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*

D3.4: Second Summer School[†]

Abstract: The following deliverable summarizes the second summer school organized within the SysSec project. The topic was ***mobile malware*** *with a special focus on* ***reverse engineering and analyzing Android malware***. Based on a questionnaire, the participants appreciated the school and a majority found that they learned new skills and new concepts that might be useful for their future research.

Contractual Date of Delivery	November 2014
Actual Date of Delivery	January 2015
Deliverable Security Class	Public
Editor	Antonis Krithinakis
Contributors	Thanasis Petsas
Quality Assurance	H. Bos, F. Maggi, Z. Minchev

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.

Document Revisions & Quality Assurance

Internal Reviewers

1. Herbert Bos
2. Federico Maggi
3. Zlatogor Minchev

Revisions

Version	Date	By	Overview
1.0	28/1/2014	Antonis Krithinakis	Addressed comments and edits. Deliverable ready for public release
0.5	28/1/2014	Zlatogor Minchev	Edits
0.4	28/1/2014	Federico Maggi	Edits
0.3	26/1/2014	Herbert Bos	Various edits + text on Bos' talk
0.2	25/11/2014	Thanasis Petsas	Second run + edits.
0.1	17/11/2014	Antonis Krithinakis	First draft.

Table of Contents

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, the SysSec consortium organized two summer schools. This document summarizes the second SysSec summer school.

The second SysSec summer school took place at Vrije Universiteit (VU) Amsterdam, Thursday September 25 to Friday September 26, 2014. Its main topic was mobile malware with a special focus on reverse engineering and analyzing Android malware. Specifically, similarly to the first SysSec summer school we decided to take a hands-on approach to teach reverse engineering of malware. 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 Android malware has been reverse engineered.

The school was free for students affiliated with an academic institution. A school longer than 2 days would have increased costs, making it difficult for some students to attend. 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 40 students and we reached it within two weeks. Finally, we managed to admit 42 participants.

Overall, 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 4.27 on a five-point scale. More than 30% of the students gave it the highest grade (5).

2 Dissemination of Event & Attendance

The project web site served as the main channel for dissemination. Through the web site, we provided details about the dates and the content of the summer school early.

Figure 1 SysSec Home page advertised the second summer school

Figure 2 SysSec summer school webpage

However, we also used other communication channels that have been established during the course of the project. Messages went out over Twitter, Facebook, and our dissemination mailing list. We also announced the summer school at some related security mailing lists not particularly focused on system security.

Figure 3 Facebook announcement

Figure 4 Twitter announcement

The registration for the Summer School opened on July 23 with announcements through our social media channels and to our mailing lists in the following couple of days. In that period a total of about 55 participants expressed their interest to participate.

All participants had to cover their travel and local costs themselves. Having to pay for one's own costs didn't seem to bar any students from attending, which is an indication that they found the speakers and the topic interesting and useful for their future.

3 Organization Committee

The summer school organizing committee was the following.

- Program Chair: Sotiris Ioannidis, FORTH
- Local Arrangement Chair: Victor van der Veen, VU University Amsterdam
- Program Committee:
    - Magnus Almgren, Chalmers University of Technology
    - Davide Balzarotti, Institut Eurecom
    - Herbert Bos, VU University Amsterdam
    - Christian Platzer, Vienna University of Technology

4 Speakers & Programme

The two days of the school were divided as follows. The first day focused on general static and dynamic analysis of Android applications with lectures and hands-on exercises, whereas the second day focused on lectures highlighting more advanced techniques in dynamic analysis. Also, towards the end of the summer school, a malware competition was held for the participants.

We had six different speakers, covering different topics. The list of speakers and their affiliations were as follows:

- Elias Athanasopoulos, FORTH
- Federico Maggi, PoliMi
- Matthias Neugschwandtner, TUV
- Herbert Bos, VU University Amsterdam
- Victor van der Veen, VU University Amsterdam
- Thanasis Petsas, FORTH

The hig-level program of the two days was as follows:

Day 1: Introductory tutorial, tools, and static analysis	
Welcome and VM installation	45 minutes
Session I - Introduction and meta-data analysis Elias Athanasopoulos	1 hour, 45 minutes
Session II - Static analysis Federico Maggi	1 hour, 45 minutes
Session III - Dynamic analysis Matthias Neugschwandtner	1 hour, 15 minutes
Session IV - Current and future research Herbert Bos	1 hour

Day 2: Dynamic analysis, revision, and future directions	
Session V - Advanced dynamic analysis Victor van der Veen	3 hours
Session VI - Evading dynamic analysis environments Thanasis Petsas	1 hour, 40 minutes
Session VII - CTF competition Federico Maggi	1 hour, 45 minutes

4.1 Highlights of the first day

The tutorials and lectures held during the first day of the summer school, covered an introduction to the Android system and ways to analyze Android applications. Elias Athanasopoulos explained the Android ecosystem and presented the Android emulator, as well as the required tools which were used throughout the summer school.

Figure 5 Elias Athanasopoulos giving an introduction to the Android ecosystem.

During the second session of the first day, Federico Maggi presented the Dalvik virtual machine, a fundamental part of Android that executes the Android applications. Federico taught students how to disassemble, decompile, unpack and modify functionality of Dalvik bytecode of Android applications.

Figure 6 Federico Maggi is about to teach Android malware static analysis.

Finally, Matthias Neugschwandtner discussed about the importance of dynamic analysis for the detection of malicious applications. Matthias also presented Andrubis, an extension for Anubis designed to analyze unknown Android applications (APKs), and AndroTotal, a free service that allows researchers to automatically scan Android apps against various Android antivirus products.

After each tutorial, the students were given various challenges, e.g., to reverse engineer and analyze a set of suspicious applications. There were also walkthroughs to explain how solutions should be implemented. During the exercises, tutors also walked around helping students to complete the exercises.

The day was closed with a presentation by Herbert Bos who discussed his view on promising directions (and not so promising ones) in malware research for smartphones. The time that smartphones were considered interesting in and of themselves is over and researchers should carefully consider what is truly novel about what they are doing. If anything, it seems today's PCs are more critical toward research, than say, Android or iOS.

Figure 7 Matthias Neugschwandtner during the hands-on exercise.

Figure 8 Tutors helping students during the hands-on exercises.

Finally, the first night we also organized a social dinner.

Figure: Summer school social dinner

4.2 Highlights of the second day

The second day, the lectures focused on highlighting more advanced techniques in dynamic analysis of mobile applications. Victor Van Der Veen introduced advanced malware tactics, such as dynamic code loading and permission circumvention. Victor also presented in detail the Trace Droid platform, a dynamic analysis tool for Android applications.

Figure 9 Victor Van Der Veen presenting the TraceDroid platform.

During the second session of the second day, Thanasis Petsas taught students techniques on evading dynamic-analysis environments. After the tutorial, students were given a custom app with malicious functionality. The challenge was to hide this functionality by patching the bytecode of the app with a simple VM-evasion technique. At the end, students had to submit both the original and the repackaged application to an online analysis service (e.g., Andrubis) in order to draw conclusions.

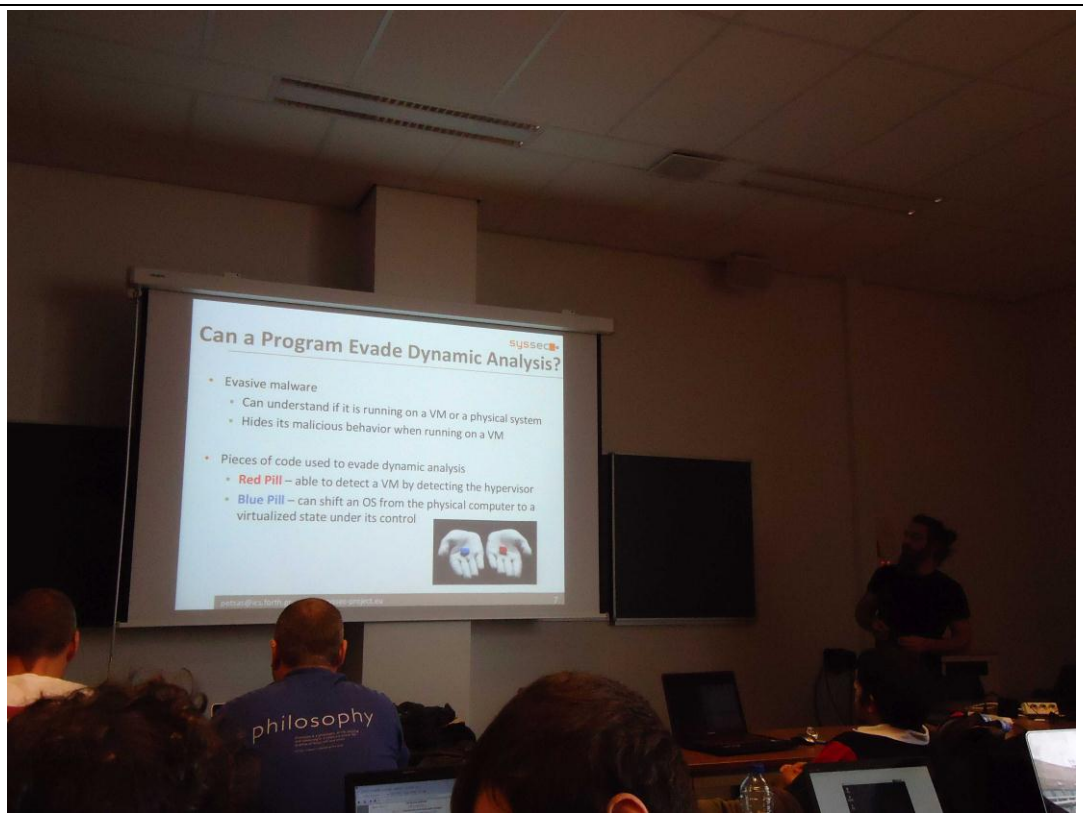


Figure 10 Thanasis Petsas is teaching techniques on how to evade dynamic-analysis.

4.3 Malware competition

Towards the end of the school, a malware competition was held for the participants. Students were divided in four teams. For each team, there was a team leader with experienced skills in Android/Java coding. A benign application with many permissions was given to the teams. The first challenge was to hide a malicious functionality of their choice inside the application. All teams had to complete the challenge and put the malicious application in a USB stick within a specific time frame.

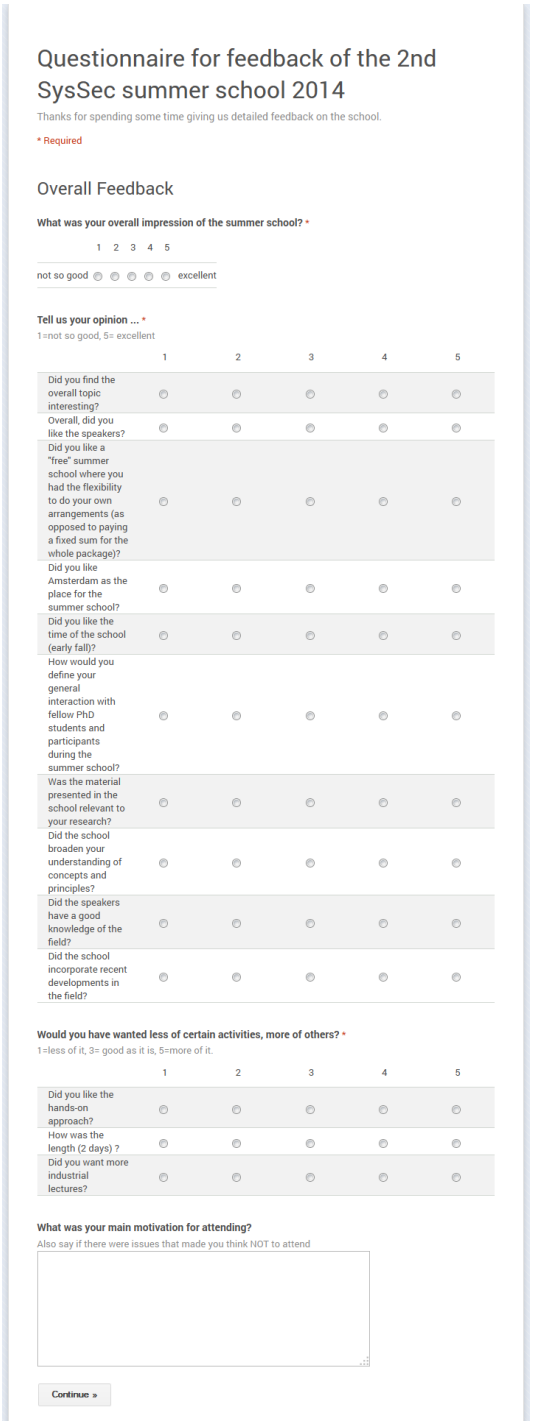
After that, each team exchanged applications with another team. By using the reverse engineering techniques, teams had to identify the malicious functionality of the given applications and infer what the other team had done. At the end, each team leader presented the findings of his team and the committee announced the winner. The criteria were based on the creativity of the teams, the sophistication of techniques used for hiding the malicious functionality inside the applications and the degree of details of their reverse-engineering tasks.

Figure 11 Malware competition.

5 Description of Web 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 implementation of the school worked. The questions were divided into three sections: overall feedback, feedback on the first day and feedback on the second day.

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.


Questionnaire for feedback of the 2nd SysSec summer school 2014

Thanks for spending some time giving us detailed feedback on the school.

* 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 incorporate recent developments in the field?	○	○	○	○	○

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

1=less of it, 3= good as it is, 5=more of it.

	1	2	3	4	5
Did you like the hands-on approach?	○	○	○	○	○
How was the length (2 days) ?	○	○	○	○	○
Did you want more industrial lectures?	○	○	○	○	○

What was your main motivation for attending?

Also say if there were issues that made you think NOT to attend

Continue »

Figure 12 Web questionnaire

5.1 Overall Feedback

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

Tell us your opinion …

- Did you find the overall topic interesting? (4.6)
- Overall, did you like the speakers? (4.4)
- 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)? (4.4)
- Did you like Amsterdam as the place for the summer school? (4.6)
- Did you like the time of the school (early fall)? (4.4)
- How would you define your general interaction with fellow PhD students and participants during the summer school? (3.6)
- Was the material presented in the school relevant to your research? (3.6)
- Did the school broaden your understanding of concepts and principles? (4.2)
- Did the speakers have a good knowledge of the field? (4.5)
- Did the school incorporate recent developments in the field? (4.2)

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

- Did you like the hands-on approach? (4.6)
- How was the length (2 days)? (4.2)

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

5.2 First Day Feedback

Overview of the first day (1 = I disagree with the statement, 5 = I fully agree with the statement)

- I liked the topics of the first day (4.1)
- The hands-on approach was excellent (4.3)
- The challenges were of just the right difficulty (3.9)
- I feel like I learned something new (4.2)
- The mix between lecture / exercise was right (4.2)
- I thought one day of tutorial and Android application analysis techniques were enough (3.0)

5.3 Second Day Feedback

Overview of the second day (1 = I disagree with the statement, 5 = I fully agree with the statement)

- I liked the topics of the second day (4.5)
- The second day was quite advanced for me (2.8)
- I feel like I learned new things the second day (4.2)
- I would have liked longer lecture slots for each teacher (3.9)
- I liked the security competition of the last session (4.3)

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

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

6 Analysis of the answers to the Questionnaire

We summarize only a few of the questions of relevance to the execution of the second summer school. 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.

Overall, the students liked the summer school. On a scale from 1 to 5, the average was 4.27. 32% of the participants gave the highest grade (5) and 63% gave the next highest grade (4).

The participants liked the topic of the school (average 4.6) and it seemed the students especially appreciated the hands on approach. 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.

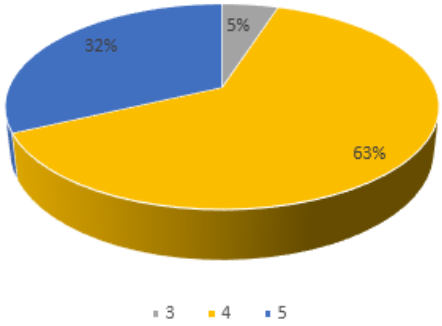


Figure 13 Overall impression

The speakers were well appreciated. On the question "Tell us your opinion ... [Did the speakers have a good knowledge of the field?]" the average is 4.4. Moreover, the participants expressed that they learned new concepts[1].

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 4.1. For the second day, the same question gave 4.5. Participants enjoyed more the second day of the summer school due to the security competition that was held at the end of the day (4.3).

It seemed that a majority of students actually felt like they did pick up new skills after the first day[2] but the tutorial sessions may were a bit advanced for some students[3]. The participants had very different backgrounds, where some were experts and others novices to Android malware and reverse engineering.

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 4.6) and the time of the school (early fall) (4.4).

[1] Tell us your opinion ... [Did the school broaden your understanding of concepts and principles?] 4.2

[2] Overview of the first day [I feel like I learned something new] 4.2

[3] Overview of the first day [The challenges were of just the right difficulty] 3.9

The length of the summer school was a bit debated. A longer school may have been appreciated more[4]. Many suggested three days as ideal. This would have given more time to the exercises and the competition but still keep the introduction lectures intact. Some stress the need for only a single day of tutorials, a second day with hands-on exercises and a final day with the malware competition. As expected, as the summer school was quite short the student participation and networking was more challenging than usual.[5]

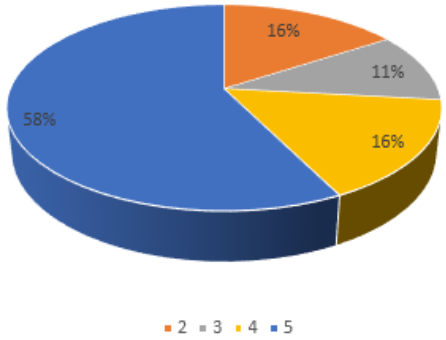


Figure 14 whether to have longer / shorter school

[4] Would you have wanted less of certain activities, more of others? [How was the length (2 days) ?] 4.2

[5] Tell us your opinion … [How would you define your general interaction with fellow PhD students and participants during the summer school?] 3.6

7 Conclusions

The second SysSec summer school took place took place at Vrije Universiteit (VU) Amsterdam, Thursday September 25 to Friday September 26, 2014. Its main topic was mobile malware with a special focus on reverse engineering and analyzing Android malware. One of the goals of the second SysSec Summer School was to have a hands-on approach similarly to the first summer school. We wanted the students to develop a skill but also learn from experts in the area.

We had six 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 static and dynamic application analysis with lectures and practical exercises, while the second day focused on lectures highlighting more advanced techniques in dynamic analysis. Also, towards the end of the summer school, a malware competition was held for the participants.

The summer school filled up very quickly and a waiting list was actually created. After changing the arrangements for the rooms, we managed to admit 42 of these to the summer school.

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.