Mentoring talent in IT security – A case study

Levente Buttyán
CrySyS Lab, BME
Budapest, Hungary
buttyan@crysys.hu

Márk Félegyházi
CrySyS Lab, BME
Budapest, Hungary
mfelegyhazi@crysys.hu

Gábor Pék
CrySyS Lab, BME
Budapest, Hungary
pek@crysys.hu

Abstract

Talent management is usually not well-supported by traditional curricula, because university courses are typically designed for a large number of average students and not for the few outstanding ones. In this paper, we share our experiences on running a talent mentoring program in IT security at our university. We describe the whole process from increasing awareness of IT security among students, via maintaining a community of practice where they can improve their skills, to finally connect them to well-established IT companies. We also introduce avatao, a platform to support hands-on IT security practice. Our methods could serve as a blueprint to establish a successful talent management program in IT security in a typical academic environment.

1 Introduction

Most universities have courses related to IT security in their official computer science curriculum. These courses are typically designed to teach a large number of students and they do not suit the requirements of talent management in IT security. Talent management requires the identification of those few students that have an increased interest in IT security and an increased potential to achieve outstanding results. We also need to provide special support for them, including a careful assessment of their current level of knowledge and skills, the understanding their individual needs for development, and a personalized training that unfolds their potential. Traditional IT security courses provide a few opportunities to meet these requirements.

We are facing these problems at the Budapest University of Technology and Economics (BME), where we have a solid IT security program consisting of (1) an introductory level course on IT Security given to all CS students in the BSc program, (2) a minor on IT Security at the MSc level, which itself includes specialized courses on Cryptographic Protocols, Computer Security, and Network Security, as well as an IT Security Lab and individual semester projects, and (3) a number of elective courses on specific topics (such as reverse engineering programs, secure software development, secure operation of computer networks, and the mathematical foundations of cryptography).

The first issue is that our introductory level course is taught in the 6th semester, and this is the first time students are exposed to the domain of IT security. Unfortunately, by that time, most of the good students are already involved in other fields of computer science that they encountered earlier in their study. Another problem is that our courses are designed to satisfy the needs of the average students, and not the outstanding ones. Furthermore, our introductory level course is given to around 500 students; hence, it is difficult to identify the interested ones and it is impossible to provide personalized training to them. The specialized courses and the laboratory exercises in our IT Security minor allow for better identification of talented students, but even in those cases, instructions cannot be personalized and custom-tailored. Teachers could give extra amount of homework or more difficult exercises to talented students, but this approach can be criticized as being unfair, requiring more work from the talented students for the same amount of credits. It may also be uncomfortable for those students that are not in the talented group as they would be treated differently from the eminent ones. Essentially, the only possibility for personalized instruction is the semester project, which is indeed valuable in talent management, but only in later stages when the students can already work alone and require only occasional instructions.

The development of IT security skills require a lot of hands-on exercises and practice. Unfortunately, the practice options are rather limited in our formal program: due to the large number of students in our introductory level course, even classroom exercises are infeasible, while the focused courses of the IT Security minor do have classroom exercises, but the volume is just a mere one

hour per week. Real hands-on practice for students is only possible in the IT Security Lab and the individual semester projects. However, the Lab covers only a few pre-defined topics, with just a 3 hour session for each topic, which is clearly not enough to become an expert in the subject. The individual semester projects are more flexible in terms of topics and amount of time for practicing, but they force the students to work on one specific problem for the entire semester. As far as we know, other universities have similar programs, yet they face similar challenges of talent mentoring in IT security.

While the traditional format of teaching may give a good basis for average students, we believe that those who are really interested in the field should be given the opportunity to grow their talent beyond what is possible by attending lectures and classroom exercises. In this paper, we describe our efforts and experiences with identifying and mentoring talented students in IT security. In particular, we introduce the two key elements of our talent mentoring program: (1) we created a community, called the CrySyS Student Core, for students with strong interest in IT security, which allows its members to learn and develop IT security skills in a non-standard way (i.e., by situated learning in a community of practice), and (2) we created a virtual practice lab, called avatao,[1] which supports talent management by allowing students to explore hands-on exercises in a realistic computing environment. avatao, as a scalable platform, also supports our traditional teaching program in various ways.

The objective of this paper is to provide a blueprint for talent mentoring in IT security that others may find useful and can adopt and modify for their own needs. Besides the methodology described here, we also offer avatao to the community as a common exercise platform with the benefit of sharing exercises, and thus, minimizing practice lab development efforts for teachers and maximizing diversity of exercises and comfort of usage for students.

2 The CrySyS Student Core

The CrySyS Student Core is an invite-only group of students from our university who feel enthusiasm for various domains of IT security and who have already proven their aptitude. One way to get invited is to score among the best students at our CrySyS Security Challenge, which is a hacking contest that we organize for our students every year (see more details in Section 2.2). Another way is to provide an impressive performance during a student semester project that we supervise. Thus, students who get invited have already achieved something, and they have a certain level of expertise in a specific IT security domain (e.g., reverse engineering programs, hacking web sites, or breaking cryptographic protocols).

The Core members meet once every week (including the holiday seasons), and they discuss various topics in IT security. Very often, members prepare talks on topics that they have been studying or working on recently, and present their experience to others. For instance, a student would explain his discovery of a software bug and a following exploit discovery. Another common activity in the Core is to prepare for international CTF games. This preparation usually means that the students give brief tutorials on various topics to each other, discuss write-ups for challenges from previous CTFs, or solve CTF challenges from previous years together. Occasionally, they invite an external expert to give a talk on a specific topic.

Students really enjoy to be member of the CrySyS Student Core, which is proven by the fact that they continue their weekly meetings even during the holiday period in the summer. One of the reasons is that they see the value of practical skills that they can acquire in the group. They can become domain experts in IT security which results in better job opportunities for them. Another reason is that they actually enjoy this kind of learning. Many of them told us that they prefer the Core meetings over traditional lectures where they just passively listen to the speaker, or even over lab exercises where they cannot choose what they are working on. In the Core, they are largely independent, meaning that they decide on what topic they discuss, what CTF they prepare for, or who they invite as an external speaker. So they have a certain level of responsibility and this actually stimulates them. And finally, the Core is a community where they feel good in a social sense.

We, as faculty members, try to minimize our control on the Student Core. Our contribution is focused on efforts for sustainability of the group, including attracting and preparing interested students, advising the selection of new Core members, and acquiring financial support for the operation of the group. Apart from this, the Core is operated by its members in a largely self-organizing manner.

In the rest of this section, we analyze the operating principles of the CrySyS Student Core from a pedagogical perspective, we describe how we addressed some of its sustainability issues, we present indicators of success, and finally, we discuss remaining challenges of operating the Core.

2.1 Principles

The CrySyS Student Core operates as a *community of practice*. The concept of community of practice as a form of learning was first proposed by Jean Lave and Etienne Wenger in 1991 [5]. Essentially, a community of practice is "a group of people who share a concern or

[1] http://www.avatao.com

a passion for something they do and learn how to do it better as they interact regularly."[2] There are three important characteristics of communities of practice:

- **Domain:** The identity of the community is defined by a shared domain of interest. Community members are committed to this domain, and they share a competence that distinguishes them from other people in the world.
- **Community:** Members of the community engage in joint activities and discussions, and they help each other by sharing information. This allows for building relationships that enable the members to learn from each other.
- **Practice:** Members of the community are real practitioners, and they develop a shared "repertoire of resources," including experiences, stories, tools, and ways of addressing recurring problems in their domain of interest.

In our case, all three characteristics are given: The domain of interest is IT security in general, and hacking computer systems in particular. The Core members engage in joint activities (e.g., they form the !SpamAndHex CTF team) and discussions, they help each other acquiring knowledge and hands-on experience, and share information on weekly meetings. Finally, they really develop a shared pool of tricks and tools that they use on hacking contests where they participate as a team.

A tremendous advantage of a community of practice is that it allows for *situated learning*, which is "learning that takes place in the same context in which it is applied."[3] It is a social process whereby knowledge is not transferred but co-constructed by members of a community. This form of learning has been used for a long time historically, and disappeared only in the modern era with the prevalence of formal education. It may not be the most optimal format for acquiring theoretical knowledge, but it is certainly a better way to learn practical, hands-on skills than lectures and classroom exercises that are used today in most schools and universities. IT security requires hands-on skills and situated learning is an effective way to acquire those skills to master the field. The CrySyS Student Core, as a community of practice, provides the appropriate environment where situated learning can naturally take place.

2.2 Sustainability

The CrySyS Student Core was officially founded in 2013 by one of the authors, Gábor Pék (still PhD student at that time) from an ad hoc student hacking group existing from 2011. At the beginning, the Core was driven by the enthusiasm and devotion of Gábor. However, later, it proved to be a very effective way of attracting talented students and growing their skills in IT security, and it quickly became a strategic asset of CrySyS Lab. Therefore, it was our best interest to identify the conditions for its sustainability, and make sure that those conditions are satisfied. We identified the following key factors for sustainability: visibility, bootstrapping, speeding up, admission, inclusion and giving back.

2.2.1 Visibility

It is very important to get in touch with students early in their curriculum, and expose them to the beauty and challenges of IT security. Of course, one should not aggressively push IT security as the only interesting field of computer science, but one could, given the opportunity, point out why it is interesting. This early exposure to IT security may ignite the interest of some students, and they may start certain activities consciously (e.g., reading security related news, paying more attention to security related bugs when developing programs, reversing some application, and taking some security related courses) that may ultimately create some bias towards IT security when choosing a specialization. As explained in [2], talent is not something which is purely coded in the genes, but it can be grown by deep practice, which requires some igniting, "life-changing" moment or event that gives the necessary force and endurance for diligent practice.

In our case, we take advantage of the fact that in their early years of study, our students are organized into groups that systematically visit the different departments and research labs with the aim of getting familiar with their ongoing activities. So we have the chance to present our talent mentoring program and the outstanding results of the CrySyS Student Core to 4-5 groups of 20-25 freshmen in each semester. Learning that some students who are just a few years older than they are and who started their studies exactly in the same conditions as they did are now top hackers and among the best teams of the world can truly have an igniting effect. Not surprisingly, we get a lot of questions on how one can join the Core, and we see some of the students again a few years later in our IT security minor in the MSc program.

2.2.2 Bootstrapping

As we said before, one needs to achieve outstanding results to be invited into the CrySyS Student Core. For many students, however, bootstrapping in IT security is difficult: they do not know where to start, what to read, and how to practice. There are plenty of IT security related articles, blog sites, and tutorials on-line, but they do not know what is worth reading. There are also plenty of security tools available on the web for free, but they do

[2] http://wenger-trayner.com/introduction-to-communities-of-practice/

[3] https://en.wikipedia.org/wiki/Situated_learning

not know which of them is worth to install and get familiar with. And finally, they do not know what they can experiment with without breaking the law or endangering their own computing platforms. It may be dangerous, for instance, to start experimenting with malware without setting up the appropriate sandbox environment, or it is forbidden to hack into web servers on the Internet.

We organize an IT security bootcamp each year to help students who are interested in joining the Student Core, but not yet experienced enough to do so. This bootcamp is not part of the official curriculum, and it needs extra work from the students (and from us). The bootcamp consists of 7 sessions, 2 hours long each. In each session, we introduce a specific topic (e.g., web security, reverse engineering, OS security, exploiting software, cryptographic protocols, ...) and we walk the students through a few practical exercises related to the topic. To make it as realistic as possible, we do not use paper-based exercises, but we use our avatao platform (see Section 3), where the students can launch, for each exercise, their own copy of a prepared computing environment. This requires the students to bring their laptops to the sessions. A few days before the sessions, we distribute reading materials to help preparation, and after the sessions, we recommend hands-on avatao exercises as homework to further improve their skills. To keep it effective, we limit the maximum number of participants in the bootcamp to 20 students. The students have to register and the 20 places are allocated in a first-come-first-served manner.

2.2.3 Speeding up

After the bootcamp, students can continue solving avatao exercises on their own. However, to speed up their progress, we offer them to join the !SpamAndHex CTF team of the Student Core. This does not mean membership in the Core yet, but it allows them to get closer to Core members and to further improve their skills. In addition, playing CTF games is fun and it has some addictive effects, so students who join actually get trapped in deep practice.

2.2.4 Admission

The Student Core needs a continuous supply of new members because Core members that complete their studies and get employed somewhere may not have time anymore to actively participate in the Core's life (although experience shows that many of them actually continues frequenting the weekly Core meeting). New members are admitted in the Student Core by invitation. This may seem to be a discriminating practice, but in effect, it is an important factor that makes the Student Core an appealing place where students want to get in and Core members are proud of belonging to. For newcomers, the strict admission procedure is a challenge, and they feel that they accomplished something (and they really did) when they are admitted. For Core members, membership represents status and the admission procedure ensures the preservation of values.

To make it a real challenge, we organize a local CTF every year, which we call the CrySyS Security Challenge. Any student of our university can participate in this CTF, but those who completed our bootcamp are strongly encouraged to do so. Our Security Challenge is a jeopardy type CTF that lasts for about 2 weeks. During this period of time, registered participants try to solve about 20-30 challenges in different domains of IT security, which are made available through our avatao platform. The top 3 students are offered valuable prizes offered by our industry sponsors. However, the real prize for the best performing students is that they get invited to the CrySyS Student Core. The number of invited students is not fixed: we invite outstanding performers, which typically means 3-4 students every year. This incoming number has so far been sufficient to sustain a stable group size (compensating for leaving members).

Besides the CrySyS Security Challenge, another way to get admitted to the Student Core is to provide an exceptional performance in a semester project (for example work that results in publications). This, however, happens quite rarely and we invite in this way only one student per year on average.

2.2.5 Inclusion

Once students become Core members, they should integrate in the Core's life and activities. This is usually an organic process that runs smoothly. Typically, new members are asked to give a presentation of some work that they did and which they are proud of. This helps senior members to learn the particular interests or domains of expertise of new members. It also helps to engage in discussions and establish relationships. New members also get involved in the !SpamAndHex CTF team, which accelerates their inclusion in the community. The goal of succeeding at highly-recognized international hacking competitions fundamentally shapes the community. Becoming part of the elite CTF team is a critical milestone to any junior Core member. Participating in the weekly Core meetings guides them towards this goal.

In a few rare cases, new members were not able to successfully integrate in the Core, and we do not know exactly why. Perhaps, the reason was that those new members were too much behind their senior fellows in terms of knowledge and skills, so they could not follow the presentations of the seniors and participate in their discussions. After some time, they got isolated, came less frequently to meetings, and finally slowly dropped out of the community. This was always sad, in particular, because so much effort has already been invested both on the student's and on our sides. We actually identify better

inclusion of new members as a challenge that we should solve in order to improve the sustainability of our talent mentoring program. We outline a possible approach in Subsection 2.4.

2.2.6 Giving back

We believe that the Student Core as a community should also participate in mentoring its own new generation, and hence, Core members should actively participate in training aspiring students, as well as in the admittance and inclusion of new members. Fortunately, many of the Core members share this belief. Today, most of the bootcamp sessions are led by Core members, and the challenges for the annual CrySyS Security Challenge are also created by them. This altruistic behavior greatly improves the sustainability of our talent mentoring program.

2.3 Measuring success

The effectiveness of our talent mentoring program is difficult to quantify, although quantitative measures would probably be useful in identifying problems and making strategic decisions to improve our program. A systematic evaluation would require careful design of measurements and collection of large amount of data, and it would take years to carry out. So far, we did not have the time and resources to perform such a systematic study.

Yet, there are some evidences showing that we are on a good track. One measurable indicator of success is the steady improvement of our group's results at international CTF's. Our team, called !SpamAndHex, which is largely built on the Student Core, was ranked 56th, 14th, and 5th in 2013, 2014, and 2015, respectively, on `ctftime.org`, the world-wide ranking of all CTF teams. The team achieved 23rd, 2nd, and 1st position on iCTF, an international CTF organized specifically for university teams, in 2012, 2013, and 2014, respectively[4]. They came in 24th on the DEFCON CTF Qualifier in 2014, while they were among the first ten teams and qualified for the DEFCON CTF Final in 2015 and 2016. Another good indicator of success is that many of the Core members got decent jobs at leading IT companies, including Google and Ericsson, as well as at successful Hungarian start-ups, including Prezi, Balabit, and Tresorit.

2.4 Better inclusion of new members

Smooth integration of new members into the Student Core is key for the sustainability of our program, and it is also one of the areas where we can improve our current practice. In this subsection, we outline a possible approach for integrating new members that we plan to follow in the future more systematically.

[4]We did not participate at iCTF 2015.

It is very important that new members understand that they are expected to be motivated and proactive in acquiring the knowledge needed to reach some status within the Core. However, it is also important to make it clear that they are not supposed to go home, study, and come back when they feel ready. Rather, they can and should take advantage of the existing know-how within the Core by frequent interactions with its senior members. In other words, new members should take responsibility in managing their learning process, but the actual learning itself can take place within the Core.

In order to catch up with the senior members, new members should follow a self-directed learning process. The challenge is that new members may be at different stages in practicing self-directed learning. In [4], Gerald Grow distinguishes 4 stages of self-directed learning: (1) Dependent, (2) Interested, (3) Involved, and (4) Self-directed. Most newcomers are somewhere between Dependent and Interested, perhaps a bit closer to Interested. In any case, they should all eventually become Self-directed in order to establish some status in the Core, and have a successful career later on when they leave the university. Faculty members and senior Core members should help them in this process by recognizing at what stage they are, and giving them challenges appropriate for their actual stage, which help them making a transition to the next stage.

The first problem is to identify at what stage a given newcomer is. This can usually be achieved by discussing with him, and asking him to talk about his previous projects. Dependent students very often have not had own projects yet, while Interested students typically have already done some mini project alone, and they are happy to talk about their work.

Giving challenges to the new members that are appropriate for the actual stage requires attention, discussions, and involvement of the new member himself. In our specific case of facilitating their integration into the Student Core, this approach can manifest itself at different self-directed learning stages as follows:

- **Dependent:** At this stage, new members still need some authority and coaching. Faculty members can discuss with the new members about their goals and fields of interests to identify what they are excited for, and then give them highly specific assignments in the identified sub-domain, such as understanding a published method and replicating it.
- **Interested:** At this stage, new members have strong interest in a specific subject, and faculty or senior Core members challenge them to let them identify a project idea related to this subject through discussions and brainstorming. For this, one can let them talk about the subject and lead the discussion to help them discover topics yet be uncovered. Therefore, achieving

some new results on those topics would be considered a real contribution even by senior Core members.

- **Involved:** At this stage, new members have already acquired a level of knowledge in a certain subject thanks to the projects of the previous stage. They may have actually became domain experts within the Student Core in a given subject, and therefore, they are now very valuable members of the community, respected by the other members. One can now start to increase the involvement of the new members in joint activities with senior members and larger challenges. One can expose them to situated learning experiences, for example by involving them in the CTF team. Another example is to ask them to give a tutorial to others, or run a bootcamp session for students.
- **Self-directed:** At this stage, the new member should be knowledgeable in multiple subjects and involved already in many activities of the Student Core. It's time now for letting the new members establish their own projects. They should be the driving force to come with the idea, initiate discussions, plan the projects, and run them. They can invite others in their project and foster collaboration. Senior Core members can start sharing tasks with them and so they can take more responsibility. For instance, they can start mentoring newcomers (this allows for sustaining the process described in these 4 steps) and designing challenges for CTF games.

In addition, it is important to continuously assess the progress of the new members and determine whether they have matured enough to step to the next stage. This can be done with the help of the community itself, i.e., with discussing about and evaluating the new members' activities with the senior members. The community should give constructive feedback to the new members, emphasizing their strong points, and encouraging continuation, but pointing also out weaknesses with possible ways to improve. Senior members can give personal examples, stories, how they overcame similar problems at the same stage. This sort of constructive peer feedback can be very valuable and appreciated by the new members, as it comes from authentic members of the community.

3 avatao: A scalable virtual practice lab

The CrySyS Student Core is becoming a *talent hotbed* [2] in the Hungarian IT security landscape. One of the key challenges in our operations, as we described above, is the sustainability of this community. So far, we discussed the pedagogical aspects of this challenge and now we describe the technical platform to offer a stable practice environment. Setting up a practice lab is a substantial effort and the senior Core members often lack the time and motivation to prepare the technical infrastructure and high-quality exercises for demonstrating interesting concepts to juniors.

We observed at various hacker groups and other technical communities of practice that the members come together for ad hoc knowledge sharing sessions with little preparation. Also, the content of the session is hard to reproduce as the presenters typically do not take the effort to properly maintain or archive the infrastructure and tools to support the session. This is the most noticeable when a senior members need to prepare and adjust exercises to the needs of junior students.

Taking one step back, we realized that the same issue applies to traditional education. Computer labs require a huge effort to build and maintain. Knowledge transfer between teachers and teaching assistants over the years was cumbersome even with the use of versioning software. Knowledge sharing between universities rarely exists. The issue became particularly urgent, when we were trusted to start an IT security class for approximately 500 undergraduate students. We needed a systematic approach to teach these students practical IT security while minimizing the effort for teachers spent on maintaining and administering practice labs.

For these reasons, we designed and built avatao, a scalable, hands-on IT security practice lab. avatao is built on content sharing by experts and universities. It allows us to provide high-quality, up-to-date practice labs for a wide range of IT security topics. In the following, we describe the avatao system and the crucial role it plays in the talent mentoring of CrySyS Lab.

3.1 Requirements

All over the world, teachers put a substantial effort to provide practice labs for students. We wanted to build a practice lab that is scalable yet inexpensive, able to serve our class of 500 and other classes over the years. Besides giving students a realistic computing environment, we wanted to use this tool to popularize IT security and increase the visibility of the CrySyS Student Core. We defined the following requirements to achieve this goal.

3.1.1 Students

From the students' perspective, the system should be motivating and allow them to use the maximum amount of skills with a minimum amount of friction.

- **Real-life, hands-on experience ((S1)):** We want to teach practical skills and not only the theoretical background.
- **Easy-to-use system (S2):** Typical labs require tedious configuration to start. We wanted a system that just works.
- **Personalization (S3):** Traditional practice labs are one-size-fits-all, leaving no space for customization by

skills and interests. Our goal was to have a system that is easy to adapt to the students' needs.

- **Rich content (S4):** To achieve true personalization by skills and interests, we need to have a rich exercise pool.
- **Quick feedback (S5):** True learning is a try-and-error process. In traditional education, the feedback loop for learning is often very long. The students have to wait until the teacher evaluates their work and gives them feedback. We wanted to automate feedback to speed up learning as much as possible.
- **Hints and recommendations (S6):** Mentoring students takes a lot of effort and it is impossible for large classes. To aid self-learning, we want to build hints and recommendations into the system to aid students on their learning path.

3.1.2 Teachers

For teachers, the avatao system should substantially reduce the workload to create and maintain practice labs.

- **Save time and effort (T1):** Administering practice labs takes the work of building and maintaining an infrastructure, and creating and updating the lab exercises. The system should substantially reduce this effort.
- **Easy challenge creation and sharing (T2):** The biggest effort for teachers is the work they put into creating the lab exercises. Creating lab exercises should be easy.
- **Continuous feedback (T3):** A basic need from teachers is to be able to monitor the progress of their students.
- **Mitigate cheating (T4):** Last, but not least, the system should be able to flag cheating and mitigate this behavior as much as possible.

3.2 Existing platforms

There are several platforms that help teachers in IT security education, for example Deterlab [1] or SEED [3] are available to the public. Deterlab spins up real machines using configuration scripts while SEED uses a few VM images to offer a pre-configured set of challenges. Both approaches limit the number of labs and the scale it can achieve (S4). These lab exercises cannot be personalized to students' needs (S3). Physical machine or VM instrumentation requires a substantial effort from teachers to stup and adapt challenges (T1) as well as SEED makes students setup a VM environment for experimentation (S2). Homeworks solutions need to be submitted via email with a description to the teacher. This lengthens the feedback loop because students need to wait for days to get comments on their solutions (T3, S5). Learning science has proven that continuous and immediate feedback is key to the effectiveness of learning, a feature that is lacking in most existing practice lab environments. For teachers, by far the biggest effort is to create and maintain their practice lab. To the best of our knowledge, existing solutions have limited options to create and share practice labs from the description down to the infrastructure provision (S4, T2).[5]

3.3 Platform implementation

3.3.1 Technical details

avatao was designed and built with the mindset of providing hands-on challenges for IT security practice (S1). We also focused on easing the access and use of online security challenges (S2). avatao comes with a complete cloud infrastructure to make challenges available 24/7. avatao offers a large number of challenges can be started within seconds (S2, S4). To achieve permanent online access, we decided to use lightweight containers (i.e., Docker) instead of full-virtualization technologies. As containerization puts only a minimal performance, I/O and memory overhead atop the application itself we can start new challenges in a couple of seconds instead of minutes to boot full-fledged OSs. At the same time, we spare the time for users to download huge virtual machine images (S2) and install corresponding hosted virtualization software (e.g., Oracle Virtualbox). Each challenge comes with a distinct Docker image which contains all the software dependencies that the challenge requires, thus we guarantee that a challenge will work correctly even in the long run when our host infrastructure changes. The online platform allows for immediate feedback that significantly speeds up the learning process (S5, T3). Based on the feedback, we plan to implement hints and recommendations (S6) to offer personalized learning (S3).

For teachers, we made challenge and learning path creation seamless also (T1, T2). We designed and exposed various challenge templates (e.g., exploitation, secure C programming) for community experts which they can adopt easily in accordance with their needs. That allows for creating and testing new challenges even faster and with minimal headache. As avatao contains a broad spectrum of different challenges (S4), custom learning paths can easily be created by teachers or field experts in minutes. Additionally, challenges are tagged by topic (e.g., SQL injection, Web Security) so as they can be found easily either by end users or teachers. Learning statistics allow teachers to monitor students' progress (T3). The platform does not yet include any methods to prevent or mitigate cheating, but we include it in our future work (T4).

[5] When we checked, Deterlab had a few publicly available exercises, but not flexible enough to allow for personalized mentoring and self-directed learning.

3.3.2 Content creation

avatao allows teachers to easily create and share challenges, relying on expert content creators (allowing T1).[6] We currently have top teachers from several universities who contributed challenges to the platform. In return, they can use all challenges created by other teachers. With about 200 challenges in the pool, this gives teachers the opportunity to rapidly generate hands-on IT security practice labs as opposed to weeks of hard work. avatao is currently in private beta, but we will soon open it to the public in return for contributions (effort or money).

We made avatao commercially available to businesses and other organizations, who contribute money instead of effort. The revenue is shared back to industry experts and individual users, who create high-quality challenges to the system without using it for their own training.

3.4 Use cases in talent mentoring

We rely on avatao to support our talent mentoring processes from increasing visibility to offering our Security Challenge CTF competition.

3.4.1 CrySyS Bootcamp

As mentioned before, we organize a 14-weeks bootcamp on IT security for interested students. avatao supports the practical exercises for the sessions of the bootcamp covering a wide range of topics. We use the platform to provide an easy-to-follow tutorial during the sessions, but also to provide optional exercises for practice at home. The experience shows that students' engagement increased significantly when shifting the bootcamp from presentations to practical exercises sessions.

3.4.2 CrySyS Security Challenge

The bootcamp is a preparation for the CrySyS Security Challenge, our annual hacking competition. The CrySyS Security Challenge is the key selection event for students to get into the Core. The competition runs completely on the avatao platform. Each year, the Core members develop a new set of security challenges for the competition centered around a different theme. For them, this serves as a teaching experience further sharpening their skills. For the aspiring students, this is an interesting learning opportunity. Many have reported the inspiration from the Challenge that directed them towards IT security and the world of CTF hacking competitions.

3.5 Enhancing regular education

We also use avatao in regular courses to significantly decrease the workload of designing and maintaining practice labs.

- **Homeworks:** In general, teachers use downloadable VMs for homeworks with detailed descriptions on how to configure these machines at home. Quite often, configuration takes a substantial time for students and a lot of effort to support from teachers. avatao spares this effort by offering an online practice lab.
- **Lab exercises:** Similar to the previous case, we used avatao to offer mentored lab exercises during classes. Here, the teacher explains the exercise and the students can solve it at the same time.
- **Self-directed learning:** We offer a large pool of avatao exercises for students to learn beyond their class. We observe that interested students actually start exploring various topics.
- **Practical exams:** As avatao is in an introductory phase, we refrained from making practical exams for grade, but other universities reported success with this use case.

4 Future work

Next, we want to implement the strategy for better inclusion of new members in the Student Core described in Section 2.4. We also want to improve our avatao platform, including the extension of challenges with hints, introducing community-based quality assurance of challenges, and better support for creating and integrating new challenges. We do hope that avatao will be adopted by many teachers and they will also contribute new challenges. Finally, we plan to study and measure quantitatively how avatao helps to acquire IT security skills.

Acknowledgement

Many thanks go to all current and former members of the CrySyS Student Core and the !SpamAndHex CTF team, as well as to all our students who provided feedback on our talent mentoring effort and avatao. We are also grateful to the anonymous reviewers and to our shepherd Jelena Mirkovic for their useful comments that helped to improve our paper.

References

[1] BENZEL, T., BRADEN, R., KIM, D., NEUMAN, C., JOSEPH, A., SKLOWER, K., OSTRENGA, R., AND SCHWAB, S. Experience with deter: a testbed for security research. In *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006.* (2006), IEEE, pp. 10–pp.

[2] COYLE, D. *The Talent Code: Greatness Isn't Born, It's Grown*. Random House, 2010.

[3] DU, W. Seed: hands-on lab exercises for computer security education. *IEEE Security & Privacy 9*, 5 (2011), 70–73.

[4] GROW, G. O. Teaching learners to be self-directed. *Adult Education Quarterly 41*, 3 (1991), 125–149.

[5] LAVE, J., AND WENGER, E. *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press, 1991.

[6] It is also one of the key challenges to maintain the involvement of the expert community and constantly motivate them to put in more content.