

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*

D1.1: First Periodic Progress Report[†]

Abstract: This is the first periodic progress report of the SysSec project. It describes the objectives of the project, the work performed during its first year, the deliverables submitted, as well as the financial figures of this reporting period.

Contractual Date of Delivery	August 2011
Actual Date of Delivery	October 2011
Deliverable Security Class	Public
Editor	Evangelos Markatos
Contributors	All <i>SysSec</i> partners

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.

Declaration by the scientific representative of the project coordinator

I, as scientific representative of the coordinator of this project and in line with the obligations as stated in Article II.2.3 of the Grant Agreement declare that:

- The attached periodic report represents an accurate description of the work carried out in this project for this reporting period;
- The project (tick as appropriate)³:
 - has fully achieved its objectives and technical goals for the period;
 - has achieved most of its objectives and technical goals for the period with relatively minor deviations.
 - has failed to achieve critical objectives and/or is not at all on schedule.
- The public website, if applicable
 - is up to date
 - is not up to date
- To my best knowledge, the financial statements which are being submitted as part of this report are in line with the actual work carried out and are consistent with the report on the resources used for the project (section 3.4) and if applicable with the certificate on financial statement.
- All beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs, have declared to have verified their legal status. Any changes have been reported under section 3.2.3 (Project Management) in accordance with Article II.3.f of the Grant Agreement.

Name of scientific representative of the Coordinator: Evangelos Markatos

Date: 31/8/2011

For most of the projects, the signature of this declaration could be done directly via the IT reporting tool through an adapted IT mechanism.

³ If either of these boxes below is ticked, the report should reflect these and any remedial actions taken.

Contents

DECLARATION BY THE SCIENTIFIC REPRESENTATIVE OF THE PROJECT COORDINATOR.....	3
CONTENTS	4
1. PUBLISHABLE SUMMARY	6
1.1. SUMMARY DESCRIPTION OF PROJECT CONTEXT AND OBJECTIVES	6
1.2. WORK PERFORMED SINCE THE BEGINNING OF THE PROJECT AND MAIN RESULTS ACHIEVED SO FAR.....	7
1.2.1. WP1: Project Management.....	7
1.2.2. WP2: Dissemination	8
1.2.3. WP3: Education and Training	9
1.2.4. WP4: Threats on the Future Internet.....	9
1.2.5. WP5: Malware and Fraud.....	10
1.2.6. WP6: Smart environments	10
1.2.7. WP7: Cyberattacks	11
1.3. EXPECTED FINAL RESULTS AND THEIR POTENTIAL IMPACT AND USE (INCLUDING THE SOCIO-ECONOMIC IMPACT AND THE WIDER SOCIETAL IMPLICATIONS OF THE PROJECT SO FAR).....	11
1.4. ADDRESS OF THE PUBLIC PROJECT WEBSITE	12
2. CORE OF THE REPORT FOR THE PERIOD: PROJECT OBJECTIVES, WORK PROGRESS AND ACHIEVEMENTS, PROJECT MANAGEMENT	13
2.1. PROJECT OBJECTIVES FOR THE PERIOD	13
2.1.1. Summary of the recommendations from the previous reviews.....	13
2.2. WORK PROGRESS AND ACHIEVEMENTS DURING THE PERIOD	13
2.2.1. WP2: Dissemination	14
2.2.1.1. Summary of progress towards objectives	14
2.2.1.2. Significant Results	14
2.2.1.3. Deviations from Annex I and their impact (if any).....	14
2.2.1.4. Failure to achieve critical objectives or not being on schedule (if applicable).....	14
2.2.1.5. Use of resources	15
2.2.1.6. Corrective Actions (if applicable).....	15
2.2.1.7. Evaluation Criteria.....	16
2.2.2. WP3: Education and Training	16
2.2.2.1. Summary of progress towards objectives	17
2.2.2.2. Significant Results	17
2.2.2.3. Deviations from Annex I and their impact (if any).....	17
2.2.2.4. Failure to achieve critical objectives or not being on schedule (if applicable).....	17
2.2.2.5. Use of resources	18
2.2.2.6. Corrective Actions (if applicable).....	18
2.2.2.7. Evaluation Criteria.....	19
2.2.3. W4: Threats on the Future Internet	19
2.2.3.1. Summary of progress towards objectives	19
2.2.3.2. Significant Results	20
2.2.3.3. Deviations from Annex I and their impact (if any).....	20
2.2.3.4. Failure to achieve critical objectives or not being on schedule (if applicable).....	20
2.2.3.5. Use of resources	21
2.2.3.6. Corrective Actions (if applicable).....	21
2.2.3.7. Evaluation Criteria.....	21
2.2.4. WP5: Malware and Fraud.....	21
2.2.4.1. Summary of progress towards objectives	21
2.2.4.2. Significant Results	22
2.2.4.3. Deviations from Annex I and their impact (if any).....	22
2.2.4.4. Failure to achieve critical objectives or not being on schedule (if applicable).....	23
2.2.4.5. Use of resources	23
2.2.4.6. Corrective Actions (if applicable).....	23
2.2.4.7. Evaluation Criteria.....	23
2.2.5. WP6: Smart Environments.....	24
2.2.5.1. Summary of progress towards objectives	24
2.2.5.2. Significant Results	24

2.2.5.3.	Deviations from Annex I and their impact (if any).....	25
2.2.5.4.	Failure to achieve critical objectives or not being on schedule (if applicable).....	25
2.2.5.5.	Use of resources	25
2.2.5.6.	Corrective Actions (if applicable).....	25
2.2.5.7.	Evaluation Criteria.....	25
2.2.6.	<i>WP7: Cyberattacks</i>	25
2.2.6.1.	Summary of progress towards objectives	25
2.2.6.2.	Significant Results.....	26
2.2.6.3.	Deviations from Annex I and their impact (if any).....	26
2.2.6.4.	Failure to achieve critical objectives or not being on schedule (if applicable).....	26
2.2.6.5.	Use of resources	27
2.2.6.6.	Corrective Actions (if applicable).....	27
2.2.6.7.	Evaluation Criteria.....	27
2.3.	PROJECT MANAGEMENT DURING THE PERIOD	28
2.3.1.	<i>Consortium Management Tasks and achievements</i>	28
2.3.2.	<i>Problems which have occurred</i>	28
2.3.3.	<i>Changes in the consortium, if any</i>	28
2.3.4.	<i>List of project meetings, dates and venues</i>	29
2.3.5.	<i>Project Planning and status</i>	30
2.3.5.1.	Project status.....	30
2.3.5.2.	Project Planning.....	30
2.3.6.	<i>Impact of possible deviations from the planned milestones and deliverables, if any</i>	30
2.3.7.	<i>Changes to the legal status of any of the beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs;</i>	31
2.3.8.	<i>Development of the Project website, if applicable;</i>	31
2.3.9.	<i>Evaluation Criteria</i>	31
2.3.10.	<i>Person Months</i>	32
2.4.	DELIVERABLES AND MILESTONES TABLES	33
2.4.1.	<i>Deliverables</i>	33
2.5.	FINANCIAL STATEMENTS – FORM C AND SUMMARY FINANCIAL REPORT	35
2.5.1.	<i>Milestones</i>	37
2.5.2.	<i>Person Month Status Table</i>	38
2.6.	EXPLANATION OF THE USE OF THE RESOURCES.....	39
2.7.	<i>FINANCIAL STATEMENTS – FORM C AND SUMMARY FINANCIAL REPORT</i>	48

1. Publishable summary

1.1. Summary Description of Project Context and Objectives

The objectives of the SysSec Network of Excellence are:

- **To create an active, vibrant, and collaborating community of Researchers with the expertise, capacity, and determination to anticipate and mitigate the emerging threats and vulnerabilities on the Future Internet.** Although European Researchers have been active in this research area, their efforts are currently relatively fragmented. SysSec aims (i) to create a sense of “community” among those researchers, (ii) to mobilize this community, (iii) to consolidate its efforts, (iv) to expand their collaboration internationally, and (v) to become the single point of reference for Systems Security research in Europe.
- **To advance European Security Research well beyond the state of the art.** Despite European Researchers making tangible contributions in the area, their efforts have been scattered over a wide spectrum of activities, spreading themselves thin, and diluting their contribution. This project aims to *provide a research agenda* and *align their research activities* with the agenda, so as to maximize not only the impact of individual researchers, but to make SysSec a leading player in the international arena.
- **To create a virtual distributed Center of Excellence in the area of emerging threats and vulnerabilities.** By forming a critical mass of European Researchers and by aligning their activities, SysSec aims to create a virtual distributed center of excellence which will have the gravitas needed to play a leading role internationally, empowered to undertake large-scale, ambitious and high-impact research efforts.
- **To create a Center of Academic Excellence in the area.** This center will create an education and training program targeting young researchers and the industry. This common program is expected to lay the foundations for a common graduate degree in the area with emphasis on Systems Security.
- **To maximize the impact of the project by proactive dissemination to the appropriate stakeholders.** SysSec will disseminate its results to international stakeholders so as to form the needed strategic partnerships (with similar projects and organizations overseas) to play a major role in the area. At the same time, dissemination within the Member States will reinforce SysSec's role as a center of excellence and will **make SysSec a beacon for a new generation of European Researchers.**
- **To create Partnerships and transfer technology to the European Security Industry.** Over the past few years, the European network security industry has started to bloom and compete head-to-head with the established software juggernauts from the United States. Several European SMEs, such as F-Secure, Panda Labs, Hispasec, etc., have started to make profitable contributions to the European Market. At the same time, sensing an opportunity, several global-reach security corporations, such as Symantec and Microsoft, have started to create Research labs in Europe, capitalizing on the available European expertise. Within SysSec we plan to create a close partnership with Security Industry and to facilitate technology transfer wherever possible to further strengthen the European Market.



1.2. Work Performed since the beginning of the project and main results achieved so far

During its first year, the project progressed as expected and achieved significant results as explained in this section.

1.2.1. WP1: Project Management

WP1 run for the entire duration of the reporting period, during which achieved several results including:

- WP1 Created and mobilized all the committees of the project. These committees included:
 - **General Assembly.** This is the main decision-making body of the project. Each partner has one regular and one alternate member in the GA. These members are:
 - Regular members:
 - Davide Balzarotti, Eurecom
 - Evangelos Markatos, FORTH-ICS
 - Kiril Boyanov, IICT-BAS
 - Stefano Zanero, PoliMi
 - Yasin Yilmaz, TUBITAK
 - Paolo Milani, TUV
 - Herbert Bos, VU
 - Magnus Almgren, Chalmers
 - Alternate members:
 - Engin Kirda, Eurecom
 - Sotiris Ioannidis, FORTH-ICS
 - Dimitar Todorov, IICT-BAS
 - Federico Maggi, PoliMi
 - Ali Rezaki, TUBITAK
 - C. Platzner, TUV
 - Andrei Bacs, VU
 - Philippas Tsigas, Chalmers
 - **Quality Monitoring Committee.** This Committee monitors and ensures the quality of the results of the project. Its members include:
 - Herbert Bos, head
 - Magnus Almgren
 - Marco Balduzzi
 - Michalis Polychronakis
 - Zlatogor Minchev
 - Federico Maggi
 - Ali Rezaki
 - Christian Platzner
 - **Industrial Advisory Board (IAB).** This committee provides feedback to the project and acts as a liaison with the industry. Its members are:
 - Marc Dacier, Symantec

- John Ioannidis, Google
- Mikko Hipponen, F-Secure
- Leif Axelsson, Lindholmen Science Park
- George Danezis, Microsoft
- Julio Canto, HISPASEC
- Jean-Pierre Faye, Thales
Raytheon Systems



- **Evaluation Committee.** Its members are the WP leaders, of the QMC and the project manager:
 - Herbert Bos, head
 - Evangelos Markatos
 - Stefano Zanero
 - Davide Balzarotti
 - Paolo Milani
 - Philippas Tsigas
 - Sotiris Ioannidis

- Within WP1, the project coordinator created, updated, and coordinated the signing of the project's **Consortium Agreement**.
- The project manager created and operated an SVN-based collaboration environment. This environment enables all partners to have access to all project-related data instantly. SVN eliminates the need to send large attachments via email all the time and freed partners from the burden of receiving, unpacking and filing project-related information. SVN is especially useful for people who joined the project at a later stage and had not received the early emails.

1.2.2. WP2: Dissemination

WP2, which runs for the entire duration of the project, coordinated several activities including:

- WP2 Created and operated the **Web site** – the main electronic dissemination arm of the project – and created a social circle around it with both a Facebook page and a Twitter account (intensely used to disseminate about events participations, published papers and news about SysSec).
- W2 organized and held one **panel** about the role of machine learning in system security at an international conference (EC2ND 2010) where people from both academia and industry participated.
- WP2 organized the first public **project workshop**, co-located with DIMVA 2011 that attracted more than 75 participants: 23 position papers and 6 strong research papers were accepted.
- SysSec supported partners in **publishing** more than several tens of papers in international conferences (including top venues such as NDSS, ACSAC, USENIX LEET, WWW, FC) and journals (such as ACM TOCS).

Viking, Göteborg Energy (Western Sweden's leading energy company), E.ON Sweden (E.ON Sweden produces and supplies energy and energy-related services to approximately one million customers), and “Swedenergy” (“the voice of the Swedish energy industry”), in particular the working group EBITS that focuses on the information infrastructure in energy systems and its security.

- Finally, WP6 members had an internal presentation for publically available simulation platforms used by Chalmers for research on Sensor Networks and Smart Cars to enhance collaboration on the consortium on the respective subjects.

1.2.7. WP7: Cyberattacks

This Work Package, which runs for the entire duration of the project, has a dual goal: (i) to advance the state of the art in the area of network-level detection and mitigation of cyberattacks, and (ii) to improve our understanding of new and emerging types of cyberattacks, such as attacks on and by mobile phones, web attacks, attacks on home and office automation devices, cross-domain attacks, etc. The major contributions include, but are not limited to, the following ones:

- Delivery of D7.1, the **Review of the State-of-the-Art in Cyberattacks**, which was due in month 9.
- Investigated packet **capturing and intrusion detection**, as well as power consumption when running security applications, on Android smartphones.
- Published eleven papers in the first year of the project, two of which were published in the 1st SysSec Workshop. An additional four papers by the lead beneficiary of WP7 are scheduled to be published in the second year of the project.
- Helped organize the 2011 **European Conference on Computer Network Defense (EC2ND 2010)**.

1.3. Expected final results and their potential impact and use (including the socio-economic impact and the wider societal implications of the project so far)

The most important result of the project consist in **achieving its objectives**. That is, to:

- Create a community of researchers to anticipate and mitigate the emerging threats and vulnerabilities on the future Internet
- Advance European security research well beyond the state of the art
- Create a distributed Center of Excellence in the area of emerging threats and vulnerabilities
- Create a center for academic excellence in the area
- Maximize the impact of the project through proactive dissemination
- Create partnerships and transfer technology to the European Security Industry

We believe that the project is on a very good track towards achieving its objectives. As explained in the remainder of this report, the project has achieved (if not over-achieved) its success indicators and it is on a good track to achieve its objectives.

1.4. Address of the public project website

The web site of the project is publicly available at www.syssec-project.eu.



Figure 3: The number of visitors (per month) to the project’s web site steadily increases.

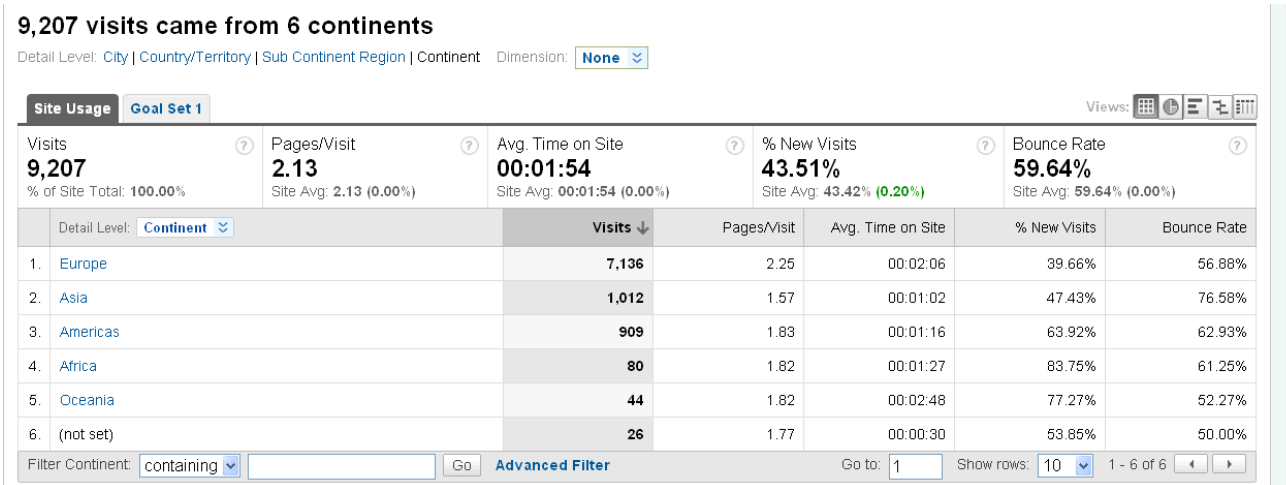


Figure 4: Geographic origin of the visitors of the SysSec web site.

The site is serving as the main electronic dissemination medium of the project.

2. Core of the report for the period: Project Objectives, work progress and achievements, project management

2.1. Project Objectives for the period

The objectives of the SysSec project for this period are:

- **To start the creation of an active, vibrant, and collaborating community of Researchers with the expertise, capacity, and determination to anticipate and mitigate the emerging threats and vulnerabilities on the Future Internet.**
- **To advance European Security Research well beyond the state of the art.** Despite European Researchers making tangible contributions in the area, their efforts have been scattered over a wide spectrum of activities, spreading themselves thin, and diluting their contribution. This project aims to *provide a research agenda and align their research activities* with the agenda, so as to maximize not only the impact of individual researchers, but to make SysSec a leading player in the international arena.
- **To start the creation of a virtual distributed Center of Excellence in the area of emerging threats and vulnerabilities.** By forming a critical mass of European Researchers and by aligning their activities, SysSec aims to create a virtual distributed center of excellence which will have the gravitas needed to play a leading role internationally, empowered to undertake large-scale, ambitious and high-impact research efforts.
- **To contribute towards maximizing the impact of the project by proactive dissemination to the appropriate stakeholders.**



2.1.1. Summary of the recommendations from the previous reviews

This is the first periodic report of the project. There have been no previous reviews.

2.2. Work progress and achievements during the period

During the first year of the SysSec project, the work has progressed in line with the structure of Annex I:

- All deliverables have been delivered.
- All milestones have been reached on time.

Some of the achievements of the first year include:

- We created a **community** of more than 200 researchers in Europe.
- We delivered a **Research Roadmap** in the area of Emerging Risks and Vulnerabilities for the Future Internet.

- We organized the **First SysSec Workshop** in Amsterdam. The SysSec workshop was so successful that attracted two more projects to collocate their events with the SysSec workshop: the BIC project and the EffectsPlus project.

2.2.1. WP2: Dissemination

The overall dissemination output of SysSec indicates the determination of the consortium to impact the security research landscape, both by developing and presenting significant research results, and by stimulating discussion, debate and the formation of a European community devoted to Systems Security Research.

2.2.1.1. Summary of progress towards objectives

The Work Package has made outstanding progress towards the objectives, meeting or exceeding, all of the evaluation criteria set forth in the DoW and the consortium plans for the first year. Particularly significant is the number of published papers and news items.

2.2.1.2. Significant Results

The determination of the consortium in dissemination and networking activity yielded many collaborations both among partners and also with external researchers. The first concrete result of this is an outstanding number of published papers (more than 30) in international conferences, workshops and journals. Another significant result is that the consortium collaborates with the leading members of 3 EU projects. Since the beginning of the project, one of the partners (VU) has been able to establish cooperation with the Dutch Ministry of Defence.

The most significant result is the outcome of the first public workshop organized by SysSec, which attracted more than 70 people, about 85% of the people who attended the main co-located conference (DIMVA 2011). During the workshop, the consortium received very positive feedback from both paper authors and participants about the need of an effort, like the one that is being undertaken by SysSec, to create a strong community of system security researchers in Europe.

2.2.1.3. Deviations from Annex I and their impact (if any)

None.

2.2.1.4. Failure to achieve critical objectives or not being on schedule (if applicable)

None.

2.2.1.5. Use of resources

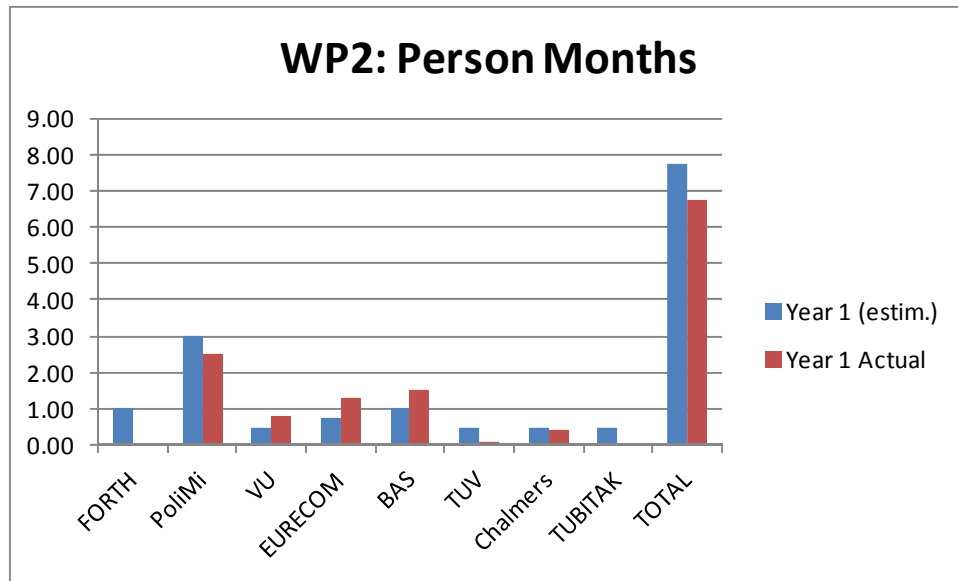


Figure 5: Person months charged in WP2 by each partner.

The above figure presents the number of person months invested by each partner in WP2. We see that for most partners the number of invested (Actual) person months are in line with the number of estimated (estim.) person months. We only see that FORTH has charged less person months than originally planned as explained in section 2.3.10. in page 32.

2.2.1.6. Corrective Actions (if applicable)

None.

2.2.1.7. Evaluation Criteria

Name	Target Value	Achieved Value
Number of papers published in leading conferences	6	7 ⁷
Number of papers published in all conferences and workshops	12	30 ⁸
Number of external attendees to the project's events	10-20 (per event)	58 ⁹
Number of collaborations with leading members of the academia/industry (outside the project's partners)	2-3 (10 total)	3 ¹⁰
Number of news/press items	2-3 (10 total)	12
Number of white papers	1-2 (6 total)	0
Memberships in the PCs of conferences and in editorial boards of journals	7-8 (30 total)	11 ¹¹
Invited talks and tutorials by members of SysSec	2-3 (10 total)	1 ¹²

2.2.2. WP3: Education and Training

Work Package 3 (WP3) consists of three tasks: (a) short-term visits (researcher exchanges), (b) common curriculum, and (c) summer schools. As the common curriculum and summer schools

⁷ Demetris Antoniadis, Iasonas Polakis, Georgios Kontaxis, Elias Athanasopoulos, Sotiris Ioannidis, Evangelos P. Markatos, and Thomas Karagiannis. we.b: The Web of Short URLs. In Proceedings of the 20th International World Wide Web Conference (WWW), Hyderabad, India, March 2011.

Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. Paranoid android: Versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), Austin, TX, December 2010.

Kaan Onarlioglu, Leyla Bilge, Andrea Lanzi, Davide Balzarotti, and Engin Kirda. G-free: Defeating return-oriented programming through gadget-less binaries. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), Austin, TX, December 2010.

Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. Comprehensive shellcode detection using runtime heuristics. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), Austin, TX, December 2010.

Alexandros Kapravelos, Iasonas Polakis, Elias Athanasopoulos, Sotiris Ioannidis, and Evangelos P. Markatos. D(e—i)aling with VoIP: Robust Prevention of DIAL Attacks. In Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS), Athens, Greece, September 2010.

Asia Slowinska, Traian Stancescu, and Herbert Bos. Howard: a dynamic excavator for reverse engineering data structures. In Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS), San Diego, CA, February 2011.

Andreas Larsson and Philippos Tsigas. A Self-stabilizing (k,r)- clustering Algorithm with Multiple Paths for Wireless Ad-hoc Networks. In Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS 2011), Minneapolis, Minnesota, USA, June 2011.

⁸ A full list of publications can be found at <http://www.syssec-project.eu/publications/>

⁹ There were 73 registered participants in the first SysSec workshop. Out of them, 58 were not affiliated with the project partners. The list of the registered participants is available on request.

¹⁰ BIC, EffectsPlus, VIKING projects

¹¹ Herbert Bos (CCS 2011, EUROSYS 2011, and DIMVA 2011), Evangelos Markatos (ASPLOS 2012 and Financial Crypto 2011), Stefano Zanero (Journal of Computer Virology), Sotiris Ioannidis (ICC 2011 and RAID 2011), Marina Papatrifaftylou (IPDPS 2011), Davide Balzarotti (NDSS 2011 and RAID 2011)

¹² Evangelos Markatos, "SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet", Northeastern University, July 2011.

subtasks are scheduled to start only in the second year of the project, we hereby discuss the short-term visits. This by no means implies that the consortium had no activities in the other two subtasks. Significant preparatory and exploratory work was done specifically for the common curriculum. However, concrete results will be achieved and reported in the second year.

2.2.2.1. Summary of progress towards objectives

In the short-term visits, we originally anticipated a single instrument: research exchange scholarships that would allow researchers from all over Europe to spend up to four months at one of the partner institutes. The scholarship would cover a significant portion of the researcher's living and travel expenses (but not necessarily all) and the procedure was intentionally kept as light-weight as possible—lowering the threshold for candidates to apply. In Q4 of the first year, however, we imitated a second instrument to boost system security research in Europe, and increase the researchers' mobility by means of the SysSec Marie Curie Fellowship Programme. The idea was that we stimulate and help system security researchers with their applications to Marie Curie Fellowships in a competitive process. While no direct funding would be allocated, the support would still be substantial. The consortium took it upon itself to:

- help the candidate look for a suitable hosting institute;
- write a support letter;
- offer successful candidates an opportunity to spend a few weeks at each and every academic partner in the SysSec consortium—thereby bolstering the candidate's application by means of demonstrable international connections and mobility;
- provide direct feedback on the proposal

Despite the lateness of the initiative (we started the activity in June 2011, while the deadline for Marie Curie Fellowships was August 11th), we received no fewer than 10 applications. Three of these looked strong and interesting enough to warrant support and eventually one was submitted.

2.2.2.2. Significant Results

We worked out a light-weight procedure for the SysSec scholarships and advertise a call for these scholarships throughout the community via direct mailing and on our websites. Similarly, we drafted a procedure for the SysSec Marie Curie Fellowship program that we advertised in similar ways. Since then we awarded 4 SysSec scholarships, which is approximately according to expectation since we started in February (after determination of the rules and procedures) and we expect to award 22 scholarship over the duration of the project. Similarly, we supported one of 10 applications to the SysSec Marie Curie Fellowship programme. Two others who were accepted in the competitive application process failed to submit their full applications to the EU in time.

2.2.2.3. Deviations from Annex I and their impact (if any)

None

2.2.2.4. Failure to achieve critical objectives or not being on schedule (if applicable)

Not applicable

2.2.2.5. Use of resources

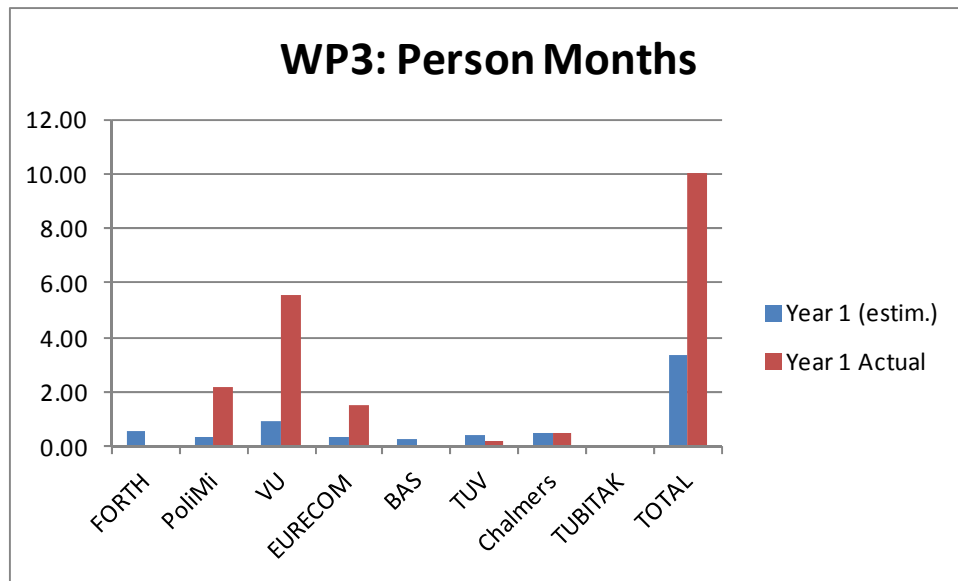


Figure 6: Person Months charged in WP3

We see that we have charged slightly more person months than originally estimated. This is due to the fact that although most of the WP3 activities do not officially start before the second year of the project, we were able to do some preliminary work during the first year as well.

2.2.2.6. Corrective Actions (if applicable)

Not applicable

2.2.2.7. Evaluation Criteria

Name	Target Value	Achieved Value
Courses designed/redesigned	10 (total)	Not started yet
Courses taught	6 (total)	Not started
Participating Universities	10 (total)	Not started
Scholarships awarded	22 (Total)	4 ¹³
Graduated Ph.Ds	5 (Total)	0
Graduated Masters	25 (Total)	19 ¹⁴

2.2.3. W4: Threats on the Future Internet

2.2.3.1. Summary of progress towards objectives

During the first year of the project, we created the three Working Groups (WGs) operating respectively in the areas of Malware and Fraud, Smart Environment, and Cyberattacks. This initial setup reflected both the research interests of the SysSec partners and the success of the working groups defined by the previous FORWARD project¹⁵. The three WGs met in Amsterdam in

¹³ The list of fellows is:

- Apr 2011: Sevil Sen, from Hacettepe University, Turkey to Eurecom
- Jul 2011: Matthias Neugschwandtner, from TUV, Austria to VU
- Jul 2011: Rafael A. RodrΓ-guez Gmez, from U. of Granada, Spain to Eur
- Sep 2011: Roman Kochanek from Ruhr Uni. Bochum, Germany to Milan

¹⁴ The following is the list of M.S. graduates:

- VU
 - o Silviu Baranga, "Probing Data Obfuscators, September 2011
 - o Valentina Sandulescu, "Adding taint analysis to native code in an LLVM compilation stage", August 2011
 - o Marthijn van den Heuvel, "Keystroke dynamics in the mobile world, August 2011
 - o Marius Sandu-Popa, "Reverse engineering high-level data structures", August 2011
 - o Traian Stancescu, "BodyArmor: Adding data protection to binary executables", August 2011
 - o Tudor Zaharia, "Nemulator: a distributed real-time network intrusion detector", February 2011
- FORTH:
 - o Giorgos Kondaxis, "A Lightweight Censorship-Resistant Web Access Architecture", June 2011
 - o Eleni Gesiou "Fishing in the Deep Web", June 2011
 - o Apostolis Zaras "Analyzing and Defending Against Fraud in the Underground Economy", June 2011
- POLIMI
 - o Andrea Bellini, "A systematic study of malware naming inconsistencies", March 2011
 - o Claudio Caronia, "Modeling and simulation of Bluetooth malware spread", March 2011
 - o Mauro Pessina, "A methodology for analyzing bot-related malware datasets", March 2011
 - o Luca di Mario, "BURN: Baring Unknown Rogue Networks", July 2011
- Chalmers
 - o Akbar Hosseinkhani, "A Study of Mitigation of Denial of Capability (DoC) Attacks"
 - o Hao Ning, "Robust Overlay networks for Volunteer Computing, Decentralized Volunteer Computing Architecture With Fault-tolerance Design"
 - o Sebastian Kloft and Eva Lina Staaf, "Alarm management for intrusion detection systems Prioritizing and presenting alarms from intrusion detection systems"
 - o Yang Yuan Jin, "Personal Information Revelation and Privacy Mining A Practice of Swedish Online Privacy Harvest"
 - o Afshan Samani, "Security Aspects of Geographic Routing Protocols In Wireless Sensor Networks"
 - o C. Baudron and D. Taborda, "Network Intrusion Detection On Suricata Using Graphic Processor Units"



¹⁵ <http://www.ict-forward.eu/>

February 2011 for a face-to-face meeting. The goal was to brainstorm about current and upcoming threats in the respective areas, and to discuss our ideas and point of view with a number of external experts. Finally, the output of the working groups was summarized and presented in Deliverable “*D4.1: First Report on Threats on the Future Internet and Research Roadmap*”. The deliverable includes a list of upcoming threats and the first research roadmap. The roadmap presents a short list of research priorities that can be used to drive the work of Work Packages WP5, WP6, and WP7, as well as for the entire stakeholder community of SysSec.

2.2.3.2. Significant Results

The threat selection process was based on four different types of contributions:

- Personal experience of the internal members of the working groups
- Feedback provided by the state of the art documents prepared by Work Package 5 (WP5), Work Package 6 (WP6), and Work Package 7 (WP7)
- External experts who participated to the face-to-face WG meeting
- External experts who are members of the WG mailing lists.

The result of this process is summarized in deliverable D4.1. Here we report a short list of the new threats we believe that could be observed in the wild in the near future:

- Hardware backdoors
- Attacks against the hypervisor, in particular attacks against the cloud virtualization system or virtualization-based malware (ring -1 malware).
- De-anonymization and correlation of Government open data
- Exploitation of smart device remote update capabilities (as is the case for some smart meters)
- Attacks against the sensors non-ICT component (such as physical attacks to create false sensor data, maybe with side-effect propagated to a larger scale)
- Attacks against provider infrastructure to tamper with data on the cloud

2.2.3.3. Deviations from Annex I and their impact (if any)

None

2.2.3.4. Failure to achieve critical objectives or not being on schedule (if applicable)

All objectives have been successfully achieved. A draft of D4.1 has been delivered two months before the deadline upon request from the EU.

2.2.3.5. Use of resources

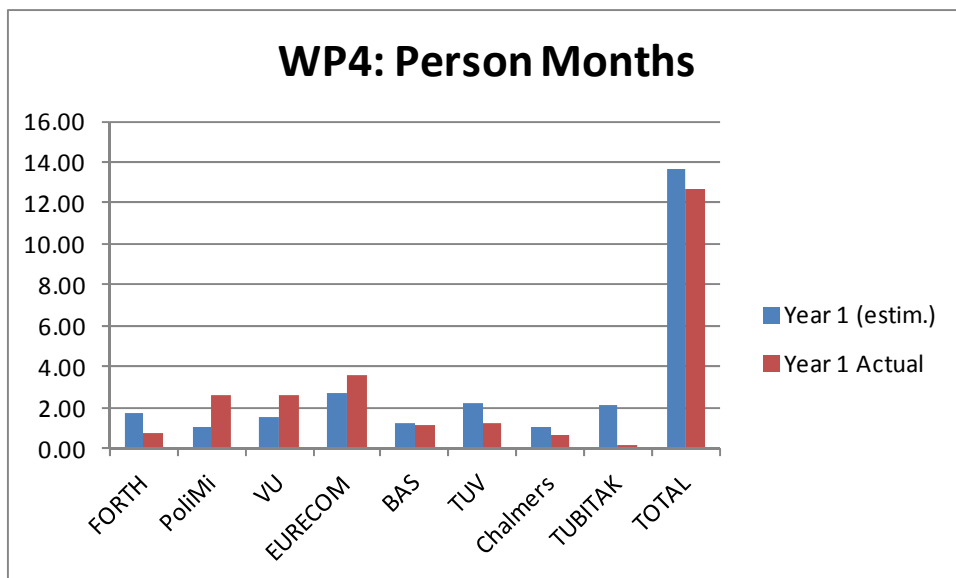


Figure 7: Person Months charged in WP4

2.2.3.6. Corrective Actions (if applicable)

2.2.3.7. Evaluation Criteria

Name	Target Value	Achieved Value
Concrete threats identified	15 (total)	6
Threats seen in the wild after being identified by the project	4 (total)	0 ¹⁶
Number of outside collaborators who contribute to the deliverables	40 (total)	17 ¹⁷

2.2.4. WP5: Malware and Fraud

2.2.4.1. Summary of progress towards objectives

In general, the main objectives during the first year of the SysSec project, as far as Work Package 5 (WP5) is concerned, can be summarized in two categories:

- a) Publications: The research conducted during the project is best quantized with the amount of published papers in leading conferences. In total, the consortium published 28 papers, some of them in leading conferences. Two of the top-tier papers are directly related to Malware and Fraud and therefore cited in the evaluation criterion.

¹⁶ Note that it is too early to see in the wild the emerging threats identified by this Work Package.

¹⁷ Page 7 of deliverable D4.1 lists the 17 people who made contributions to the list of emerging threats and the Roadmap.

- b) Deliverables: Deliverable 5.1, which was due in month 9, provides a survey of research and data collection initiatives relevant for this Work Package. Its main objective is to get an understanding on the “state-of-the-art” in malware. In other words, it describes which threats are currently the most discussed and researched in the academic community.

Overall, the project progress in Work Package WP5 is as expected and lives up to the proposed timeline.

2.2.4.2. Significant Results

The most significant result, which is also part of the evaluation criteria, was to gain a deeper understanding of current malware and advance the possibilities of an automated detection of such malicious programs. To this end, we employed automated analysis tools like *Anubis*.

Also a short explanation of the numbers presented in Section 2.2.4.7 shall be given:

- **Identified Threats:** As of today, we identified a number of threats but cannot claim to have already dealt with them properly. Nevertheless, we plan to properly address this shortcoming in the next year.
- **Malware analysis tools made public:** *Anubis* represents our publicly available implementation for malware analysis. It is actively developed and analyses tens of thousands of samples per day. Since we base our research on this framework, we add new features on a regular basis, while the concepts behind it are published as research papers.
- **Malware families analyzed:** From October 2010 until July 2011, a total of 4.639.690 samples were analyzed and categorized into families. As a lower bound (samples with assured family affiliation) we were able to identify 1017 malware families. Although this may look as if the target value of 5,000 families for the project duration is hard to achieve, the reality is different:
 - First, malware families were queried with a minimum size. Therefore, families with at least 25 members are needed to reflect in this number. The family labels were obtained by querying the *Anubis* database for their corresponding virus total identification. Smaller families were omitted because they don't represent a decent-sized tuple within the analysis results.
 - Second, smaller families will be grouped into larger families once an in-depth analysis is performed and similarities are discovered. This effectively increases the total number because samples not yet classified into families will form new clusters. Furthermore, results are then based on previous history, which was not available before the project started.

Therefore it can be expected to have more than 5,000 analyzed malware families after the total project duration of 4 years. A rough estimation will be given after the second year.

We will also elaborate on this point in the following yearly reports.

2.2.4.3. Deviations from Annex I and their impact (if any)

None

2.2.4.4. Failure to achieve critical objectives or not being on schedule (if applicable)

All objectives were completed according to the time plan, except the delivery of D.5.1, which was slightly delayed by 8 days. The delay was mainly caused by an additional round of proofreading and comments which had to be incorporated.

2.2.4.5. Use of resources

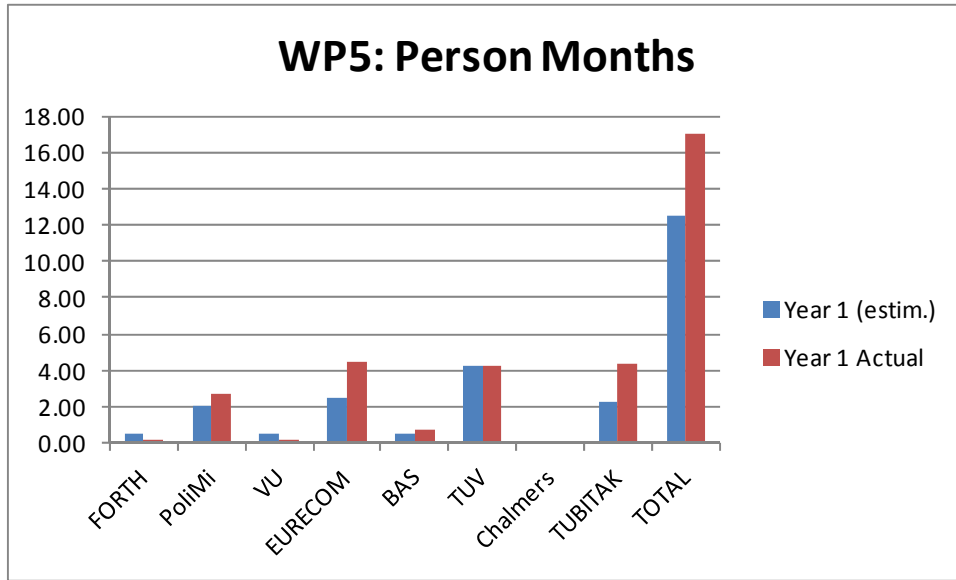


Figure 8: Person Months charged in WP5

2.2.4.6. Corrective Actions (if applicable)

None

2.2.4.7. Evaluation Criteria

Name	Target Value	Achieved Value
Number of papers published in leading conferences	2 (per year)	2 ¹⁸
Threats identified and dealt with	3 (total)	0
Malware analysis tools made available to the public	1 (total)	1 ¹⁹
Malware families analyzed	5,000 (total)	1,017

¹⁸ Asia Slowinska, Traian Stancescu, Herbert Bos. Howard: a dynamic excavator for reverse engineering data structures. In Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS). February 2011, San Diego, CA, USA.

Leyla Bilge, Engin Kirda, Christopher Kruegel, Marco Balduzzi. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. In Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS). February 2011, San Diego, CA, USA.

¹⁹ Anubis

2.2.5. WP6: Smart Environments

This work-package runs from the start of the project and is focused on sensor networks and Smart Car and Grid applications.

2.2.5.1. Summary of progress towards objectives

The activities in the Work Package 6 (WP6) have been focused toward the completion of the deliverable D6.1 (“Report on the State of the Art on Security in Sensor Networks”) and paper publications on relevant research describing our work. Some effort has also been spent to reconnect to experts from the previous EU FORWARD project²⁰ and connect with other leading industries related to the theme of the Work Package 6. In that, we have had several meetings with SP Technical Research Institute of Sweden, members of the EU project Viking, Göteborg Energy (Western Sweden's leading energy company), E.ON Sweden (E.ON Sweden produces and supplies energy and energy-related services to approximately one million customers), and “Swedenergy” (“the voice of the Swedish energy industry”), in particular the working group EBITS that focuses on the information infrastructure in energy systems and its security.

2.2.5.2. Significant Results

We have been working on the following issues: (i) secure routing on sensor networks, (ii) secure clustering in sensor networks, (iii) security issues and modeling of the connected car (iv) attack models that make use of the ON/OFF feature of smart meters and (v) Electricity routing on Smart Grids.

We have published two papers at leading conferences related to smart environments. One paper is related to the area of sensor networks and the other one to the smart grid:

- Phuong Nguyen, Wil Kling, Giorgos Georgiadis, Marina Papatriantafidou, Anh Tuan Le and Lina Bertling. Distributed Routing Algorithms to Manage Power Flow in Agent-Based Active Distribution Network. Proceedings of 1st Conference on Innovative Smart Grid Technologies Europe. Göteborg, Sweden, October 2010.
- Andreas Larsson and Philippas Tsigas. A Self-stabilizing (k,r)-clustering Algorithm with Multiple Paths for Wireless Ad-hoc Networks. In Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS 2011), June 2011, Minneapolis, Minnesota, USA.

The latter paper presents an algorithm that organizes the network using multiple communication paths to mitigate attacks by malicious insider nodes. The suggested algorithm mitigates certain attacks, and thus we successfully met the expected Work Package criterion for identification and mitigation of a smart-environment attack. Furthermore, some security issues of the connected car is summarized in

- Pierre Kleberger, Tomas Olovsson, and Erland Jonsson. Security Aspects of the In-Vehicle Network in the Connected Car. In Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (VI 2011), June 2011, Baden-Baden, Germany

The deliverable D6.1, the “Report on the State of the Art on Security in Sensor Networks”, was due in month 12. The deliverable summarizes the state of the art of sensor networks, describing attacks and current security strategies developed within the community.

²⁰ <http://www.ict-forward.eu/>

2.2.5.3. Deviations from Annex I and their impact (if any)

None

2.2.5.4. Failure to achieve critical objectives or not being on schedule (if applicable)

No significant failures or delays.

2.2.5.5. Use of resources

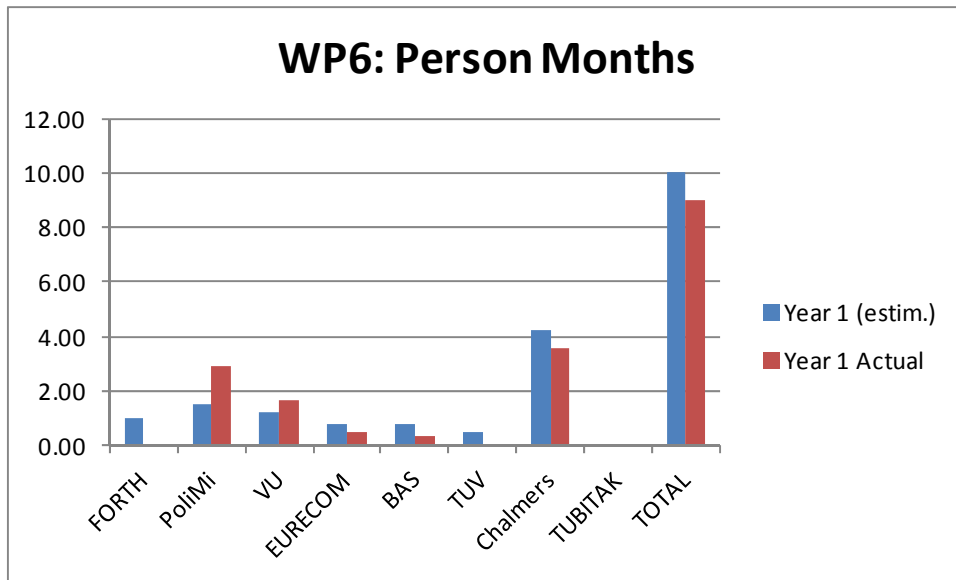


Figure 9: Person Months charged in WP6

2.2.5.6. Corrective Actions (if applicable)

None

2.2.5.7. Evaluation Criteria

Name	Target Value	Achieved Value
Number of papers published in leading conferences	2 (per year)	2 ²¹
Smart-environment attacks identified and mitigated	3 (total)	1 ²²

2.2.6. WP7: Cyberattacks

2.2.6.1. Summary of progress towards objectives

The main activities of the WP7 (Cyberattacks) Work Package can be summarized as follows:

- Deliverable 7.1, which was due in month 9, provides a **Review of the State-of-the-Art in Cyberattacks**. Cyberattacks were categorized in a number of main classes, and within those classes the most important types of attacks were presented.

²¹ Explanation in section 2.2.5.2

²² ICDCS paper in section 2.2.5.2

- We published a number of **papers** in the area of cyberattacks. A number of them in leading conferences in the area such as ESORICS, WWW and ACSAC.
- We worked on designing and building better systems for **intrusion detection and prevention** using graphics processors as accelerators.
- We worked on developing **packet-capturing application for Android smartphones**, as well as understanding the platform, the capabilities and power requirements.
- We worked on attacks on new **web services**. Specifically, data-mining online documents for private information and extracting private information from newly deployed online, state services.

Overall, the project progress in Work Package WP7 is as expected and lives up to the proposed timeline.

2.2.6.2. Significant Results

Throughout the course of the first year new research has been conducted in the area of cyberattacks. Since the area we have worked on is very broad, we highlight our achievements by focusing on three published papers in leading conferences.

The first paper explores a new attack made possible by the connection of the telephony network and the Internet. The second one explores new methods for detection attacks on software. The last one is a study that maps the newly emerging network of short URLs.

- Alexandros Kapravelos, Iasonas Polakis, Elias Athanasopoulos, Sotiris Ioannidis, Evangelos P. Markatos. **D(e)i**aling with VoIP: Robust Prevention of DIAL Attacks. In Proceedings of the *15th European Symposium on Research in Computer Security (ESORICS)*. Athens, Greece, September 2010.
- Michalis Polychronakis, Kostas G. Anagnostakis and Evangelos P. Markatos. **Comprehensive Shellcode Detection using Runtime Heuristics**. In Proceedings of the *26th Annual Computer Security Applications Conference (ACSAC)*. December 2010, Austin, TX, USA. [pdf](#) (323.7 KB)
- Demetris Antoniadis, Iasonas Polakis, Georgios Kontaxis, Elias Athanasopoulos, Sotiris Ioannidis, Evangelos P. Markatos, Thomas Karagiannis. **we.b: The Web of Short URLs**. In Proceedings of the *20th International World Wide Web Conference (WWW)*. March 2011, Hyderabad, India.

During the first year, we also did a comprehensive survey of all top systems security conferences categorizing research done in cyberattacks. Our results were presented in deliverable D7.1.

2.2.6.3. Deviations from Annex I and their impact (if any)

N/A

2.2.6.4. Failure to achieve critical objectives or not being on schedule (if applicable)

N/A

2.2.6.5. Use of resources

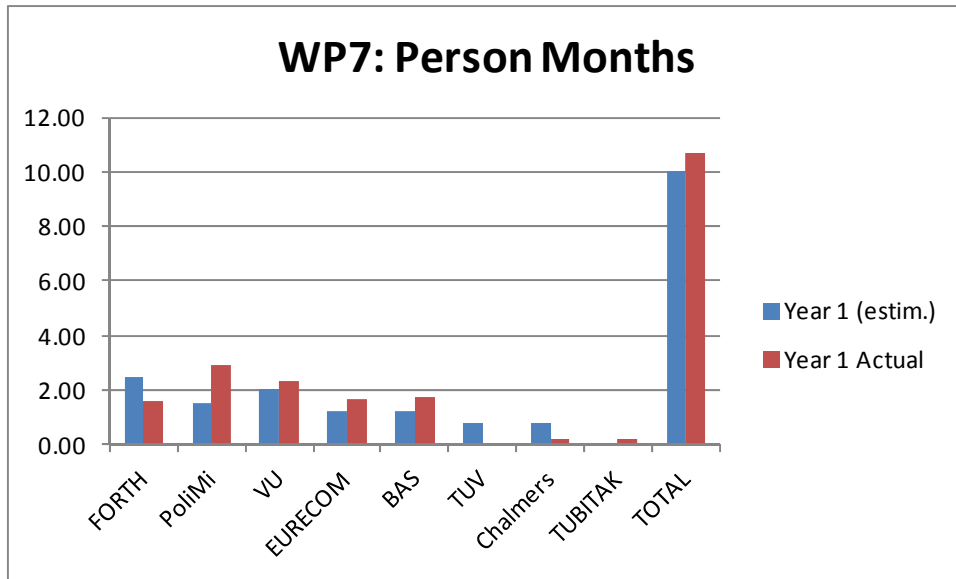


Figure 10: Person months charged in WP7

2.2.6.6. Corrective Actions (if applicable)

N/A

2.2.6.7. Evaluation Criteria

Name	Target Value	Achieved Value
Number of papers published in leading conferences	2 (per year)	3 ²³
Types of lightweight devices being protected by new defense mechanisms	3 (total)	1 ²⁴
Tools that protect clients against server-originating attacks	2 (total)	N/A

²³ As explained in section 2.2.6.2

²⁴ We worked on developing packet-capturing application for Android smartphones, as well as understanding the platform, the capabilities and power requirements. In this context we are evaluating the cost-benefit tradeoff with respect to running more heavy-weight security software on the Android platform versus the energy requirements of such an approach.

2.3. Project Management during the period

2.3.1. Consortium Management Tasks and achievements

During the reporting period, we successfully completed several management tasks including:

- **Consortium agreement:** We drafted and signed a consortium agreement which deals with various issues of the project, including IPR.
- **Meetings:** We held four periodic project plenary meetings, one General Assembly meeting, and one Working Group meeting. The meetings were organized around an agenda circulated well in advance to all partners. During these meetings we discussed the progress of the tasks and scheduled the future work. After the meetings, the coordinator circulated the minutes containing the action points to all partners.
- **Collaborative Environment:** we operate on a 24/7 basis a collaborative repository based on SVN. Using this repository, partners can share documents and ideas. We also operate a mailing list for the project and individual mailing lists for the committees.
- **First SysSec workshop infrastructure.** We installed and operated HotCRP, a conference management software which handled the submission, evaluation, and acceptance of papers submitted to the First SysSec Workshop.
- **Committees.** We manned and started the operation of all project committees and bodies as mentioned in the proposal and subsequent contract. The meetings and attendance lists for these meetings can be found in the project's SVN.
- **Reporting.** Prepared reporting templates for the partners to document their work, their person months and their expenses. The templates have to be filled twice per year.
- **Bimonthly Reports.** Prepared (in collaboration with PoliMi and the rest of the partners) bimonthly dissemination reports, submitted on time to the project officer.
- **Liaison:** The coordinator acted as a liaison between the partners and the commission conveying several questions as well as their replies.
- **Change of (names of) partners.** Handled all the necessary work associated with the change in names (and PIC number) for two of the partners: TUBITAK, and IICT-BAS (see section 2.3.3.).



2.3.2. Problems which have occurred

During this period we did not encounter any problems. We encountered some unexpected events, such as name (and PIC number) changes, but there were handled smoothly.

2.3.3. Changes in the consortium, if any

During the reporting period we had the following changes in the consortium:

- IPP-BAS changed their name to IICT-BAS and their PIC number as well. IICT-BAS will undertake all obligations of IPP BAS;


- TUBITAK UEKAE changed their name to TUBITAK BILGEM. BILGEM will undertake all obligations of UEKAE.

After discussions within the consortium and with the project officer, we concluded that no amendment is needed. The relevant information letters were sent by the Commission.

2.3.4. List of project meetings, dates and venues

During the reporting period we had the following project meetings:

Name	Place	Date	
Kick off project meeting	Heraklion	3/9/2010	
Second plenary project meeting	Milan	1/12/2010	
First GA (General Assembly) Project meeting	Milan	1/12/2010 (collocated with the Second plenary project meeting)	
Third plenary project meeting	Amsterdam	22/2/2011	
Meeting of the SysSec Working Groups	Amsterdam	23/2/2011 (collocated with the third plenary project meeting)	
Fourth plenary project meeting	Vienna	2/6/2011	
First SysSec workshop	Amsterdam	6/7/2011 (collocated with the DIMVA conference)	

First IAB (Industrial Advisory Board) meeting	Amsterdam	5/7/2011 (collocated with the First SysSec workshop)	
---	-----------	--	--

During this first year of the project, we made every effort to reduce the number of trips by collocating meetings as much as possible. Thus, we managed to hold 8 meetings with only 5 trips.

2.3.5. Project Planning and status

2.3.5.1. Project status

The project successfully completed its first year. During this time, the project managed to achieve its objectives as can be seen by the produced results:

- It created a community of more than 200 researchers in the area
- About half of them contributed to the First SysSec workshop
- It created a Research Roadmap containing contributions from tens of people

2.3.5.2. Project Planning

Over the next few years we expect to continue our research and community building activities and start our education activities as well.

2.3.6. Impact of possible deviations from the planned milestones and deliverables, if any

There were not any significant deviations from the planned milestones and deliverables.

There were however, the following changes:

- FORTH's overhead has been reduced from 101% to 95%. This will reduce FORTH's budget and requested funding. We plan to use these extra funds made available due to the smaller overhead in order to pay for the travel costs for some of the concertation meetings in which FORTH participates. For example, during the first year of SysSec's project FORTH participated in 4-5 meetings organized by the EffectsPlus project²⁵. Unfortunately, no budget was originally envisioned in the SysSec Technical Annex for the participation in EffectsPlus meetings. We take this opportunity and plan to use the funds released by the smaller FORTH's overhead to pay for the travel costs for some of these concertation meetings.
- PoliMi has a budget of 60 Keuros for the travel of the members of the Industrial advisory board and of the associated partners: 1Keuros per trip x 1 trip per year x 4 years x (8 members of the IAB + 7 associated partner) = 60 Keuros (section B.2.4.2 of the DoW). We decided that our Industrial Advisory Board will be more flexible with 7 (rather than 8)

²⁵ Effectsplus is a FP7 funded Coordination & Support Action, across a large spectrum of R&D activity in the ICT Framework Programme that relates to the twin requirements of trust and security, and their constituent concepts and components.

members, and thus we would need 56 (instead of 60) Keuros for the travel budget. We propose to use these 4 Keuros to pay for dissemination expenses such as the publication of the proceedings of the SysSec workshops. Btw, in case a member of the IAB or an associated partner would not be able to attend these meetings, we are thinking of inviting external experts, who will be able to provide feedback to the project.

2.3.7. Changes to the legal status of any of the beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs;

There were no changes in the legal status of any of the beneficiaries. There were, however, the following changes:

- IPP-BAS changed name and PIC number. Their new name is IICT-BAS and their new PIC number is 973354455
- TUBITAK UEKAE changed their name and PIC number. Their new name is TUBITAK BILGEM and their new PIC number is 999587135

2.3.8. Development of the Project website, if applicable;



The project's web site was completed during the first month of the project.

Actually, the web site was an official deliverable of the project (D2.1) which was delivered on-time – at the end of M2. The web site consists of a public section and a private section (accessible only by the partners). The public sections of the SysSec website aim to (i) provide information about the project and its goals, (ii) make public the results produced by the project, such as papers, organized events, talks etc., and (iii) help interested parties to get in touch with the SysSec consortium and community. The main parts of the



public section are: Home, partners, publications, and publicity. To capitalize on the recent proliferation of social networks, we have added a social toolbar at the bottom of each page on the SysSec website which allows visitors to easily share the content with their social network contacts.

2.3.9. Evaluation Criteria

Name	Target Value	Achieved Value
Times each Deliverable is downloaded	50 times (after a year of publication)	As shown in table Table 1 in page 32
Internal Project Committees activated	All (by the end of the first month)	All (by the end of the first month)

Deliverable	Delivered	Times Downloaded until 31/8/2011
D2.1: Web Site	November 2010	100
D2.3: 1 st Project Workshop Proceedings	August 2011	48
D3.1: Framework for Researcher exchanges	February 2011	64
D5.1: Survey of Research and Data Collection Initiatives in Malware and Fraud	June 2011	74
D7.1: Review of the State-of-the-Art in Cyberattacks	June 2011	170

Table 1: Number of times each deliverable was downloaded

2.3.10. Person Months

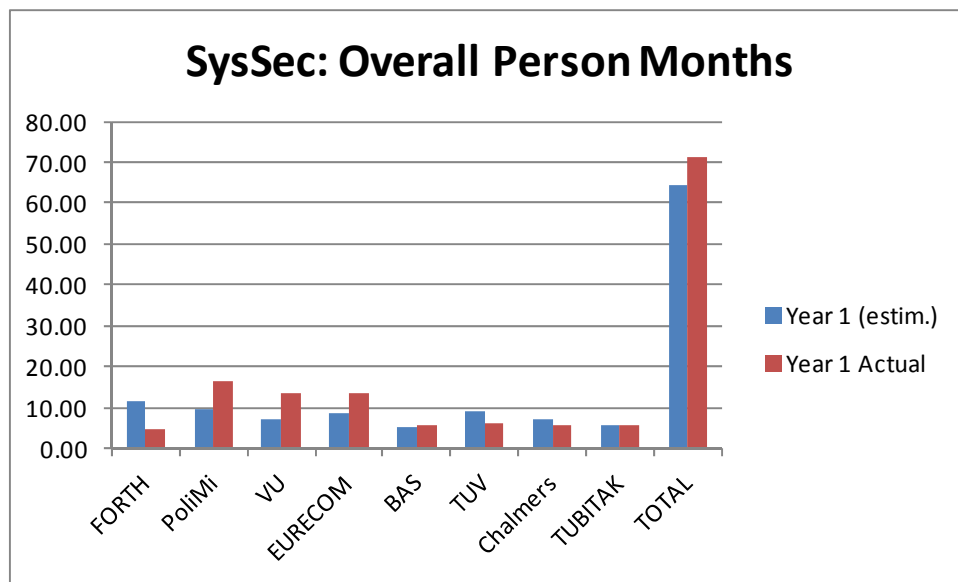


Figure 11: Overall person Months charged in the project.

Figure 11 shows the number of person months charged to the project. We see that the total number of person months charged (Year 1 Actual) is somewhat less (about 10%) than originally envisioned (Year 1 (estim.)). This is mostly pronounced in FORTH and to some extent in some of the other partners as well. This major difference for FORTH is due to the fact that FORTH was able to invest a significant amount of effort that was not charged in the project. Indeed, during the first semester

of 2011, the project manager was relieved from his teaching duties at the University of Crete and thus was able to dedicate a significant amount of his time to SysSec without, however, charging it to SysSec.

2.4. Deliverables and milestones tables

2.4.1. Deliverables

The following table presents the deliverables due in this reporting period²⁶. We see that all deliverables has been delivered.

TABLE 1. DELIVERABLES											
Del. no.	Deliverable name	Version	WP no.	Lead beneficiary	Nature	Dissemination level ²⁷	Delivery date from Annex I (proj month)	Actual / Forecast delivery date Dd/mm/yyyy	Status No submitted/ Submitted	Contractual Yes/No	Comments
D2.1	Web Site		WP2	FORTH	Report + web site	PU	M2	M3	Submitted	Yes	-
D3.1	Framework for Researcher exchanges		WP3	VU	Report	PU	M6	M6	Submitted	Yes	-
D5.1	Survey of Research and Data Collection Initiatives in Malware and Fraud		WP5	TUV	Report	PU	M9	M10	Submitted	Yes	

²⁶ The table is cumulative. It shows all deliverables from the beginning of the project.

²⁷

PU = Public

PP = Restricted to other programme participants (including the Commission Services).

RE = Restricted to a group specified by the consortium (including the Commission Services).

CO = Confidential, only for members of the consortium (including the Commission Services).

Make sure that you are using the correct following label when your project has classified deliverables.

EU restricted = Classified with the mention of the classification level restricted "EU Restricted"

EU confidential = Classified with the mention of the classification level confidential " EU Confidential "

EU secret = Classified with the mention of the classification level secret "EU Secret "

D7.1	Review of the State of the Art in Cyberattacks		WP7	FORTH	Report	PU	M9	M10	Submitted	Yes	
D4.1	First Report on Threats on the Future Internet and Research Roadmap		WP4	EURECOM	Report	PU	M12	M13	Submitted	Yes	
D6.1	Report on the State of the Art in Security in Sensor Networks		WP6	Chalmers	Report	PU	M12	M12	Submitted	Yes	
D2.3	First Project Workshop Proceedings		WP2	PoliMi	Report	PU	M12	M12	Submitted	Yes	
D2.5	First Periodic Dissemination Report		WP2	PoliMi	Report	PU	M12	M14	Submitted	Yes	
D1.1	First Periodic Progress Report		WP1	FORTH	Report	PU	M12	M14	Submitted	Yes	

2.5. Financial statements – Form C and summary financial Report

2.5.1. Milestones

TABLE 2. MILESTONES							
Milestone no.	Milestone name	Work package no	Lead beneficiary	Delivery date from Annex I dd/mm/yyyy	Achieved Yes/No	Actual / Forecast achievement date dd/mm/yyyy	Comments
MS1	Research Roadmap	WP4	EURECOM	31/8/2011	Yes	31/8/2011	A draft version was ready well in advance

2.5.2. Person Month Status Table

WorkPackage	WP1		WP2		WP3		WP4		WP5		WP6		WP7		TOTAL per Beneficiary	
	Actual WP total	Planned WP total	Actual WP total	Planned WP total	Actual WP total	Planned WP total	Actual WP total	Planned WP total	Actual WP total	Planned WP total	Actual WP total	Planned WP total	Actual WP total	Planned WP total	Actual WP total	Planned WP total
Coordinator	2.20	4.00	0.00	1.00	0.00	0.58	0.75	1.75	0.21	0.50	0.00	1.00	1.56	2.50	4.72	11.33
PoliMi	0.52	0.52	2.53	3.00	2.15	0.33	2.63	1.00	2.76	2.00	2.90	1.50	2.92	1.50	16.41	9.85
VU	0.51	0.51	0.82	0.50	5.58	0.92	2.62	1.50	0.23	0.50	1.68	1.25	2.33	2.00	13.77	7.18
EURECOM	0.39	0.39	1.29	0.75	1.53	0.33	3.54	2.75	4.42	2.50	0.47	0.75	1.69	1.25	13.33	8.72
BAS	0.17	0.17	1.52	1.00	0.00	0.25	1.14	1.25	0.73	0.50	0.33	0.75	1.77	1.25	5.66	5.17
TUV	0.28	0.28	0.11	0.50	0.17	0.42	1.21	2.25	4.27	4.25	0.00	0.50	0.00	0.75	6.04	8.95
Chalmers	0.20	0.20	0.40	0.50	0.50	0.50	0.70	1.00	0.00	0.00	3.60	4.25	0.20	0.75	5.60	7.20
TUBITAK	0.88	0.88	0.06	0.50	0.06	0.00	0.12	2.13	4.37	2.25	0.00	0.00	0.23	0.00	5.72	5.76

2.6. Explanation of the use of the resources

Table 6.3 Personnel, subcontracting and other major Direct cost items and Indirect costs for beneficiary FORTH for this reporting period			
Work Package	Item description	Amount (€)	Explanation
WP4-7	Personnel (RTD activity)	7.670,52	Salaries of researchers and engineers for RTD activities
WP2,3	Personnel (Other activity)	0,0	-
WP1	Personnel (Management activity)	4.335,85	Salaries of researchers and engineers for management activities.
WP all	Travel and meeting costs	24.174,65	<p><u>Travel for project result presentations(name, place, dates, etc)</u></p> <ul style="list-style-type: none"> • Evangelos Markatos/Patra/10.12.2010, Presentation to the University of Patras titled "Managing Threats and Vulnerabilities in the Future Internet". • Georgios Kontaxis/Berlin/27.10-30.10.2010, Paper presentation in the EC2ND 2010 Conference. • Evangelos Markatos/Brussels/26.09-29.09.2010, Participation in the ICT 2010 Conference. • Sotirios Ioannidis/Berlin/27.10-30.10.2010, Participation in the EC2ND 2010 Conference and in the Panel Machine Learning of Computer Security:Blessing or Curse? • Sotirios Ioannidis/Milan/29.11-03.12.2010, SysSec project meeting. • Evangelos Markatos/Milan/29.11-03.12.2010, SysSec project meeting. • Evangelos Markatos/Brussels/14.12-17.12.2010, Participation in the Future Internet Assembly. • Evangelos Markatos/Brussels/31.01-02.02.2010, Representation of the SysSec project to the EffectPlus open communications event. • Sotirios Ioannidis/Amsterdam/21.02-24.02.2011, SysSec project meeting. • Evangelos Markatos/Amsterdam/20.02-26.02.2011, Participation in the Plenary meeting and in working group meetings of the SysSec project. • Evangelos Markatos/Brussels/28.3-31.03.2011, Representation of the SysSec project to the EffectPlus 1st kick off technical cluster meeting. • Georgios Kontaxis/Austria/09.04-14.04.2011, Paper presentation and participation in the EuroSys 2011 and Eurosec 2011 conference. • Iason Polakis/Vienna/26.04-28.04.2011, Paper presentation in the 3rd COST TMA Conference.

			<ul style="list-style-type: none"> • Evangelos Markatos/Vienna/01.06-03.06.2011, SysSec Project meeting. • Sotiris Ioannidis/Vienna/01.06-03.06.2011, SysSec Project meeting. • Sotiris Ioannidis/Amsterdam/04.07-07.07.2011, Participation in the SysSec Workshop and Industrial Advisory Board meeting. • Evangelos Markatos/Amsterdam/02.07-09.07.2011, Representaion of the SysSec project to the 2nd EffectsPlus clustering event, Participation in the SysSec workshop and in the DIMVA Conference 2011. • Iason Polakis/Chicago/03.10-09.10.2010, Paper presentation and participation in the WPES 2010 conference and CCS 2010. • Moulakakis/Heraklion/Kick off meeting/09.09.2010.
WP all	Lab consumables	0,00	
WP all	Any other direct cost category	4000,00	External Researcher
TOTAL DIRECT COSTS		40.181,02	Total of above
	Indirect Costs of the 1st reporting period	11.406,05	Indirect costs of the 1 st reporting period
TOTAL COSTS		51.587,07	Equal to costs reported in from C

Table 6.3 Personnel, subcontracting and other major Direct cost items and Indirect costs for beneficiary POLIMI for this reporting period			
Work Package	Item description	Amount (€)	Explanation
WP4-7	Personnel (RTD activity)	24.817,00	Salaries of 1 Full professor, 1 Researcher, 2 Term Researcher for a total of 12.59 MM
WP2,3	Personnel (Other activity)	13.034,00	Salaries of 1 Full professor, 1 Researcher, 1 Term Researcher for a total of 2.46 MM
WP1	Personnel (Management activity)	2,033,00	Salaries of 1 Researcher for a total of 0.63 MM
WPall	Travel and meeting costs	8.561.00	<p>Travel for project result presentations(name, place, dates, etc)</p> <ul style="list-style-type: none"> • Kick-off mtg/Heraklion/02-5.09.2010 Prof. Stefano Zanero • Kick-off mtg/Heraklion/02-5.09.2010 Dr. Federico Maggi • Trip to Rome and Berling, 27-29/10/2010, Prof. Stefano Zanero to speak at a security event and to co-chair the EC2ND conference and take part in a SysSec panel • Ghent (Belgium), 15-16/12/2010 Mr. Federico Maggi to represent the project at FIA • Amsterdam (Netherlands), 22-23/02/2011 Prof. Stefano Zanero for project meeting • London (UK) and Vienna (Austria) : 31/05-04/06/2011 Prof. Stefano Zanero took part in worldwide cybersecurity summit and then to project meeting • Crete, 29/06-01/07/2011, Dr. Federico Maggi took part in ENISA summer school • Amsterdam, 06-08/07/2011 Prof. Stefano Zanero and Dr. Federico Maggi took part in project workshop and meeting, and in the DIMVA conference
WP5	Lab consumables	647,00	Software
WP1	Any other direct cost category	1.135,00	Catering and work dinner meeting for project meeting, 01/12/2010
TOTAL DIRECT COSTS		50.227,00	Total of above
	Indirect Costs of the 1st reporting period	20.779,00	Indirect costs of the 1 st reporting period
TOTAL COSTS		71.006,00	Equal to costs reported in form C

Table 6.3 Personnel, subcontracting and other major Direct cost items and Indirect costs for beneficiary VUA for this reporting period			
Work Package	Item description	Amount (€)	Explanation
WP all	Personnel (RTD activity)	32.762,88	Salary of A. Bacs MSc (12 PM)
WP1	Personnel (Mngt)	7.668,96	Salary of dr. ir. H.J. Bos (1,1 PM)
WP all	Travel and meeting costs	9.433,25	<u>Travel for project result presentations(name, place, dates, etc)</u> <ul style="list-style-type: none"> • Bos;Heraklion;02/09/2010;Syssec project meeting • Bos;Vancouver;2-7/10/2010;OSDI 2010 • Slowinska, J.M.; San diego; 5-19 feb'11 • Bos;Salzburg;Eurosys wrkshp;09/04/2011 • Bos;Austria;Meeting Syssec; 1/6/11 • Bos; Amsterdam;Syssec meeting; 22/02/2011 • Cavallaro L;Salzburg;09/13.04.11;conf.
WPall	Equipment	374,56	Computer
WP2-3	Other	1.800,--	Scholarship for students
WP1	Any other direct cost category	80,--	Publication costs
TOTAL DIRECT COSTS		52.119,65	Total of above
	Indirect Costs of the 1st reporting period	104.248,50	Indirect costs of the 1 st reporting period
TOTAL COSTS		156.368,15	Equal to costs reported in from C

Table 6.3 Personnel, subcontracting and other major Direct cost items and Indirect costs for beneficiary EURECOM for this reporting period			
Work Package	Item description	Amount (€)	Explanation
WP4-7	Personnel (RTD activity)	45,505.84	10.13MM Leading the workgroups and preparing the research roadmap (WP4) and contributing with several papers to the research in malware analysis and cyberattacks.
WP2,3	Personnel (Other activity)	10,001.64	2.81MM For dissemination activities and the participation in the definition of the current curriculum
WP1	Personnel (Management activity)	2,058.55	0.38MM For participating to the management meetings and taking care of the defined action points.
WPall	Travel and meeting costs	17,889.72	<u>Travel for project result presentations(name, place, dates, etc)</u> <ul style="list-style-type: none"> • Kick-off mtg/Heraklion/02-5.09.2010 • Project mtg/Milan/29.11-03.12.2010 • NDSS Conf + UCSB mtg/SanDiego/05-12.02.2011 • Workshop/Amsterdam/22-23.02.211 • Financial Crypto Conf./Sainte-Lucia/26.02-06.03.2011 • Paper Presentation WWW Conf/Hyderabad/28.03-01.04.2011 • Paper at EUROSEC Workshop/Salsburg/09-11.04.2011 • Talk to Swiss Cyber Storm/Zurich/11-15.05.2011 • Security & Privacy Conf + RAID mtg Oakland/22-27.05.2011 • OWASP AppSec Eur Conf/Dublin/08-11.06.2011 • Workshop + DIMVA/Amsterdam/05-06.07.2011 • Paper at OWASP NL + DIMVA/Amsterdam/06-08.07.2011
WPall	Lab consumables	0.00	Short description
WPall	Any other direct cost category	0.00	<u>Short description</u>
TOTAL DIRECT COSTS		75,455.75	Total of above
	Indirect Costs of the 1st reporting period	35,414.91	Indirect costs of the 1 st reporting period
TOTAL COSTS		110,870.66	Equal to costs reported in form C

Table 6.3 Personnel, subcontracting and other major Direct cost items and Indirect costs for beneficiary ICT for this reporting period			
Work Package	Item description	Amount (€)	Explanation
WP4-7	Personnel (RTD activity)	11,089.49	Salaries of researchers and engineers for RTD activities
WP2,3	Personnel (Other activity)	4,245.85	Salaries of researchers and engineers for dissemination activities
WP1	Personnel (Management activity)	474.86	Salaries of researchers and engineers for management activities
WP all	Travel and meeting costs	6,499.67	Travel for project result presentations(name, place, dates, etc) <ul style="list-style-type: none"> • Zlatogor Minchev /Heraklion/02.09-04.09.2010 • Zlatogor Minchev, Vladimir Dimitrov /Milano/30.11-02.12.2010 • Zlatogor Minchev, Vladimir Dimitrov, Edita Djambazova /Amsterdam/21.02-24.02.2011 • Zlatogor Minchev, Vladimir Dimitrov /Vienna/29.09-30.09.2010 • Zlatogor Minchev, Vladimir Dimitrov, Toni Atanasov /Amsterdam/04.07-06.07.2011
WPall	Lab consumables	24.80	Memory module
WPall	Any other direct cost category	125.65	Courier services and bank taxes
TOTAL DIRECT COSTS		22,460.31	Total of above
	Indirect Costs of the 1st reporting period	13,476.19	Indirect costs of the 1 st reporting period
TOTAL COSTS		35,936.50	Equal to costs reported in from C

Table 6.3 Personnel, subcontracting and other major Direct cost items and Indirect costs for beneficiary TUWIEN for this reporting period			
Work Package	Item description	Amount (€)	Explanation
WP4-7	Personnel (RTD activity)	21667,31	5,47 Man months in total. Personnel costs for Martina Lindorfer, Paolo Milani and Martin Jauernig leading to Deliverable 5.1
WP2,3	Personnel (Other activity)	1310,12	0,28 Man months for dissemination activities and establishing a common curriculum
WP1	Personnel (Management activity)	1310,12	0.28 Man months For participating to the management meetings and taking care of the defined action points.
WPall	Travel and meeting costs	3312,05	<u>Travel for project result presentations(name, place, dates, etc)</u> <ul style="list-style-type: none"> • Kick-off mtg/Heraklion/02-5.09.2010 • Project mtg/Milan/29.11-03.12.2010 • Workshop/Amsterdam/22-23.02.211 • DIMVA Program Committee Meeting/Bochum/24-25.03.2011 • Workshop + DIMVA/Amsterdam/05-06.07.2011
WPall	Lab consumables	0.00	Short description
WPall	Any other direct cost category	0.00	<u>Short description</u>
TOTAL DIRECT COSTS		27599,60	Total of above
	Indirect Costs of the 1st reporting period	16559,76	Indirect costs of the 1 st reporting period
TOTAL COSTS		44159,36	Equal to costs reported in form C

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 7, CHALMERS FOR THE PERIOD			
Work Package	Item description	Amount in €	Explanations
All	Personnel direct costs	44 470	5.6 PMs
			Salaries for two senior researchers, one post-doc and
			one Ph D student
All	Travel costs	8 903	Travel costs for various project meetings, such as: Kick-off meeting, Crete, Sep 02-06, 2010 Project meeting, Nice, Sep 08-11, 2010 Project meeting Milan, Nov 30-Dec 02, 2011 Expert group meeting Amsterdam Feb 21-24, 2011 Project meeting Vienna, Jun 01-04 2011 Workshop Amsterdam, Jul 04-07, 2011
All	Other direct costs	64	
	Indirect costs	10 687	
TOTAL COSTS		64 124	

Table 6.3 Personnel, subcontracting and other major Direct cost items and Indirect costs for beneficiary TUBITAK for this reporting period			
Work Package	Item description	Amount (€)	Explanation
WP4-7	Personnel (RTD activity)	13219	Salaries of researchers and engineers for malware and botnet detection mechanisms (RTD activities)
WP2,3	Personnel (Other activity)	345	Salaries of researchers and engineers for integration with dissemination and educational seminar applications
WP1	Personnel (Management activity)	1392	Salaries of researchers and engineers for integration with management applications
WP all	Travel and meeting costs	3255	<ul style="list-style-type: none"> • 1st SysSec plenary Meeting/Heraklion/03-09-2010 • 2nd SysSec plenary Meeting/Milano/01-12-2010 • 3rd SysSec plenary Meeting/Amsterdam/22-02-2011 • 4th SysSec plenary Meeting/Vienna/02-06-2011 • 5th SysSec plenary Meeting/Gothenburg/08-09-2011
WPall	Lab consumables	0	N/A
WPall	Any other direct cost category	0	N/A
TOTAL DIRECT COSTS		18211	Total of above
	Indirect Costs of the 1st reporting period	10926	Indirect costs of the 1 st reporting period
TOTAL COSTS		29137	Equal to costs reported in from C

2.7. Financial statements – Form C and Summary financial report

All FORMS C can be found in the NEF on-line system.

IMPORTANT:

Form C varies with the funding scheme used. Please make sure that you use the correct form corresponding to your project (Templates for Form C are provided in Annex VI to the Grant Agreement). An example for collaborative projects is enclosed hereafter.

A Web-based online tool for completing and submitting forms C is accessible via the Participant Portal: <http://ec.europa.eu/research/participants/portal>, (except for projects managed by DG MOVE and ENER).

If some beneficiaries in security research have two different rates of funding (part of the funding may reach 75%²⁸) then two separate financial statements should be filled by the concerned beneficiaries and two lines should be entered for these beneficiaries in the summary financial report.

²⁸ Article 33.1 of the EC FP7 rules for participation - REGULATION (EC) No 1906/2006.

FP7 - Grant Agreement - Annex VI - Collaborative Project

Form C - Financial Statement (to be filled in by each beneficiary)			
Project nr	nnnnnn	Funding scheme	Collaborative Project
Project Acronym	xxxxxxxxxxxxxxxxxxxxxx		
Period from	dd/mm/aa	Is this an adjustment to a previous statement ?	Yes/No
To	dd/mm/aa		
Legal Name		Participant Identity Code	nn
Organisation short Name		Beneficiary nr	nn
Funding % for RTD activities (A)		If flat rate for indirect costs, specify %	%

1- Declaration of eligible costs/lump sum/flat-rate/scale of unit (in €)

	Type of Activity				TOTAL (A+B+C+D)
	RTD (A)	Demonstration (B)	Management (C)	Other (D)	
Personnel costs					
Subcontracting					
Other direct costs					
Indirect costs					
Lump sums/flat-rate/scale of unit declared					
Total					
Maximum EC contribution					
Requested EC contribution					

2- Declaration of receipts

Did you receive any financial transfers or contributions in kind, free of charge from third parties or did the project generate any income which could be considered a receipt according to Art.II.17 of the grant agreement ?
If yes, please mention the amount (in €)

Yes/No

3- Declaration of interest yielded by the pre-financing (to be completed only by the coordinator)

Did the pre-financing you received generate any interest according to Art. II.19 ?
If yes, please mention the amount (in €)

Yes/No

4. Certificate on the methodology

Do you declare average personnel costs according to Art. II.14.1 ?

Yes/No

Is there a certificate on the methodology provided by an independent auditor and accepted by the Commission according to Art. II.4.4 ?

Yes/No

Name of the auditor		Cost of the certificate (in €), if charged under this project	
----------------------------	--	--	--

5- Certificate on the financial statements

Is there a certificate on the financial statements provided by an independent auditor attached to this financial statement according to Art.II.4.4 ?

Yes/No

Name of the auditor		Cost of the certificate (in €)	
----------------------------	--	---------------------------------------	--

6- Beneficiary's declaration on its honour

We declare on our honour that:

- the costs declared above are directly related to the resources used to attain the objectives of the project and fall within the definition of eligible costs specified in Articles II.14 and II.15 of the grant agreement, and, if relevant, Annex III and Article 7 (special clauses) of the grant agreement;
- the receipts declared above are the only financial transfers or contributions in kind, free of charge, from third parties and the only income generated by the project which could be considered as receipts according to Art. II.17 of the grant agreement;
- the interest declared above is the only interest yielded by the pre-financing which falls within the definition of Art. II.19 of the grant agreement ;
- there is full supporting documentation to justify the information hereby declared. It will be made available at the request of the Commission and in the event of an audit by the Commission and/or by the Court of Auditors and/or their authorised representatives.

Beneficiary's Stamp	Name of the Person(s) Authorised to sign this Financial Statement
	Date & signature

FP7 - Grant Agreement - Annex VI - Collaborative Project

Form C - Financial Statement (to be filled in by Third Party) Only applicable if special clause nr 10 is used			
Project nr	nnnnnn	Funding scheme	Collaborative Project
Project Acronym	xxxxxxxxxxxxxxxxxxxxxx		
Period from	dd/mm/aa	Is this an adjustment to a previous statement ?	Yes/No
To	dd/mm/aa		
3rd party legal Name			
3rd party Organisation short Name		Working for beneficiary nr	nn
Funding % for RTD activities (A)		If flat rate for indirect costs, specify %	%

1- Declaration of eligible costs/lump sum/flat-rate/scale of unit (in €)

	Type of Activity				TOTAL (A+B+C+D)
	RTD (A)	Demonstration (B)	Management (C)	Other (D)	
Personnel costs					
Subcontracting					
Other direct costs					
Indirect costs					
Lump sums/flat-rate/scale of unit declared					
Total					
Maximum EC contribution					
Requested EC contribution					

2- Declaration of receipts

Did you receive any financial transfers or contributions in kind, free of charge from third parties or did the project generate any income which could be considered a receipt according to Art.II.17 of the grant agreement ? Yes/No

If yes, please mention the amount (in €) _____

3- Declaration of interest yielded by the pre-financing (to be completed only by the coordinator)

Did the pre-financing you received generate any interest according to Art. II.19 ? Yes/No

If yes, please mention the amount (in €) _____

4. Certificate on the methodology

Do you declare average personnel costs according to Art. II.14.1 ? Yes/No

Is there a certificate on the methodology provided by an independent auditor and accepted by the Commission according to Art. II.4.4 ? Yes/No

Name of the auditor		Cost of the certificate (in €), if charged under this project	
----------------------------	--	--	--

5- Certificate on the financial statements

Is there a certificate on the financial statements provided by an independent auditor attached to this financial statement according to Art.II.4.4 ? Yes/No

Name of the auditor		Cost of the certificate (in €)	
----------------------------	--	---------------------------------------	--

6- Beneficiary's declaration on its honour

We declare on our honour that:

- the costs declared above are directly related to the resources used to attain the objectives of the project and fall within the definition of eligible costs specified in Articles II.14 and II.15 of the grant agreement, and, if relevant, Annex III and Article 7 (special clauses) of the grant agreement;
- the receipts declared above are the only financial transfers or contributions in kind, free of charge, from third parties and the only income generated by the project which could be considered as receipts according to Art. II.17 of the grant agreement;
- the interest declared above is the only interest yielded by the pre-financing which falls within the definition of Art. II.19 of the grant agreement ;
- there is full supporting documentation to justify the information hereby declared. It will be made available at the request of the Commission and in the event of an audit by the Commission and/or by the Court of Auditors and/or their authorised representatives.

Beneficiary's Stamp	Name of the Person(s) Authorised to sign this Financial Statement
	Date & signature

FP7 - Grant Agreement - Annex VI - Collaborative Project

Summary Financial Report - Collaborative Project- to be filled in by the coordinator

Project acronym	xxxxxxxxxxxxxxxxxxxxxxxxxxxx	Project nr	nnnnnn	Reporting period from	dd/mm/aa	to:	dd/mm/aa	Page	1/1
-----------------	------------------------------	------------	--------	-----------------------	----------	-----	----------	------	-----

Funding scheme		CP	Type of activity								Total (A)+(B)+(C)+(D)		Receipts	Interest	
Beneficiary n°	If 3rd Party, linked to beneficiary	Adjustment (Yes/No)	Organisation Short Name	RTD (A)		Demonstration (B)		Management (C)		Other (D)					
				Total	Max EC Contribution	Total	Max EC Contribution	Total	Max EC Contribution	Total	Max EC Contribution	Total	Max EC Contribution		
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
TOTAL															

Requested EC contribution for the reporting period (in €)

