Leveraging Competitive Gamification for Sustainable Fun and Profit in Security Education

Adrian Dabrowski[†], Markus Kammerstetter[‡], Eduard Thamm[‡], Edgar Weippl[†], Wolfgang Kastner[‡]
[†]SBA Research, Vienna, Austria [‡]Vienna University of Technology

Abstract

With the ongoing IT security arms race advancing at a fast pace, there is a continuously high requirement for well-educated security professionals to protect today's IT infrastructure from malicious attacks. While the necessary IT security expertise can be gained through continuous learning and practical exercise, the approach quickly becomes tedious and tiring for students. At Vienna University of Technology, we offer a series of two consecutive security courses leveraging gameful design and competition to increase the motivation among students. The courses have been established for a decade with currently more than 400 participants each year and $1,219$ educated students since 2012. In this paper, we present our game-like course setup and evaluate the unique approach through student surveys. Our results indicate that the well-established gaming-like competitive approach is not only highly appreciated by our students, but also raises their interest and motivation to put more effort and extra work into their security education.

1 Introduction

With numerous attacks on websites and IT systems each day, IT security has become one of the main concerns for many business and government organizations. Consequently, there is a high demand for security education ranging from awareness training for employees to in-depth and highly technical security know-how for security professionals. As a result, security education has to address a number of unique challenges [2]. For instance, in comparison to engineering-related computer science topics such as database design, programming, algorithms or calculus, the field of IT security moves at a much faster pace. While a defense for an attack strategy might work just fine in one year, a year later it could already be surpassed due to adapted or even new attack techniques allowing the circumvention of previous defense mechanisms. With the ongoing security arms race, we believe that security education should not merely rely on technical aspects, but the primary focus should include the mindset and typical methods of attackers to keep up with their pace. A key element to teach this skill set to students are real-world exercises within a controlled environment. The more practical experience students can gain from learning and applying attacks as well as countermeasures, the higher their IT security skill set will become [2, 7]. While practical learning has one of the highest human memory retention rates [1], it can become tedious. Within a security course, it is thus challenging to keep students motivated and willing to spend the extra hours of hard work it requires until the security of a practical exercise breaks down and a personal triumph can be gained from the experience. In this paper, we present a competitive teaching approach based on gameful design (gamification) that keeps students in security education highly motivated. The approach has evolved over a decade of security teaching, with many individuals who have contributed their experience. It comprises an individual lecture style with a strong focus on practical but also fun security education, a challenge-based game-like practical part and a scoring system allowing real-time competition between students in solving security challenges. Moreover, together with our students we regularly take part in CTF competitions such as the iCTF [7] for a good team experience and an additional incentive to improve their knowledge in IT security. Since 2006, the introductory course of our Internet Security series is a compulsory course in Software Engineering bachelor computer science studies.

Summing up, the contributions presented in this paper are as follows:

- We present a security teaching approach that leverages game-like elements and competition amongst students to keep their motivation and effort put into security challenges and education high. We also show how our approach has evolved over a decade of security teaching. With currently about 400 participants each year, we have used this approach to educate more than $1,219$ students since 2012 and more than $2,200$ students since the introduction of the course in 2004.
- We evaluate our teaching approach with a security teaching survey conducted with 183 students who either currently attend one of our courses or have done so in the past. In addition, based on 130 survey interviews, we include collected student feedback from the general university course surveys on the courses from the past 5 years in our evaluation.

- We present the results of our surveys, showing that our students not only enjoy the game-like competitive teaching concept, but it also raises their interest in IT security and pushes them to put more effort into the course and its practical exercises.

2 Gameful Design of the Security Course

For the courses *Internet Security* (InetSec) and *Advanced Internet Security* (InetSec2) at Vienna University of Technology we leverage a highly automated environment with gaming-like lab exercises aiding us to handle more than 400 participants each year. Amongst students, the course has gained popularity due to its *hacking*-like experience in practical lab exercises. Starting in 2004, the gamification approach has been refined and extended several times. Basically, students have to solve a number of practical exercises (so called *challenges*) in addition to visiting ordinary lectures. The objective was to move away from traditional (and potentially boring) text book examples towards offering students a motivating environment that should increase their interest in computer security. Motivated through these courses, we hope that some of them return to us for their bachelor's, master's and PhD theses.

2.1 Storyline

Security researchers typically refuse to be associated with the Hollywood *hacking* movie style and its stereotypes. However, for our undergraduate course we make use of those often funny and unrealistic movie impressions to introduce students to real-world security attacks and defense mechanisms throughout the course and its lab challenges. Each challenge is embedded into a small (typically funny) story line including secret missions, big companies, helicopters, or the image of boring office workers turning into computer security superheroes at night.

To push students even further into their own hacker adventure, each of them is assigned a *leet hacker pseudonym*. Those pseudonyms are generated randomly through a database of name pre- and suffixes to create names such as *Warez Ninja*, *Leet Barcode*, *R00t Master*, *Blood Syntax*, or *Audio Outlaw*. We also keep a database of already assigned names to ensure that each name is uniquely assigned to a student and can thus be used throughout our courses.

For each challenge, students have to submit their solutions (often in form of source code) to an automated testing service denoted *grading bot*. The grading service automatically evaluates the solution and generates feedback reports. Approximately every two weeks our students receive new challenges to solve.

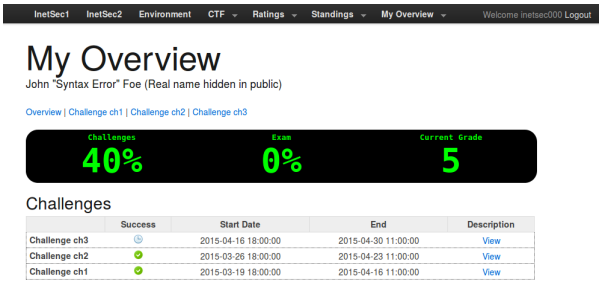


Figure 1: Student Dashboard showing open and solved challenges as well as the currently achieved grade

2.2 Competitive Elements

Throughout the course, we provide short and long term incentives for our students. First, there is a score board for each challenge showing who submitted a correct solution in what time, listing the students with the highest number of submissions and those with the latest submissions. Additionally, a similar score board (*ranking*) exists for all courses so far. Each student is awarded extra points if she or he is among one of the five fastest to solve a challenge. This is visible in a separate ranking list as well. Although the extra points do not count for the course exam, for many students a place in the high scores is a matter of honor. Competing against each other to be among the first five, we even received complaints from students demanding the restart of challenges when interruptions occurred due to university network downtimes. In our course, the score boards serve two purposes:

First, they drive competition among students and serve the more casual participants as a means to compare their progress with each other, including the progress of their friends.

Second, we offer long term incentives in the form of badges and privileges. For every challenge students solve (not all are mandatory), they move up in the hierarchy. The respective ranks are global (over all courses and persistent over the years) ranging from *Nobody* to *Master Guru*. This way, ranks are kept for the followin courses. The highest rank can only be achieved if students joined the CTF team at least once for a competition. The International Capture the Flag (iCTF) contest organized by UCSB [7] typically takes place in the last weeks of the *Advanced Internet Security* class. Additionally, students with the two highest ranks (i.e. *Guru* and *Master Guru*) receive the right to choose their own *leet hacker pseudonym*.

2.3 Sociotechnical Aspects

At the beginning of the weekly lectures, we include a "News from the Lab" slide with the current scoring in addition to a "News from the Field" section, where we briefly discuss new security developments reported in

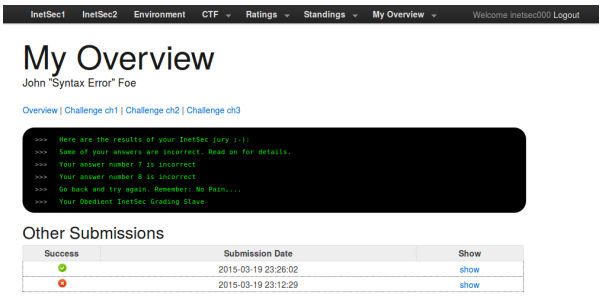


Figure 2: Feedback from a Challenge

the media or at academic conferences. The first slide shows the achievements of the students and allows others to not only compare their performance, but reminds them that they could be on that slide as well. The latter slide embeds the lecture topic into real world security developments.

Students can opt out of showing their real name on the public website next to their hacker pseudonym, but logged-in participants can always see the real names which, we believe, amplifies personal involvement. We thus focus on honoring positive achievements, but refrain from showing negative achievements, overall course marks or results of written exams to other students, since we do not want to cause a negative impact.

We also offer a cooperative element in the form of an Internet forum where students can not only get support from the tutor(s) but have the opportunity to exchange ideas and help each other. However, postings containing entire solutions are not tolerated and will be deleted. In the end, we believe that helping others is yet another way for students to show off their competence and achievements.

2.4 Didactic Aspects

The immediate feedback through the grading bot is an important element of the intrinsic reinforcement (i.e. reward-driven) loop. Only through instant gratification upon successful finishing, students will reinforce the positive feelings of mastering a challenge. This is important as breaking a security system can be a very creative riddle-solving process, often requiring many hours of systematically scrutinizing the system until vulnerabilities can be identified. Considering that later challenges will become harder, increasingly complex and more tedious to solve, the immediate feedback is necessary to increase long-term engagement. To give students room for their creativity, the grading bot typically tests the outcome but does not assess the selected approach for the solution.

Rank	# Challenges
Master Guru	CTF and $\geq$12
Guru	$\geq$12
expl0it Warlock	11
Stackmaster	10
Apprentice Professional	9
Apprentice Senior	8
Apprentice Junior	7
Apprentice+	6
Apprentice Stackmaster	5
Nobody Professional	4
Nobody Senior	3
Nobody Junior	2
Nobody	1

Table 1: Rank Names and their required Number of Solved Challenges

Besides positive reinforcement, there are elements of peer pressure and deadline-driven negative feedback through the score boards. In order to enhance the experience and to provide additional motivation, we decided to include students with the highest number of submissions and those whose submissions were closest to the deadline as well. This adds another dimension of game design elements, identified by Deterding et al. in [4], to our approach.

At the same time, we are aware that the gamification has its limits, both in gaining motivation as well as in how well the learning experience can be transformed into a game. After all, the lectures and lab exercises are offered as a university course for students who need to be graded for the final certificate. Moreover, the first course of our series has become mandatory for some undergraduate computer science curricula.

2.5 Historic Development

Prior to 2012, the competitive teaching approach only included three major elements of gamification as discussed in Detering et al. [4]. First, it provided students with a scoreboard displaying the order of successful completions of a task on a per-challenge basis. Second, a ranking system was used to award titles to students based on the overall amount of challenges they solved. These titles ranged from *Skript Kiddy* to *Master Guru*. Third, the challenges followed a storyline in which the student morphed from a white-collar worker to a master security specialist coveted by top intelligence agencies. In contrast, our current gamification approach now covers six of the ten motivational requirements as identified by Hamari et al. [5]:

Achievements and badges in form of ranks and privileges, scoreboards, points for speed, a theme covered by single stories for each exercise, challenges that need to be solved, and feedback by an automated system as well as help from our staff and fellow students.

2.6 Technical Description

To enable a gamified approach engaging students in IT security, a holistic competition environment allowing for exploitation of systems without crossing legal

boundaries is essential [6]. The environment we use has evolved from an experimental and hard-to-manage environment into a well rounded system for challenge based-trainings over the course of the last 10 years. Initially starting out with two physical servers that ran everything from website and grading down to student accounts, the system has evolved into a fully virtualized network of servers with well-separated tasks (Fig. 3).

Technically, we transitioned from a hard-to-manage Perl-script-based approach with multiple configuration files, version dependencies and different deployment scenarios for each challenge to a unified Python and database-driven approach enabling fast and easy setups with a separate virtual machine for each challenge. This reduces the work time for the environment, allowing us to minimize the time requirements for new content or challenges.

Students can work from computer rooms at the university, from their own PCs at home or even on the road, as long as they have Internet connectivity. For shell-based challenges, they need to log into a virtual network via SSH, whereas for web-based challenges they visit a password protected site that is handled by the appropriate challenge VM. Since 2012, we especially focused our environment towards the following factors:

Isolation The system can provide the experience of an internal corporate network, but is safely coupled off the Internet and other university networks. This serves the purpose of encouraging students to try different and possibly destructive approaches without the risk of severe repercussions like lawsuits or similar issues as discussed in [6].

Performance Our experience and log data taken from previous development iterations showed that student activity peaks twice during the time a challenge is open for submission of solutions. Once at the end, typically within 6 hours before the submission deadline, and once shortly after the challenge is released. The time interval of the latter varies between challenges. Virtualization and monitoring enable us to gain high availability, keeping the experience consistent for all participants.

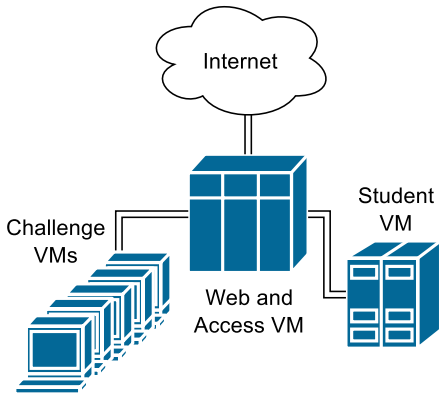


Figure 3: Overview of the Automated Internet Security Teaching Environment

Automation In order to provide fast feedback and instant gratification upon successful completion of a task, grading of submissions must be automated. In addition to automation, the grading system has the ability to process submissions in parallel. Otherwise the continuity of the student experience would be broken. Immediate gratification helps us to increase the engagement of participants by activating their reward systems and linking the reward directly to the work they have just completed [3].

3 Evaluation and Discussion

To evaluate whether the gameful competitive security teaching approach fulfills its goals (i.e. increased student incentive to put extra effort in the course, raised interests in security, etc.) we leveraged two types of surveys to get student feedback. The first type of survey was a short term online survey with specific questions to our security teaching approach. In contrast, the second type of survey is carried out each term by the university covers more general teaching and course related questions. In the past, we did not only use it to improve our course, but it is also an especially valuable data source as it covers the last four years of our security courses. In the following, we describe those two surveys and how we used them to evaluate our security teaching approach.

3.1 Short Term IT Security Course Survey

The short term survey was an online survey that ran for 13 days from 2015-04-17 to 2015-04-30. The survey questionnaire can be found in the Appendix Section of this paper (Table 4). Overall, we sent out survey invitation e-mails to $1,079$ students who are either currently taking part in one of our Internet Security courses or did so in the past three years. Since many students have graduated during that time, we feared that we could no longer contact them as their university e-mail addresses were no longer functioning. However, due to special e-mail addresses for alumni, this was only the case for 33 (3.06%) of them. Overall, 261 students (24.19%) opened the online survey questionnaire and 183 of them (16.77% of our students in the the last three years) completed the full survey. Due to missing data we were unable to include students who attended one of the courses from 2004 to 2011.

3.2 Long Term University TISS Survey

To allow students as well as lecturers to get feedback on their courses, in 2011 the university started to conduct generic online student surveys at the end of each term. Since the Internet Security courses were already well established at that time, we used the opportunity to

Year	Term	Overall Students	Completed questionnaires
2004		–	–
...		...	...
2010	S	–	–
2011	W	–	20
2012	S	212	4
2012	W	99	21
2013	S	282	33
2013	W	122	11
2014	S	270	41
2014	W	canceled	canceled
2015	S	234	–

Table 2: Returned University TISS Questionnaires per Term

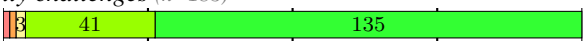
obtain long-term evaluation results from 2011 to 2014. However, some of the data has gaps since the university no longer has access to it. There is no data available yet for 2015, since our course is still running. In the winter term of 2014 we were unable to hold the course due to a lack of university funding. An overview is available in Table 2. The table includes the year, the term (i.e. either winter or summer term), the number of registered students per term as well as the number of survey interviews we received. The full university TISS survey questionnaire can be found in the Appendix Section (Table 5).

4 Results

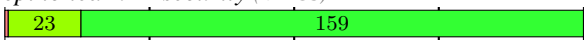
4.1 Short Term Course Survey Results

Students were able to choose from a Likert scale between *strongly disagree*, *disagree*, *neither agree nor disagree*, *agree*, and *strongly agree*. We removed unanswered and *don't know* answers from the bar charts below. The first questions where designed to set the students back into the time when they visited the course. Overall, most students appreciated the course and the way it was conducted.

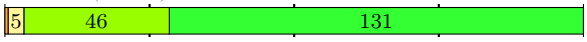
I enjoyed the gaming-like concept of the practical security challenges (*n*=183)



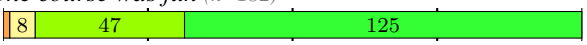
I believe practical security challenges are a good concept to learn IT security (*n*=183)



I prefer practical security challenges over conventional exercises (*n*=183)

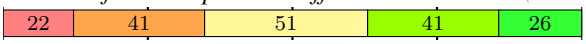


The course was fun (*n*=182)

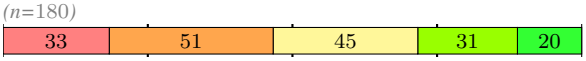


As expected, the ongoing competition and the scoreboards motivated our students to move up ranks, and they also enjoyed it.

The competition during the challenges (i.e. be the fastest, be the one with most points earned, ...) was an incentive for me to put more effort into the course (*n*=181)

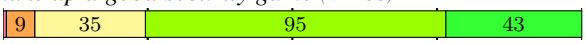


I tried to be better (i.e. faster in solving) than other students to earn extra points in the challenge competition (*n*=180)

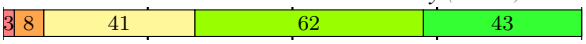


I spent extra effort to show up in the competition hi-scores (standings) (*n*=180)

I think that security challenges combined with competitive gaming strategies (i.e. hi-scores, extra points, etc.) make up a good security game (*n*=183)

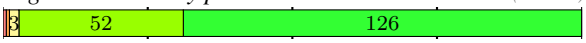


From my experience and/or from feedback I received from fellow students, I think that the gamification approach draws more students to IT security (*n*=157)

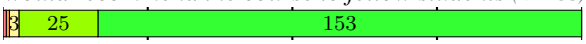


The vast majority of students acknowledged the usefulness of the practical lab exercises and would recommend the course to others.

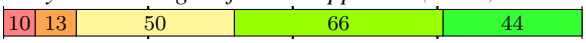
The security challenges allowed me to gain practical insight into security problems and their solutions (*n*=183)



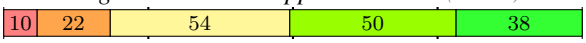
I would recommend the course to fellow students (*n*=183)



I would recommend the course to fellow students especially due to the gamification approach (*n*=183)

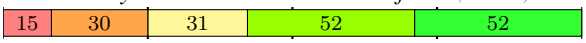


After hard security challenges I enjoyed writing up and submitting the individual approach I took (*n*=174)



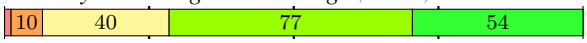
However, in some cases students were unable to invest more time into the lab challenges, even though they would have enjoyed to do so.

I would like to have invested more time in the lab exercises but my schedule didn't allowed for it (*n*=180)

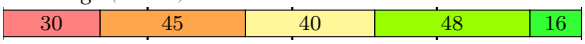


Due to the fact that our approach allows students to use their full creativity by not enforcing a specific solution approach, our grading bot is unable to asses partially finished exercises. Especially for students submitting their solutions late, this can be problematic if due to minor issues their solution is not accepted even though the approach they took would work.

The security challenges allowed me to bring in my own creativity in solving the challenge (*n*=183)

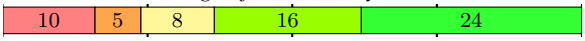


I find it unfair that I only get points if I fully solved the challenge (*n*=179)

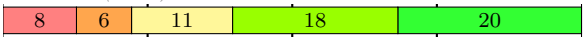


Students also attending the CTF competition mostly agreed that the challenge-based exercises prepared them well.

The Capture-the-Flag (CtF) competition required the combined knowledge of the security courses I took (*n*=63)



The Capture-the-Flag (CtF) competition allowed me to gain practical insight into security problems and their solutions (*n*=63)



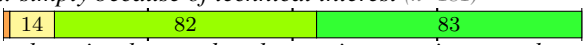
We also wanted to know if gamification might marginalize the implications of *hacking*.

Gamification might cause students to lose touch with the ethical questions regarding hacking (*n*=176)

4.1.1 Motivational aspects

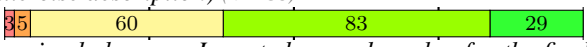
Additionally we wanted to know which features of the setup motivated the most and how much time the students spent because of it: *much less time*, *less time*, *about the same time*, *more time*, and *much more time*.

... simply because of technical interest (*n*=181)

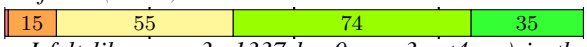


... knowing how to break security can give me advantages in future (*n*=178)

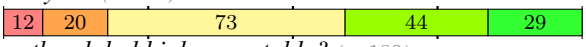
... the funny side stories (vs. just a plain technical exercise description) (*n*=180)



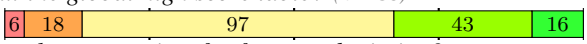
... simply because I wanted a good mark a for the final certificate (*n*=180)



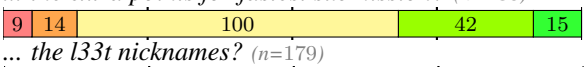
... I felt like a sup3r 1337 hax0r sup3r st4r :-) in the storyline (*n*=178)



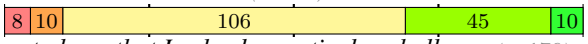
... the global high score table? (*n*=180)



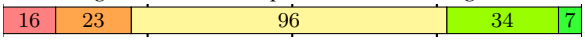
... the extra points for fastest submission? (*n*=180)



... the l33t nicknames? (*n*=179)



... to brag that I solved a particular challenge (*n*=176)



4.2 Long Term University Survey

The results for the TISS survey conducted by the university at the end of each term is based on 130 student survey results (Table 3). Due to their relevancy and space requirements, we only cover questions impacting our gamification approach. In the *Term* column, the course term is visible: in the summer term we hold the *Internet Security* course and in the winter term the sequel *Advanced Internet Security*. Before the winter term 2011 the university didn't conduct course surveys and hence no data is available. The *Participants* column shows the number of course participants per term. From those, the n (*Number*) column indicates the number of returned student surveys and the *Attendance* column provides an overview of how much students attended the lectures throughout the term. Beginning at the *Organization* column, we use the following scheme: To answer these survey questions, the students could choose from a scale ranging from 'strongly agree' (1) to 'do not agree at all' (5). Since most of the feedback was positive, we only show these responses in the table, *'s. agree'* in the column description means *strongly agree*. In that regard, the *Organization* columns indicate how much our students where satisfied with the course organization. In general, the results show that our gamification approach did not have a negative impact on the course organization. However, it appears that due to this approach our students also enjoyed visiting the lectures (*Visiting* columns) and we were able to raise their interest in IT security as well (*Raised Interest* columns). The majority of all students strongly agreed that the course content is useful for their future (*Usefulness* columns) and they experienced a strong knowledge gain (*Knowledge Gain* columns). On average, the *Overall Satisfaction* columns show that 73.85% of the 130 students giving survey feedback were very satisfied and 20.96% were satisfied with the course, indicating that only 5.19% of them were either not satisfied or did not answer the question.

5 Conclusion and Future Work

In this paper, we presented a competitive gaming-based security teaching approach that has been used at Vienna University of Technology for a decade. During that time we have learned many lessons causing the approach and the automated infrastructure behind it to evolve from a hard-to-manage solution to a scalable Python and database-driven solution relying on a virtualized network of systems.

Overall, the gamification concept has been used to teach more than 2,200 students so far with currently more than 400 participants in our Internet Security and Advanced Internet Security courses each year. We evaluated our approach with two surveys: One generic course survey conducted by the university with 130 students and a specific *Internet Security* course survey with 183 students. Our results indicate that the game-like course experience and the competition among students is an effective way to motivate students to put more effort and hard work into their security education.

Term	Partici-	n	Atten-	Organization		Visiting		Raised Interest		Usefulness		Knowledge Gain		Overall Satisfaction	
	pants		dance	s. agree	agree	s. agree	agree	s. agree	agree	s. agree	agree	s. agree	agree	s. agree	agree
2011W	n/a	20	68.95	70.00	30.00	80.00	15.00	70.00	25.00	80.00	15.00	80.00	20.00	65.00	35.00
2012S	212	4	71.67	100.00	0.00	75.00	25.00	100.00	0.00	50.00	25.00	75.00	25.00	75.00	25.00
2012W	99	21	71.00	100.00	0.00	85.71	4.76	85.71	14.29	80.95	19.05	100.00	0.00	85.71	14.29
2013S	282	33	62.97	72.73	15.15	66.67	15.15	72.73	24.24	87.88	9.09	82.82	18.18	75.76	18.18
2013W	122	11	86.88	81.82	9.09	81.82	9.09	90.91	9.09	81.82	18.18	100.00	0.00	72.73	27.27
2014S	270	41	77.18	70.73	26.83	80.49	14.63	70.73	19.51	75.61	19.51	80.49	19.51	70.73	17.07

Table 3: Combined University TISS Survey Results in Percent

Additionally, the approach also raises their interest in IT security and subsequently leads to a high knowledge gain. However, a significant factor to achieve these goals are not only the rewards offered through the gaming-like experience, but also the fun experience and the use of Hollywood hacking storylines. On the other hand, students were not driven by the speed components of the setup. Only 18% of the students fear that gamification of hacking may lead to unethical behavior.

Apart from continuously upgrading our lecture content and creating new security challenges to keep up-to-date, we plan to add additional security courses relying on the same gamification concept. Specifically, we plan to address currently evolving trends and challenges in security such as critical infrastructure and production system security or hardware and embedded security topics through additional courses.

Acknowledgements

We would like to especially thank **Christopher Kruegel** and **Engin Kirda** who came up with the initial idea and first implementation of the gaming-like competitive *InetSec* teaching environment for security education in 2004. Since then, the Inetsec environment has undergone a decade of continuous development and improvement with many who have been involved over the time, including (in no particular order): Christian Platzer, Matthias Neugschwandtner, Paolo Milani Comparetti, Clemens Kolbitsch, Manuel Egele, Martin Szydlowski, Gilbert Wondracek, Andreas Moser, Thorsten Holz, the authors and probably others as well. Without their work, the environment and the security education at Vienna University of Technology wouldn't be where it is today. In addition, we would like to thank the university's TISS team for helping us gather the TISS survey data for our security courses as well as *soscisurvey.de* for their excellent service.

The research was partly funded by the COMET K1 program by the Austrian Research Funding Agency (FFG), by the $(SG)^2$ project under national FFG grant number 836276 through the KIRAS security research program, and the AnyPLACE project under EU H2020 grant number 646580. *Internet Security* and *Advanced Internet Security* take part in the *10K Students to Improve Cyber Security* initiative of the Syssec Consortium.

References

[1] Creating Mindware for the 21st Century. Corporate University Xchange May/June 1996, Volume 2-3.

[2] A. Conklin. Cyber defense competitions and information security education: An active learning solution for a capstone course. In *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 9, pages 220b–220b, Jan 2006.

[3] S. Deterding. Gamification: designing for motivation. *interactions*, 19(4):14–17, 2012.

[4] S. Deterding, D. Dixon, R. Khaled, and L. Nacke. From game design elements to gamefulness: defining gamification. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, pages 9–15. ACM, 2011.

[5] J. Hamari, J. Koivisto, and H. Sarsa. Does gamification work?–a literature review of empirical studies on gamification. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, pages 3025–3034. IEEE, 2014.

[6] P. Y. Logan and A. Clarkson. Teaching students to hack: curriculum issues in information security. In *ACM SIGCSE Bulletin*, volume 37, pages 157–161. ACM, 2005.

[7] G. Vigna, K. Borgolte, J. Corbetta, A. Doupé, Y. Fratantonio, L. Invernizzi, D. Kirat, and Y. Shoshitaishvili. Ten years of ictf: The good, the bad, and the ugly. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, San Diego, CA, Aug. 2014. USENIX Association.

Appendix

Age	[ ]	( ) n/a				
Gender	170 male	10 female	( ) n/a			
Are you a current or former InetSec student ?	81 I visited (only) the Internet Security (InetSec1) lecture in the past years. 52 I visited the Internet Security (InetSec1) *and* the Advanced Internet Security (InetSec2) lectures in the past years. 50 I'm currently (SS2015) enrolled for Internet Security (InetSec1).					
I enjoyed the gaming-like concept of the practical security challenges	2	2	3	41	135	0
I believe practical security challenges are a good concept to learn IT security	1	0	0	23	159	0
I prefer practical security challenges over conventional exercises	0	1	5	46	131	0
The competition during the challenges (i.e. be the fastest, be the one with most points earned, ...) was an incentive for me to put more effort into the course	22	41	51	41	26	2
I tried to be better (i.e. faster in solving) than other students to earn extra points in the challenge competition	33	51	45	31	20	3
I spent extra effort to show up in the competition hi-scores (standings)	40	51	42	25	22	3
I think that security challenges combined with competitive gaming strategies (i.e. hi-scores, extra points, etc.) make up a good security game	1	9	35	95	43	0
From my experience and/or from feedback I received from fellow students, I think that the gamification approach draws more students to IT security	3	8	41	62	43	26
From my experience and/or from feedback I received from fellow students,I think a gamification approach in computer science courses can draw more students to computer science studies in general as well	4	15	36	75	38	15
The security challenges allowed me to gain practical insight into security problems and their solutions	1	1	3	52	126	0
I would recommend the course to fellow students	1	1	3	25	153	0
I would recommend the course to fellow students especially due to the gamification approach	10	13	50	66	44	0
The course was fun	0	2	8	47	125	1
I think the security challenges/games are a good way for people with different backgrounds, skill levels, and cultural experiences to utilize their strengths	5	20	59	57	31	11
After hard security challenges I enjoyed writing up and submitting the individual approach I took	10	22	54	50	38	9
The security challenges allowed me to bring in my own creativity in solving the challenge	2	10	40	77	54	0
I would like to have invested more time in the lab excercises but my schedule didn't allowed for it	15	30	31	52	52	3
I needed help to solve challenges	33	57	46	38	7	1
The InetSec team provided helpful information to solve the challenges	3	16	39	93	19	13
I received most of the help from fellow students	40	38	27	46	21	10
I find it unfair that I only get points if I fully solved the challenge	30	45	40	48	16	4
I also took part in the Capture-the-Flag (CtF) competition	87	10	2	7	37	40
The Capture-the-Flag (CtF) competition(s) were especially exciting for me	8	2	14	10	29	120
The Capture-the-Flag (CtF) competition required the combined knowledge of the security courses I took	10	5	8	16	24	120
The Capture-the-Flag (CtF) competition allowed me to gain practical insight into security problems and their solutions	8	6	11	18	20	120
Due to the course I would be interested in working in security research	5	21	44	74	36	3
Due to the course I would be interested in working in the security industry	6	14	47	73	39	4
I believe that presenting current up-to-date security research topics in the lecture makes the lecture more interesting	1	0	4	48	127	3
Before taking the course, I was already familiar with IT security topics	6	14	42	84	36	1
Gamification might cause students to lose touch with the ethical questions regarding hacking	53	50	41	28	4	7
These features/incentives motivated me to spent more ore less time	much less time	less time	about the same	more time	much more time	don't know
... the funny side stories (vs. just a plain technical exercise description)	3	5	60	83	29	3
... the global high score table?	6	18	97	43	16	3
... the l33t nicknames?	8	10	106	45	10	4
... the extra points for fastest submission?	9	14	100	42	15	3
... simply because I wanted a good mark a for the final certificate	1	15	55	74	35	3
... I felt like a sup3r 1337 hax0r sup3r st4r :-) in the storyline	12	20	73	44	29	5
... knowing how to break security can give me advantages in future	0	6	24	81	67	5
... (to be the first) to brag that I solved a particular challenge	16	23	96	34	7	7
... simply because of technical interest	0	2	14	82	83	2
Survey Understanding	strongly dis-agree	disagree	neither agree nor dis-agree	agree	strongly agree	don't know
The questions in this survey were clearly understandable for me	0	0	5	54	123	1

Figure 4: Internet Security Course Survey Questionnaire

I attended [x] % of the course sessions	[---] percentage			( ) no answer		
This course is assigned a total of 3.0 ECTS credits, which corresponds to around 5.0 hours per week during the semester. The actual amount of time I spent on the course was..	( ) much more than that		( ) about the same		( ) much less than that	( ) no answer
Course Preparation	strongly dis-agree	disagree	neither agree nor dis-agree	agree	strongly agree	no an-swer
Information about previous knowledge required for the course was provided in a timely manner	( )	( )	( )	( )	( )	( )
The course requirements were presented clearly	( )	( )	( )	( )	( )	( )
Course Implementation						
I was satisfied with the organization of the course	( )	( )	( )	( )	( )	( )
The course contents were communicated clearly	( )	( )	( )	( )	( )	( )
The materials provided were helpful	( )	( )	( )	( )	( )	( )
Enough examples were used	( )	( )	( )	( )	( )	( )
The instructors responded adequately to students' questions	( )	( )	( )	( )	( )	( )
Interactions between the instructors and students were respectful	( )	( )	( )	( )	( )	( )
I enjoyed attending the course	( )	( )	( )	( )	( )	( )
Questions were posed in a comprehensible manner	( )	( )	( )	( )	( )	( )
The advisors are available often enough	( )	( )	( )	( )	( )	( )
The contents of the lecture and tutorial are well coordinated	( )	( )	( )	( )	( )	( )
The lecture and tutorial take place at times that are well coordinated	( )	( )	( )	( )	( )	( )
Increased skills/Usefulness						
The course raised my interest in exploring the topic further	( )	( )	( )	( )	( )	( )
Information was provided during the course about how I will be able to use the contents in the future	( )	( )	( )	( )	( )	( )
The course increased my knowledge	( )	( )	( )	( )	( )	( )
I am capable of using the knowledge I gained from the course	( )	( )	( )	( )	( )	( )
Summary						
Overall I am satisfied with the course	( )	( )	( )	( )	( )	( )
I particularly enjoyed...	[----------]			( ) no answer		
The following should be improved...	[----------]			( ) no answer		

Figure 5: General University Course Survey Questionnaire. (Space restrictions prohibit the inclusion of yearly data in this table.)