SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World*

D3.2: First Summer School [†]

Abstract: The following deliverable summarizes the first summer school organized within the SysSec project. The topic was *System Security and malware reverse engineering with a special focus on critical infrastructure protection*, with a hands-on approach to teach reverse-engineering. Based on a questionnaire, the participants appreciated the school and a majority found that they had learned new skills and new concepts that might be useful for their future research.

Contractual Date of Delivery	August 2012
Actual Date of Delivery	January 2013
Deliverable Security Class	Public
Editor	Magnus Almgren
Contributors	All *SysSec* partners
Quality Assurance	Herbert Bos, Stefano Zanero

The *SysSec* consortium consists of:

FORTH-ICS	Coordinator	Greece
Politecnico Di Milano	Principal Contractor	Italy
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
Institut Eurécom	Principal Contractor	France
IICT-BAS	Principal Contractor	Bulgaria
Technical University of Vienna	Principal Contractor	Austria
Chalmers University	Principal Contractor	Sweden
TUBITAK-BILGEM	Principal Contractor	Turkey

[†] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement № 257007.

Table of Contents

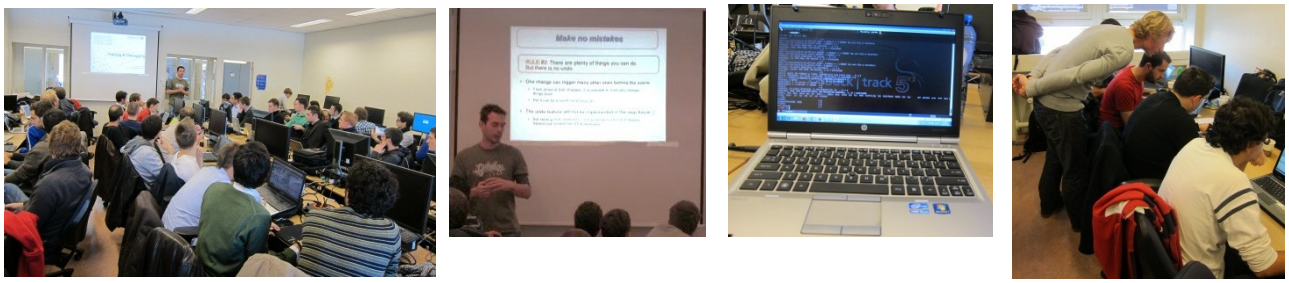


Figure 1: Pictures from the first day

1 Introduction

The EU/FP7 SysSec project aims to create a Network of Excellence in the field of Systems Security for Europe to play a leading role in shaping protection of cyber assets of the future. One of the core goals is promoting cyber security education, by creating a curriculum as well as organizing and collecting material that can be used by teachers across Europe to educate the next generation of researchers and industrial practitioners. During the course of the project, two summer schools will be organized. This document summarizes the first such summer school.

The first SysSec summer school took place October 11th-12th at VU University Amsterdam. The topic of the school was system security and malware reverse engineering with a special focus on critical infrastructure protection. Specifically, we decided to take a hands-on approach to teach reverse-engineering of malware, especially looking at the recent threats targeting critical infrastructure. We offered practical exercises to go through, and in many of the lectures code examples were shown at the blackboard with a step by step analysis, allowing the students to learn how recent malware had been reverse engineered.

The topic of the summer school reflected some of the recent threats described in one of the project deliverables, *First Report on Threats on the Future Internet and Research Roadmap* (D4.1)[1], and it is a cross section of the research performed within the project as a whole. Given how the security landscape changed with the discovery of stuxnet and flame, the topic highlights the need to protect critical infrastructures. To differentiate it from other summer schools, it was decided to focus on a hands-on approach so that the students would gain a skill for their future research or industrial undertaking. Among the speakers, we mixed industrial representatives with the best researchers in Europe in reverse engineering. For example, Heiko Patzlaff (Siemens CERT) was a key person analyzing stuxnet and having him give a lecture at the school to exemplify his analysis would demonstrate the intricacies and the time criticality of malware analysis.

The length of the school, two days, was chosen to allow both students from academia as well as industrial representatives to participate. A longer school would have made it more difficult for some of the industrial participants to come. A longer school would also have increased cost, making it difficult for some master students to attend. However, to offset the short physical meeting, we suggested the students to

[1] http://www.syssec-project.eu/media/page-media/3/syssec-d4.1-future-threats-roadmap.pdf

study some material before the school at their home university and then we offered exercises to be solved after the end of the physical meeting in Amsterdam.

Due to generous sponsoring by HexRays (IDA Pro disassembler licenses) and that many of the lecturers did not charge for their time or travel, we were able to give the summer school free of charge to the students, but they had to cover local costs themselves.

The interest in the summer school was well beyond our expectations and we had to close the registration due to lack of space. We had a limit where we could accept 50 students and we reached it within a week. Overall, the summer school was very popular. Based on a questionnaire, the summer school was seen as a success by the students. On the question, "What was your overall impression of the summer school?" the average grade given was 4.3 on a five-point scale. More than 35% of the students gave it the highest grade (5) and only two students gave it an average score (3) (no lower grade was given).

1.1 Organization Committee

The summer school organizing committee was the following.

- **Co-Chairs:** Magnus Almgren, Philippas Tsigas
- **Program Committee:** Herbert Bos, Davide Balzarotti, Evangelos Markatos
- **Publicity Chair:** Stefano Zanero

We also had help from the following people at VU University, with the design of the challenges, the setup of the labs, and supervision of the summer school participants.

- Istvan Haller
- Asia Slowinska (postdoc)
- Eric Bosman
- Remco Vermeulen
- Chen Xi
- Andrei Bacs

2 Program

The two days of the school were divided as follows. The first day focused mainly on tutorials to learn the basics of malware, reverse engineering, the tools to be used, as well as certain tricks that malware writers use to avoid their code being debugged. The first day also contained several student exercises. The second day focused on lectures, with a hands-on approach where the presenter showed code in a debugger and showed step-by-step how it should be analyzed. We had nine different speakers, covering different topics.

- Herbert Bos, VU University Amsterdam & SysSec
- Davide Balzarotti, Institut Eurecom & SysSec
- Heiko Patzlaff, Siemens CERT
- Damiano Bolzoni, University of Twente & CRISALIS
- Dina Hadziosmanovic, University of Twente
- Boldizsár Bencsáth, CrySyS Lab
- Gábor Pék, CrySyS Lab
- Erwin Kooi, Alliander, Netherlands
- Frans Campfens, Alliander

The detailed program of the two days was as follows.

Day 1: Introduction to reverse engineering

- Welcome and VM installation
  Magnus Almgren
- Session I: Binary Analysis
  Herbert Bos
- Session II: Tracing & Debugging, Ida Pro, Anti-Analysis Techniques
  Davide Balzarotti
- Practical Exercise (3h30min)
- Industry-perspective: Security in a changing DSO infrastructure
  Erwin Kooi, Alliander

Day 2: Advanced Malware and recent attacks against critical infrastructures

- Critical Systems and their special constraints
  Damiano Bolzoni, Dina Hadziosmanovic, UT and CRISALIS
- Description and detailed analysis of Stuxnet
  Heiko Patzlaff, Siemens CERT
- Analysis of Duqu/Flame
  Boldizsár Bencsáth, CrySyS Lab
- Hooks and code injection in Duqu and Flame
  Gábor Pék, CrySyS Lab
- Role of the DNO in SmartGrid Cyber Security
  Frans Campfens, Alliander

2.1 Highlights of the first day

The tutorials and lectures the first day covered the process of reverse engineering and the tools often used. For example, Davide Balzarotti explained the use of gdb and IDA Pro.

After the tutorials and lectures the first day, the students were given two challenges to reverse engineer. Among other tools, they used IDA Pro as Hex-Rays had generously sponsored the summer school with a set of licenses for the students. Tailoring the challenges to the knowledge of the students was quite difficult, because we suspected we would get both experts and novices applying to the summer school.

Before the start of the school, we sent out a questionnaire to tune the exercises to the participants. As expected, they differed in their knowledge so each challenge was offered in two different levels of difficulty. First, the students had a chance to look at the challenge. Then we released an associated hint sheet. Finally the complete solutions were released. As a final step for each challenge, we also had a walk through to explain how the solution should be implemented.

During the practical hands-on exercises, both Herbert Bos and Davide Balzarotti walked around and helped students. Several other experts from VU were also available if the students had questions. Even though we had many more students than envisioned, there was enough support available to help even the ones that did not know much before the start of the school.

2.2 Highlights of the second day

The second day focused on lectures highlighting the structure of new advanced malware and how it can be analyzed, thus a bit more theoretical but still with a hands-on approach where possible. For example, the lecturers pointed out the need to be careful with how the analysis is being done and even that one should sometimes avoid Google searches to keep the analysis unknown to the malware writers. Several of the lectures also adopted a hands-on approach where the lecturer loaded the malware in IDA Pro and then went through the analysis in this environment.

Figure 2: Pictures from the second day

3 Deviation of planned summer school date

Originally the First SysSec Summer School was scheduled for summer 2012. The partners considered several alternatives for its location, including San Servolo (Italy), Heraklion (Greece), etc. We wanted the summer school to reflect the focus of SysSec, considering hands-on research related to one of the key areas of the project. Key priorities were (i) to have a hands-on summer school where the student would learn a new skill, (ii) to mix academic teachers with representatives from industry, and (iii) to align the topics with one key area that have been identified as being important in the *First Report on Threats on the Future Internet and Research Roadmap*. It was decided that in order for a summer school (and especially a new one) to be successful, it should try to collocate and/or associate with another related event. During the summer 2012 we could not find such a high-profile event in Europe. The closest we could find was RAID 2012 in September in Amsterdam, a top-tier academic conference. For this purpose, we asked permission from our PO (at the time) to move the summer school to September and he gave his approval. Immediately after that, however, there was a connection with the ENCS[2] in the Netherlands. This is a cooperative association focusing on securing Europe's infrastructure. They suggested that we should have our summer school at the same time as they planned to have an event in Amsterdam. At the same time, there would also be three other major conferences in Amsterdam: Smart Homes[3], Transmission & Distribution Smart Grids[4], Metering Billing/CRM[5].

We saw several advantages with such an arrangement. It seemed likely that the participation of our summer school would increase if the participants could also attend other, related events at the same time. We also hoped it would draw a mix of participants to the school, with a majority of PhD students but also with some industrial participants to create future networking connections. We also wanted to provide the school with as low cost as possible to the students. With this arrangement we hoped to be able to attract interesting lecturers with (possibly) a shared travel cost. As a result, we were able to offer the school free of charge for students. Finally, several SysSec partners are also very interested in making this connection with the smart metering world which opens a wide range of possibilities to the threats and vulnerabilities for the Future Internet. We discussed it with our PO who understood the new potential offered to SysSec. Thus, the Summer School took place October 11-12 in Amsterdam just after the three other conferences in Amsterdam, with a program that mixes academic lectures, hands-on exercises and an industrial perspective on current threats (analysis of Stuxnet, for example from Siemens). Without the movement in time of the summer school we would not have been able to offer the same quality of program with no charge to students.

[2] The European Network for Cyber Security, https://www.encs.eu/

[3] http://www.smarthomes-europe.com

[4] http://www.td-europe.eu

[5] http://www.metering-europe.com/

4 Dissemination of Event

The project web site served as the main channel for dissemination. Through the web site, we could early on provide details about the dates and the content of the summer school. However, we were also able to use some of the other communication channels that have been established during the course of the project. Messages went out over twitter, Facebook, and the dissemination mailing list. We also announced the summer school at some related security mailing lists not particularly focused on system security. We also announced the summer school at major security venues taking place in Europe, such as DIMVA. We had planned to also announce the school at RAID but by that time, we had already closed admission as the school was full.

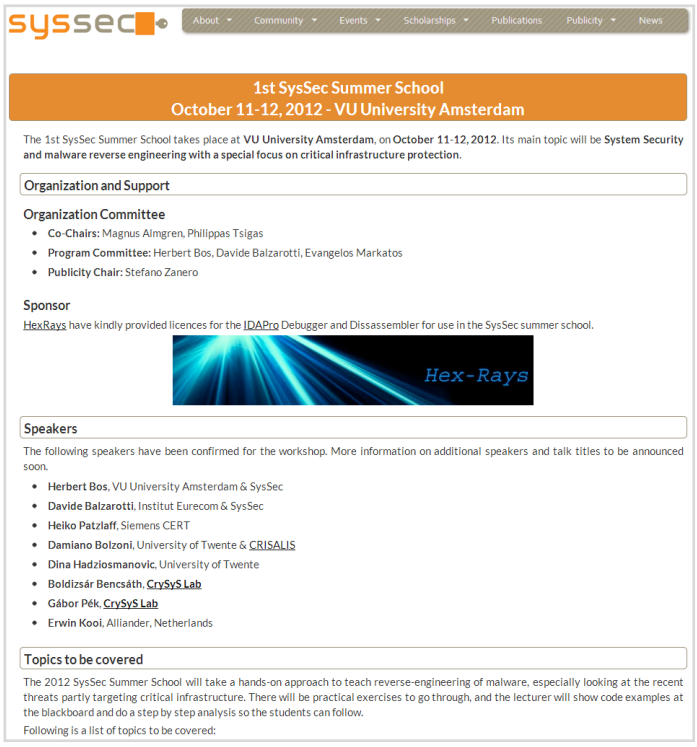


Figure 3: Web page for summer school

The registration for the summer school opened on September 4 with the second wave of announcements going out on September 4 (Tuesday) and September 5. Already by Monday the following week, we were overwhelmed with the number of applications so we had to close the registration and create a waiting list. In about a week, 65 participants had expressed their willingness to participate. Due to the hands on approach, we had originally foreseen a smaller summer school but by changing rooms we managed to admit 50 of these to the summer school (where 49 actually participated). The local host at VU University also managed to recruit more students to help during the exercise sessions than originally planned for.

Figure 4: Twitter announcement

The school was free for students affiliated with an academic institution while others paid a nominal fee of 200 euros, but participants had to cover their local cost themselves. Despite this, several students decided to attend even though they covered their expenses by themselves, because they found the speakers / topics so interesting and useful for their future. Mostly Europeans participated but we also had a student from Brazil, for example.

As we could not admit all people who were interested, other sites also contacted us asking for the material afterwards so that they could run a similar school on their own premises for their own students. We are currently exploring possibilities in how to share the material (see Section 6).

5 Sponsoring and collaboration with other projects

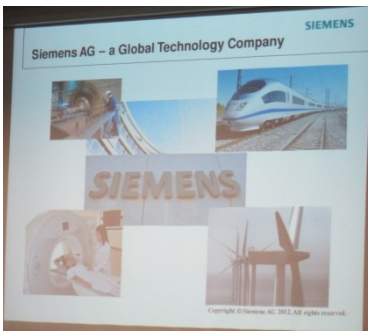
We would like to express our gratitude to Hex Rays for licenses to Ida Pro.

We would also like to thank the organizations of many of the speakers that covered their trip, such as Siemens and Alliander.

We would like to thank ENCS[6] that provided contact information to several speakers.

Finally, also the EU/FP7 project CRISALIS provided speakers to highlight the need for research into the protection of critical infrastructures.

[6] The European Network for Cyber Security, https://www.encs.eu/



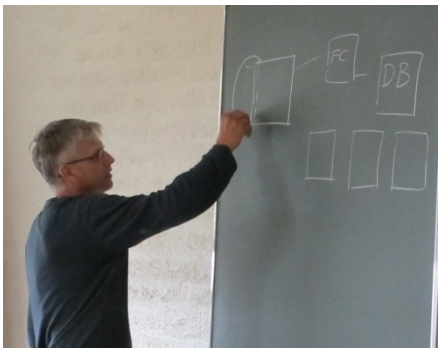



Figure 5: Pictures lecture by Siemens CERT Heiko Patzlaff

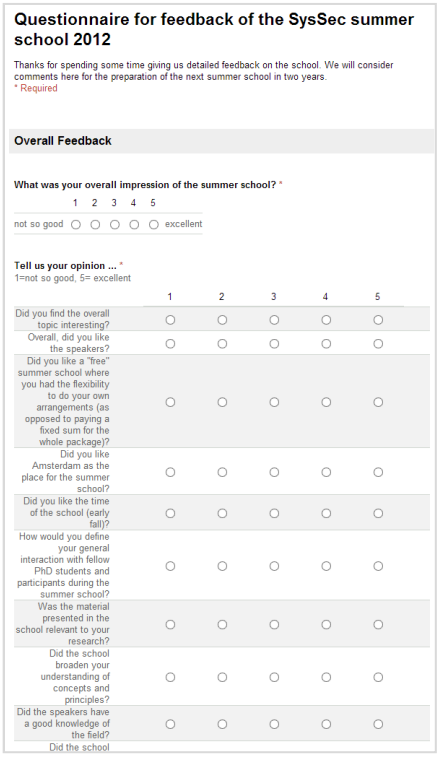
6 The SysSec Course Repository

As part of the efforts within SysSec, we are collecting and distributing high-quality lectures in system security to educators across Europe in the form of a course repository with slides and exercises[7].

Given the popularity of the school, several sites asked if we would be able to provide some of the material from the summer school to them so that they could run the course by themselves. For that reason, we are adding the material to the course repository.

[7] http://www.syssec-project.eu/community/

7 Description of Web Questionnaire


Questionnaire for feedback of the SysSec summer school 2012

Thanks for spending some time giving us detailed feedback on the school. We will consider comments here for the preparation of the next summer school in two years.
* Required

Overall Feedback

What was your overall impression of the summer school? *
1 2 3 4 5
not so good ○ ○ ○ ○ ○ excellent

Tell us your opinion ... *
1=not so good, 5= excellent

	1	2	3	4	5
Did you find the overall topic interesting?	○	○	○	○	○
Overall, did you like the speakers?	○	○	○	○	○
Did you like a "free" summer school where you had the flexibility to do your own arrangements (as opposed to paying a fixed sum for the whole package)?	○	○	○	○	○
Did you like Amsterdam as the place for the summer school?	○	○	○	○	○
Did you like the time of the school (early fall)?	○	○	○	○	○
How would you define your general interaction with fellow PhD students and participants during the summer school?	○	○	○	○	○
Was the material presented in the school relevant to your research?	○	○	○	○	○
Did the school broaden your understanding of concepts and principles?	○	○	○	○	○
Did the speakers have a good knowledge of the field?	○	○	○	○	○
Did the school					

Figure 6: Web-based questionnaire

A couple of weeks after the end of the summer school, we sent out a web-based questionnaire to collect feedback from the participants. We had a range of questions, for example to see how the current implementation of the school worked, but also questions related to the next summer school in the project. The questions were divided into four sections: overall feedback, feedback on the first day, feedback on the second day, and suggestions for the next summer school.

The following is the list of questions we asked. The number in parenthesis is the computed average from the received responses. Most questions were asked with a scale, 1=not so good, 5= excellent or 1=less of it, 5= more of it. The response to some questions was of the form of free text.

Overall Feedback

What was your overall impression of the summer school? (4.3)

Tell us your opinion …

- Did you find the overall topic interesting? (4.7)
- Overall, did you like the speakers? (4.3)
- Did you like a "free" summer school where you had the flexibility to do your own arrangements (as opposed to paying a fixed sum for the whole package)? (4.3)
- Did you like Amsterdam as the place for the summer school? (4.5)
- Did you like the time of the school (early fall)? (3.9)
- How would you define your general interaction with fellow PhD students and participants during the summer school? (3.8)
- Was the material presented in the school relevant to your research? (3.8)
- Did the school broaden your understanding of concepts and principles? (4.3)
- Did the speakers have a good knowledge of the field? (4.8)
- Did the school incorporate recent developments in the field? (4.4)

Would you have wanted less of certain activities, more of others?

- Did you like the hands-on approach? (4.7)
- How was the length (2 days)? (4.0)
- Did you want more industrial lectures? (2.8)

What was your main motivation for attending? Also say if there were issues that made you think NOT to attend (free text).

First Day

Overview of the first day

- I liked the first day (4.6)
- The hands-on approach was excellent (4.4)
- The challenges were of just the right difficulty (4.3)
- I feel like I learned something new (4.6)
- The mix between lecture / exercise was right (3.9)
- I thought one day of tutorial and general reverse-engineering techniques were enough (2.0)

Any comments to help us improve the first day (free text).

Second Day

Overview of the second day

- I liked the topics of the second day (4.0)
- I feel like I learned new things the second day (3.8)
- I would have liked longer lecture slots for each teacher (2.7)
- I would have liked more hands-on also the second day (4.5)

Any comments related to the second day (free text).

The Next Summer School

Please give us a few ideas for the next summer school.

About the next SysSec summer school

- Would you like to come again to the 2nd summer school? (4.5)
- Would you recommend it to your colleagues? (4.7)

Give us a system security topic that would make you intrigued to also attend the second SysSec summer school. (free text)

Give a grade to the following possible locations for the next summer school (may change!)

- Amsterdam, the Netherlands (3.8)
- Crete, Greece (3.5)
- Göteborg, Sweden (4.1)
- Bertinoro, Italy (3.6)
- San Servolo, Venice, Italy (4.1)

Any other place for a summer school? (free text)

8 Analysis of Web Questionnaire

We will use the questionnaire to plan for the next summer school. In this document we summarize only a few of the questions of relevance to the execution of this particular summer school. 50 people were admitted to the summer school, and 49 of these came. 42 people answered our questionnaire. Most questions were asked with a scale, 1=not so good, 5= excellent or 1=less of it, 5= more of it. The response to a few questions was of free text form.

8.1 General feedback

Overall, the students liked the summer school. In the survey after the school we asked the students of their overall impression and on a scale from 1 to 5, the average was 4.3. 36% of the participants gave the highest grade (5) and 60% gave the next highest grade (4). The lowest score, given by two students, was 3.

The participants liked the topic of the school (average 4.7) and it seemed the students especially appreciated the hands on approach (average 4.7). However, given that the school was voluntary for most participants and they chose to attend themselves, a high score here was expected. Indeed, the fast registration rate and the fact that there was a waiting list tells more about the suitability of the topic of the school.

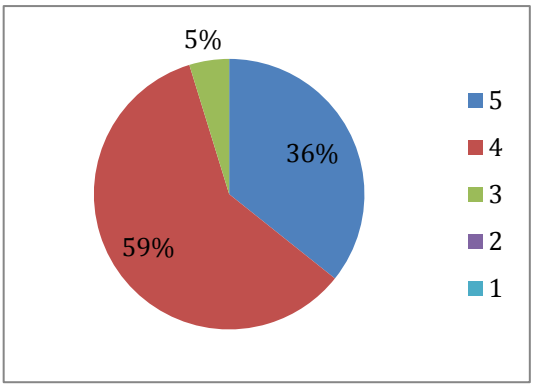


Figure 7: Overall impression

The speakers were very well appreciated. On the question "Tell us your opinion ... [Did the speakers have a good knowledge of the field?]" the average is 4.8. Moreover, the participants expressed that they learned new concepts[8] and that the school was relevant to their research[9].

Due to the popularity of the school, we filled the available rooms to their limit. Even though the rooms were crowded, the average score for the first day was 4.6 (with no 3s). For the second day, the same question gave 4.0 (with 10 3s).

8.2 One goal of the summer school: teach a concrete skill

One core goal of the summer school was to teach a skill. It seemed that a majority of students actually felt like they did pick up new skills after the first day.[10] Most students also thought the tutorial sessions were fruitful[11], something that in practice had required quite a lot of preparation before the school. The participants had very different backgrounds, where some were experts and others novices to malware and reverse engineering. Before the school, we sent out a couple of questions to judge the

[8] Tell us your opinion ... [Did the school broaden your understanding of concepts and principles?] 4.3

[9] Tell us your opinion ... [Was the material presented in the school relevant to your research?] 3.8 It should be pointed out that quite a few people attending the school did so as master's students, meaning that they had not yet started with research.

[10] Overview of the first day [I feel like I learned something new] 4.6

[11] Overview of the first day [The challenges were of just the right difficulty] 4.3

knowledge of the participants and based on this feedback we created two sets of challenges -- one of normal difficulty and one set of difficult challenges. We also collected the students in groups based on their knowledge and had a step-by-step explanation of the normal challenges, so that even if participants got stuck on one part they could easily move onward. The high score of the students on the suitability of the difficulty of the exercises shows how successful this approach in reality turned out to be.

8.3 Organization

We also asked a few questions on the organization, such as if the location was suitable and the length of the school. The attendees liked Amsterdam as the place for the summer school (average 4.5) and as one student expressed it. *"Something in the middle of western Europe, so many people can easily* attend."

The length of the summer school was a bit debated. A longer school would have been appreciated.[12] Many suggested three days as ideal. This would have given more time to the exercises but still keep the introduction lectures and the industrial perspective. The hands on approach was very much appreciated and also the issue that cost was kept to a minimum. Some suggested splitting the lectures between the two days to give more hands on for both days. Others did stress the need for only a single day of tutorials. For this particular instance, we asked the students to prepare material before coming to the school and then also gave exercises they could complete at their home university, but obviously the length of the summer school is something to be discussed also for the next instance. Several industrial participants stressed that they would not be able to attend a long summer school, so if a mix between industry and academia is a goal the summer school cannot be much longer. Several participants also paid their local costs themselves (flight and hotel), and for these participants the cost might have been a prohibiting factor if the school had been longer.

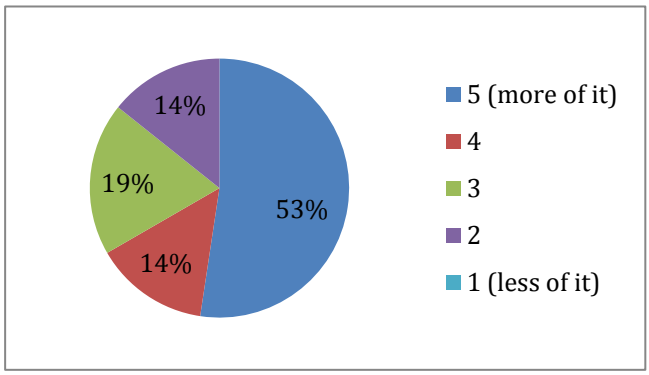


Figure 8: Whether to have longer / shorter school

As expected, as the summer school was quite short the student participation and networking was more challenging than usual.[13] We encouraged working in groups and we also organized a social dinner the first night. We also created a mailing list for

[12] Would you have wanted less of certain activities, more of others? [How was the length (2 days) ?] 4.0

[13] Tell us your opinion ... [How would you define your general interaction with fellow PhD students and participants during the summer school?] 3.8

Figure 9: The social dinner

interactions between the students after the school, to allow them to easily ask each other questions. One student suggested that we should have some sort of follow-up.

> *"A births of a feather or an additional workshop might be useful - participants can quickly present (e.g. 5 mins) their topics"*

It may be possible to target a subset of the students that participated in this instance also for the next summer school, thus creating a link between the schools. The SysSec scholarships are also an opportunity to work more closely with the researchers from the school, thus going further into the topics demonstrated.

8.4 Questions regarding the next summer school

Finally, we asked a few questions about the next summer school. The answers to a few of these questions can indirectly also tell us about the satisfaction of the participants of the current summer school. For example, a majority of the participants would like to return to the second SysSec summer school[14] and they would gladly recommend it to their colleagues[15].

[14] About the next SysSec summer school [Would you like to come again to the 2nd summer school?] 4.5

[15] About the next SysSec summer school [Would you recommend it to your colleagues?] 4.7

9 Summary

The first SysSec Summer School took place at Vrije Universiteit, Amsterdam, Thursday October 10 to Friday October 11, 2012. Its main topic was system security and malware reverse engineering with a special focus on critical infrastructure protection. One of the goals of the 2012 SysSec Summer School was to have a hands-on approach. We wanted the students to develop a skill but also learn from experts that have analyzed recent threats partly targeting critical infrastructures.

We had nine speakers in total, mixed with hands-on sessions where the students could explore techniques that they had just seen in a lecture. The first day focused on general reverse engineering with lectures and practical exercises, while the second day focused on lectures highlighting the structure of new advanced malware and how it had been analyzed. We mixed academic and industrial speakers to show research issues as well as the recent threats and the resulting analysis done by industry of recent malware.

The summer school filled up very quickly and a waiting list was actually created. For that reason we are exploring ways of sharing the material to sites where the students could not participate directly, something that may be possible to do through other efforts within the SysSec Network of excellence.

Based on a web-based questionnaire after the school, we can say that the participants appreciated the school and that a majority found that they both had learned a new skill but also had understood new concepts where the material might be useful for their future research.