the rapidly evolving nature of this area of expertise it is of great importance to offer adequate ways of introducing people into the area and allowing them to keep track with the state-of-the-art in relevant attacks and defensive techniques [4].

As Erickson points out in his book [5],

> Hacking is the art of creative problem solving, whether that means finding an unconventional solution to a difficult problem or exploiting holes in sloppy programming.

Thus, it is of minor use to teach common attack techniques and defensive measures to people dealing with IT-Security, but it is of great importance to give them insights into the way of thinking of a potential attacker. Being able to take the attacker's perspective and to solve the problem of attacking a system or application enables the person doing this to think about ways to defend the system and anticipate evasive manoeuvres a potential attacker may conduct.

Inspired by a course taught at the University of Mannheim, the so-called "Hacker Praktikum", a group of students, including the authors, started with their research and competitive activities in IT-Security under the name "squareroots" in 2006. In the early days the main activity was participation in IT-Security contests called Capture-The-Flag (CTF) contests. In these competitions, the participating teams are faced with synthetic, but realistic, security-related challenges, covering code analysis, forensics, networking, reverse engineering, and many more. Although, being an extracurricular activity, the team members spent much time on broadening their knowledge in related topics, sharing this knowledge with fellow team members, and, of course, participating in CTF competitions. In the following competitions the effort that was spent by the team resulted in successful participations in numerous competitions, e.g. 2nd place in iCTF 2007 or 1st place in RuCTF 2009. As

the team evolved the squareroots started offering penetration testing and server hardening services to the university and external parties. Apart from internal teaching in small groups, the team started to support the regular curriculum at the University of Mannheim by giving an exercise in "Applied IT-Security".

As more and more founding members graduated, the team was faced with decreasing number of regular participants. Thus, the idea of offering an extra-curricular weekly course "Introduction to IT-Security" was born. The students of the university were offered the possibility to be introduced to the field of IT-Security, while the team was able to train potential future team members and, thus, secure the future existence and success of the squareroots.

In order to motivate the goals of our teaching efforts, the next section will describe the previous knowledge of the students participating in the workshops and the environmental characteristics encountered in a CTF. Then we will lay out the specific capabilities derived from these characteristics. In Section 3 the layout of two iterations of the IT-Security course will be presented and then analysed regarding to its success in reaching the goals stated before. In Section 4 we will then conclude the paper by summarising the experiences from the teaching activities and will give an outlook into further work.

2 Goal of Teaching Efforts

The following section will lay out the goals of our teaching efforts, starting with an overview of the previous knowledge and skills of the students in the area of IT-Security, the properties of a CTF, and the derived abilities needed for a successful participation in such an event.

2.1 Previous Knowledge

The fields of study and degrees at our university that have a focus on computers science comprise a bachelor degree and a master degree in information systems. The bachelor students participate in a mixed curriculum consisting of foundations in information systems, computer science and economics. Due to this heterogeneous curriculum, the security-related knowledge of the bachelor students participating in our workshops is rather limited. In most cases they got a general introduction into the foundations of computer science and software development. The consecutive master degree that is offered, allows the students to focus on their preferred fields of study with the option to choose from a wide range of potential courses. As IT-Security is also included in the range of courses, the students often have an idea of IT-Security, relevant concepts and technologies.

2.2 Capture The Flag

A Capture-The-Flag (CTF) competition is a team-oriented, usually distributed IT-Security exercise. The most important academic CTF contest is organised by Giovanni Vigna as part of his IT-Security course at the University of California Santa Barbara (UCSB) [6, 7]. The basis of the competition is a hard drive image of a virtual machine that is distributed to the teams. Each image consists of an operating system, Linux or BSD flavored in most cases, and 5 to 10 services that offer some kind of functionality. During the competition a server of the event host, the game server, connects to the services of the teams and uses them to store data, so-called flags. An example for such a service would be a simple web-shop, where the flag, in most cases a hash-value, is stored in the customer information, e.g. as credit card number. The goal of the competition is twofold: to steal the flags of the other teams and to protect own flags from being stolen by the other teams. The services are custom-made and in most cases cover different programming languages ranging from wide-spread languages, e.g. Java, Perl, PHP, to exotic languages like Whitespace, Brainfuck or even custom-made languages. Thus, the teams have to analyse the source code or binary data of the services and find vulnerabilities that allow stealing flags, develop exploit code for these and fix the vulnerability in their own service instances. Due to the custom nature of the services the usage of automated tools which do not require actual research do not reveal any vulnerabilities. The idea of so-called quests, small challenges from the areas of forensics, reverse-enginneering or puzzling is another common part of CTF competitions. The submission of flags and solutions for quests are handled by the game server which also assigns the achieved scores to the corresponding teams. Since the early days, a vivid scene of CTF teams and competition organisers has involved and led to an active community. Alternative modus operandi for competitions evolved, ranging from pure quest-based CTFs, CTFs that focus on certain skills (e.g. reverse engineering, language devleopment, etc), to competitions that operate on real-world system with real-world services. The most famous academic CTF, the UCSB International CTF (iCTF), organised by Giovanni Vignas team, also was reworked due to some emerging problems from having experienced teams playing against teams new to the concept of CTF . As he stated in an interview with Telepolis [8], "And then the teams are put into the lion's den CTF and are disintegrated in seconds by the other teams". Thus the iCTF always features unique concepts different from the classic CTF setting, like stealing money instead of flags from a hypothetic bank, drive-by exploiting of simulated browsers, penetrating a corporate network in order to steal secret information, and many more. Overall, the teams that participate in a CTF competition are faced with various and dynamic challenges. The fast pace of the game makes it a necessity to quickly adapt to the modus operandi of a compe-

tition and to quickly apply their programming and exploitation skills as well as quickly adopting uncommon or even unknown programming languages. The custom services require both a broad an in-depth understanding of common vulnerabilities, since they have to be reveal manually. For example, typical signature based black-box vulnerability scanner do not reveal any vulnerabilities, since the services are custom made for the CTF and therefore no signatures exist.

2.3 Goal

Based on the intrinsic properties of CTF competitions the goals of our teaching efforts are as following:

- Capability to quickly adapt dynamic settings
- Capability to quickly get insights into unknown techniques and technologies (e.g. new types of vulnerabilites)
- Vulnerability-oriented mind set
- Team and Communication Skills
- Ethics

The first three capabilities address the ever changing environments of CTF. It is not unlikely that rules are changing during a competition or that new, unknown services are released. These changes, in turn, often comprise new, unknown technologies which must be understood quickly. Therefore our teaching methodology strive for the development of as much self-learning skills as possible. Even though our workshops prepare the participants for a broad field of skills, specialised sub-teams are formed during a CTF. In order to allow an effective cooperation during the CTF and the efficient sharing of knowledge, the development of team and communication skills is important. As part of the workshops is teaching offensive techniques to the participants, of course, bringing a mindset of ethics regarding the application of these techniques is of great importance.

3 Teaching Methodology

As described before, in the beginning our team consisted of students that took part in a seminar dealing with practical approaches on IT-Security. Over time the team grew by recommendations from team members to interested individuals. When the core members of the team finished their degrees and started their work-life the team was at the edge of dissolving due to decreasing number of active members. In this time the idea of sharing our knowledge with interested students and, thus, acquire new team members was born. The need for the acquisition of new members also results from the course orientation of our university, which is not strictly technical (refer also to Section 2.1). The following section will present the evolving teaching concepts we applied, reflect on their effectivity and give a short evaluation for each.

3.1 Lecture-based Teaching

In our first attempt to introduce students to the area of IT-Security we created a set of topics that might be of interest to the students, that are relevant for a CTF, and that are also useful for further investigations into this area of research. These topics presented an overview of common attack vectors, how to exploit them, and how to secure an application against these attacks. These topics comprised for example lectures on reverse engineering, SQL injection, automated code analysis, or scripting languages.

As the early members of the team got to know the techniques mentioned above in lectures at the university, we layed out our teaching events in the form of lectures with small examples for the students to practise. In a first step we motivated and presented the idea of a specific attack vector combined with a small introductionary example. This was followed by common counter-measures and possible ways to circumvent these counter-measures.

3.1.1 Analysis

The observations from the first iteration will now be presented and be analysed respective to the goals specified in Section **??**. From the first iteration described in Section 3.1 people made it to be a member of the team. The following analysis is based on interviews and discussions with the new team members and old team members reflecting on the performance of the new members in their first competitions.

- **Capability to adapt to dynamic settings**
  The new members had a hard time applying the learned knowledge about vulnerabilities to specific software source code during the first CTF contest. Contest environments do not allow to simply applying pre-made recipes and or allow the application of static checklists to solve problems. Since the workshops were lecture-based, the participants tried to apply the content presented in the slides directly to the presented contest challenges without having understood the actual nature of a specific vulnerability.
- **Capability to quickly get insights into unknown techniques and technologies**
  As for the general problem solving skills, unknown languages, concepts, architectures, or even vulnerabilities were not properly assessed. The lecture slides were used as a single source of reference and the participants did not

exhibit comprehensive research skills when facing new technologies. Without extensive preparation for a specific problem set, it was hard for them to get accustomed to new technologies based on documentation, information sources on the Internet or even to finding these sources. According to this lack of understanding, a lot of time was invested to research unimportant details since it was assumed that it would improve the overall understanding. Therefore the lecture-based setting did not give a foundation to understand new concepts and see the "big picture" in a dynamic environment.

- **Team and Communication Skills**
  Following Einstein's approach of "if you can't explain it simply, you don't understand it well enough", people were used to get well-thought explanations which were easily understandable. However these explanations and the corresponding presentation did not enable them to ramp up as a team in the beginning of a CTF phase, take the initiative to research on new problems, or to compose a team which researches a new vulnerability. Additionally, a CTF requires strong team processes for documentation, communication, and collaboration which were not communicated in the lecture-based teaching. As time is a crucial factor during a CTF contest, this increased communicational overhead, long ramp up sessions, lost information due to a lack of communication, or missing initiative which in turn required interaction and therefore time of other team members lead to severe loss of scores during several contests.

- **Motivation**
  Both the lectures as well as commitment to the team is extra-curricular. Since the bachelor and master programs do not leave much time for such activities, it was hard to motivate the students to go to additional lectures which aren't even accredited for their degree program. This leads to a high drop out rate or at least a lack of willingness to do research or post-processing of the lectures on their own. This fact became even more important since people joined the lectures with the expectation to learn interesting hacking techniques in the short run and then realised that it is hard work following scientific principles.

- **Ethics**
  Offensive IT-security is closely connected to an important ethical mindset which enables participants to understand consequences of the learned techniques and the potential impact a vulnerability may have. This mindset could not be taught by the pure lecture-based approach, since it is hard to spark interest in such a – from a beginner's point of view – rather theoretical topic. As there was not direct discussion or contact between the lecturer and the students, it was hard to encourage them to think about possible actions and their results.

3.2 Workshop-based Teaching

After the first CTF participation, our core teaching team summarised the problems described in Section 3.1.1 which resulted in a rigorous re-design of our teaching approach. The new concept should address the mentioned topics in a way which motivated the participants and lead to the willingness to deeply commit to the workshops and spend a lot of time on the solving of the workshops. Therefore we decided to develop a series of workshops which covers different IT-security topics. Each workshop comprises three levels of challenges, analogous to video games, which have to be solved in order since each level contains hints and communicates skills for the next levels. In addition to the three levels, a so called "hack-it of the week" was implemented, which was a exceptionally hard challenge. Each of the challenges contains a so-called secret which has to be found and is represented by a random string (e.g. "e07910a06a086c83ba41827aa00b26ed"). These secrets can only be retrieved when the vulnerability of the challenge is exploited successfully. Each vulnerability is designed in a way that communicates important IT-security and CTF skills in order to ensure that participants, who successfully solve all workshops, are well prepared for CTF participations or even professional activities in the IT-security industry. The retrieved secret may then be submitted to a web-application which keeps track of the score of each participant, the so-called scoreboard. This scoreboard also provided a list of the top scoring participants in order to provide a competitive situation. In addition to this factor, a final CTF contest was designed and only the top scoring participants were allowed to participate in this contest.

Each workshop comprises 90 minutes and implements a simple pattern. Initially, a short introduction on the security concept of the week is given in ten to 15 minutes providing basic information. These information are enough for an abstract understanding, but not to solve all challenges. This approach requires the participants to do intensive research on their own in order to be able to solve all provided challenges. At the end of each workshop, some more information about the challenges – yet no complete solution – is provided within five to ten minutes in order to discuss the gathered results in the group and to provide further information for participants who struggled finding any of the hidden secrets.

During the workshops, all of our instructors helped the participants to solve the challenges in a way that pointed them in the right direction and enabled them find the actual solution on their own. During all workshops, no complete solutions were provided.

3.2.1 Analysis

The new concept addressed most of the problems described in 3.1.1. The close contact of the instructors with the participants also lead to a tight integration of new participants in the existing team structures. It was also possible to motivate people, based on the exemplary behaviour of the instructors, to interact with each other and to explain solved challenges in a way that did not reveal the actual solution. In addition, a mailing list was provided to enable the participants to continue this interaction also for the hack-it of the week challenges. The new approach solved the most urgent problems of lacking the skill to quickly adapt new situations and understand new technologies or vulnerabilities. As Section 4 lays out, future iterations of the workshop will set a focus on concrete team building challenges as well as ethical aspects, which by now could only be taught by exemplary behaviour of and interaction with the instructors.

4 Conclusion and Further Work

During the course of this paper the evolving teaching approaches of an active group of IT-Security-focused students and post-graduates has been laid out. As the teaching efforts had a focus towards ramping up students of computer science for the successful participation in a Capture-The-Flag competition, the expected environment and the accompanying characteristics served as a motivation for the teaching activities. In two case studies the teaching methodology and the results of the specific approaches were presented and analysed regarding the fulfilment of the goals described before. Based on these observations the following conclusions are drawn:

- **Enabling learners to help themselves**
  The teaching of ”recipes” and static processes will not prepare students for a CTF competition. As mentioned in the analysis, the students where overburdened by the dynamic nature of such a competition as well as by the unexpected challenges and changing goals. By having a strong focus on encouraging learners to solve problems by themselves before asking for help or the sample solution, they were well prepared for tackling unexpected challenges and solving complex problems. The availability of self-teaching resources (i.e. tutorials and articles) dealing with IT-Security problems, especially on the world wide web, is sufficient to rapidly ramp-up in this area of expertise.
- **Creation of competitive setting**
  Teaching extra-curricular courses makes effective motivational incentives a necessity. Especially in the are of IT-Security people seem to be attracted by the idea of getting introduced into the ”mystic world of hacking” and, thus, being part of an appealing and mysterious community. However, when they realise, that there is no magic involved, but hard work und commitment, they tend to drop out, if there is no motivational mechanism. By focusing on practical exercises and by introducing the scoreboard-based reward system, the motivation of the students was sustained and they even invested much of their time to solve even the very difficult brain teasers.
- **Encourage collaboration and open discussion**
  Having introduced the competitive setting there was a fear of a rather fierce competition and uncooperative atmosphere. Thus, the lecturers were encouraging open discussion and cooperative problem solving during the exercises. Fortunately, the students realised that sharing knowledge and explaining problems and solutions to their co-learners allowed them to deepen their knowledge, exchange insights and solve complex exercises by cooperating. Some of the exercise were also designed to be solvable only by cooperation of multiple participants.

Following these guiding themes, our IT-Security, the squareroots, were able to solve the problem of graduating members leaving the team due to a change in life and location. The team members are motivated and the frequency of participation in different flavours of CTF competitions, as well as, the success in these competitions further encourages them to keep dedicating their time and potential to IT-Security. Furthermore, the team broadened its expertise and field of research. Active research is done with a focus on processes and tool support for CTF competitions. The knowledge gained during this research is also applied to penetration tests, the team offers to interested parties, thus, transferring the knowledge to real world applications and scenarios. Repeated success in a competition based on real-world infrastructure and security problems, called Packet Wars [10], shows the applicability of problem solving capabilities from synthetic, academic competitions to real world problems being effective [11]. The team is also active in communicating their perception of IT-security to the public. In so-called ”Science Slams” members of the team were successful in explaining topics related to Hacking and IT-Security to an audience that is not related and unaware of the real-world implications of this field of research.

The teaching approaches developed during the multiple iterations of the workshops is being applied in regular basis, thus, allowing interested students to get to know this field of computer science and allowing them to get full members of the team participating in competitions. Many choose to focus their studies in the are of IT-Security and later on aspire to work in this area either in academia or in industry. Having the connections to practitioners offers the possibility to transfer knowledge from their professional experience back to academic domain and offers the possibility of being able to offer internships for interested students, thus, further encouraging them to

commit.

At the moment the author's are planning to extend the approach to another field, by creating an e-learning solution evolving around teaching programming languages based on the condensed guiding themes as in the IT-Security workshops. This approach will be aimed towards unexperienced students that want to ramp-up their programming skills. The idea is to present them with programming exercises integrated into a social networking platform, thus, allowing the students to share their knowledge, keeping up motivation by integrating competitive aspects in the form of scores and achievements, and encourage them to help each other. Furthermore, the current security-related teaching approaches are being refined with the goal of strengthen the importance of collaboration and team work, as well as, introducing a separate workshop with an extended discussion regarding ethical topics.

References

[1] Aurora IT, Information Security a Priority at Fortune 1000 Organizations, http://www.aurorait.com/pdfs/IS-fortune-1000-whitepaper.pdf, retrieved Feburary 2012.

[2] Forbes, Anonymous Takes Revenge On Security Firm For Trying To Sell Supporters' Details To FBI, http://www.forbes.com/sites/parmyolson/2011/02/06/anonymous-takes-revenge-on-security-firm-for-trying-to-sell-supporters-details-to-fbi/, retrieved February 2012.

[3] Telegraph, Millions Of Internet Users Hit By Massive Sony PlayStation Data Theft, http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html, retrieved Fabruary 2012.

[4] ISC2, The ISC2 Global Information Security Workforce Study, https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC\%20Study_020811_MLW_Web.pdf, retrieved February 2012.

[5] J. Erickson, Hacking: The Art of Exploitation, No Starch Press, 2008.

[6] G.Vigna, Teaching Hands-On Network Security: Testbeds and Live Exercises, Journal of Information Warfare Vol. 3, No. 2, 2003, pp. 8–25.

[7] G. Vigna, Teaching Network Security Through Live Exercises, Proceedings of the Third Annual World Conference on Information Security Education (WISE 3), Monterey: Kluwer Academic Publishers, 2003.

[8] Telepolis, "Die Russen sind wirklich gut, http://www.heise.de/tr/artikel/Die-Russen-sind-wirklich-gut-276415.html, Retriever Feburary 2012.

[9] C. Cowan, S. Arnold, S. Beattie, C. Wright, and J. Viega, Defcon Capture the Flag: defending vulnerable code from intense attack, DARPA Information Survivability Conference and Exposition, Vol. 1, 2003, pp. 120–129.

[10] Packetwars, Information Warfare Simulation, http://packetwars.com/, retrieved February 2012;

[11] S. Bratus, What Hacker Research Thaugh Me, Troopers, 2010.

Towards Practical Differential Privacy for SQL Queries. Noah Johnson. University of California, Berkeley.Â We build FLEX, a practical end-to-end system to enforce differ-ential privacy for SQL queries using elastic sensitivity. We demon-strate that FLEX is compatible with any existing database, can en-force differential privacy for real-world SQL queries, and incurs negligible (0.03%) performance overhead.Â Cur-rent approaches for data security and privacy cannot guarantee pri-vacy for individuals while providing general-purpose access for the analyst. As demonstrated by recent insider attacks [7, 8, 10, 11], allowing members of an organization unrestricted access to data is a major cause of privacy breaches. My approach would include my beliefs and values. It includes any positions I take on classroom issues. In addition, any pedagogy theories that I espouse will be included. Basically, you can consider it my overall perspective on teaching.Â I would say that my approach to teaching is my overall philosophy of teaching. My approach would include my beliefs and values. It includes any positions I take on classroom issues.Â As such, methods are the practical applications of my teaching approach. Again, as an example, Iâ€™m currently teaching a Greek mythology unit in which my students are researching Greek mythology to design a classroom website in groups. I have given them control over several choice options within the project as to both content and product. Approaches, methods, procedures, and techniques Approach : this refers to â€œtheories about the nature of language and language learning that serve as the source of practices and principles in language teachingâ€. It offers a model of language competence. An approach describes how people acquire their knowledge of the language and makes statements about conditions which will promote successful language learning. Method : a method is the practical realization of an approach. Methods include various procedures and techniques as part of their standard fare. Procedure : a procedure is an ordered sequ Â· define different approaches of teaching. Â· explain merits and demerits of different approaches. Â· use different approaches contextually _3.3. Structural Approach _. It is also known as Aural-oral Approach. Each language has its own pattern of structure. The structural approach is an outcome of the experiments carried out in language teaching in the army campus during World War II. Meaningful words are used in particular order. Every structure embodies an important grammatical point.