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*

3rd Periodic Dissemination Report [†]

September 2012–August 2013

Abstract: This is the dissemination report for SysSec for the period September 2012–August 2013.

Contractual Date of Delivery	August 2013
Actual Date of Delivery	September 2013
Document Dissemination Level	Public
Editor	Stefano Zanero
Contributors	Manolis Stamatogiannakis

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 n° 257007.

1 Executive Summary

This report summarizes the dissemination activities carried out by the *SysSec* project in the September 2012–August 2013 period. Specifically, in the following pages we will list the papers presented by the consortium in conferences as well as the presentations related to the project made at various events and forums. Any additional coverage of the project by the press and online media is also presented in this document.

During this third year of *SysSec* the consortium published a total of 21 peer-reviewed papers, plus 23 presentations, talks and seminars.

Moreover, we organized an international school, a workshop, we interacted with the international press, and with other EU funded projects.

The overall dissemination output of *SysSec* is an indication of the global excellence and recognition of the project partners.

2 Conference and journal papers

Following is the list of peer-reviewed papers that were presented or published in the period September 2012–August 2013.

[1] Georgios Kontaxis, Michalis Polychronakis, and Evangelos P. Markatos. **Minimizing information disclosure to third parties in social login platforms**. *International Journal of Information Security*, 11:321–332, October 2012.

Local copy: papers/sudoweb-ijis12.pdf

Online: http://syssec-project.eu/nNa#sudoweb-ijis12.pdf

[2] Zlatogor Minchev. **Social Networks Security Aspects: A Technological and User Based Perspectives**. In *Proceedings of the 20th National Jubilee Conference with International Participation (TELECOM)*, Sofia, Bulgaria, October 2012.

Local copy: papers/zm-telecom12.pdf

Online: http://syssec-project.eu/nNa#zm-telecom12.pdf

[3] Zhang Fu and Marina Papatriantafilou. **Off The Wall: Lightweight Distributed Filtering to Mitigate Distributed Denial of Service Attacks**. In *Proceedings of the 31st IEEE International Symposium on Reliable Distributed Systems (SRDS)*, Irvine, CA, USA, October 2012.

Local copy: papers/fu-srds12.pdf

Online: http://syssec-project.eu/nNa#fu-srds12.pdf

[4] Markus Kammerstetter, Christian Platzer, and Gilbert Wondracek. **Vanity, Cracks and Malware: Insights into the Anti-Copy Protection**

Ecosystem. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS)*, Raleigh, NC, USA, October 2012.

Local copy: papers/kammerstetter-ccs12.pdf

Online: http://syssec-project.eu/nNa#kammerstetter-ccs12.pdf

[5] Iasonas Polakis, Marco Lancini, Georgios Kontaxis, Federico Maggi, Sotiris Ioannidis, Angelos D. Keromytis, and Stefano Zanero. **All your face are belong to us: Breaking Facebook's Social Authentication**. In *Proceedings of the 2012 Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

Local copy: papers/polakis-acsac12.pdf

Online: http://syssec-project.eu/nNa#polakis-acsac12.pdf

[6] Martina Lindorfer, Alessandro Di Federico, Federico Maggi, Paolo Milani Comparetti, and Stefano Zanero. **Lines of Malicious Code: Insights Into the Malicious Software Industry**. In *Proceedings of the 2012 Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

Local copy: papers/lindorfer-acsac12.pdf

Online: http://syssec-project.eu/nNa#lindorfer-acsac12.pdf

[7] Mario Graziano, Corrado Leita, and Davide Balzarotti. **Towards Network Containment in Malware Analysis Systems**. In *Proceedings of the 2012 Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

Local copy: papers/graziano-acsac12.pdf

Online: http://syssec-project.eu/nNa#graziano-acsac12.pdf

[8] Leyla Bilge, Davide Balzarotti, William Robertson, Engin Kirda, and Christopher Kruegel. **DISCLOSURE: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis**. In *Proceedings of the 2012 Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

Local copy: papers/bilge-acsac12.pdf

Online: http://syssec-project.eu/nNa#bilge-acsac12.pdf

[9] Lyuben Boyanov, Zlatogor Minchev, and Kiril Boyanov. **Some Cyber Threats in Digital Society**. *International Journal "Automatics & Informatics"*, 1, January 2013.

Local copy: papers/boyanov-autoinfo-2013.1.pdf

Online: http://syssec-project.eu/nNa#boyanov-autoinfo-2013.1.pdf

[10] Frank Breitinge and Kaloyan Petrov. **Reducing time cost in hashing operations**. In *Proceedings of the 9th Annual IFIP WG 11.9 International Conference on Digital Forensics*, Orlando, FL, USA, January 2013.

Local copy: papers/breitinge-ifip-wg11.9-2013.pdf

Online: http://syssec-project.eu/nNa#breitinge-ifip-wg11.9-2013.pdf

[11] Davide Canali and Davide Balzarotti. **Behind the Scenes of Online Attacks: an Analysis of Exploitation Behaviors on the Web**. In *Proceedings of the 2013 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2013.

Local copy: papers/canali-ndss13.pdf

Online: http://syssec-project.eu/nNa#canali-ndss13.pdf

[12] Evangelos Ladakis, Lazaros Koromilas, Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. **You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger**. In *Proceedings of the 6th European Workshop on System Security (EuroSec)*, Prague, Czech Republic, April 2013.

Local copy: papers/ladakis-eurosec13.pdf

Online: http://syssec-project.eu/nNa#ladakis-eurosec13.pdf

[13] Mar Callau-Zori, Ricardo Jiménez-Peris, Vincenzo Gulisano, Marina Papatriantafilo, Zhang Fu, and Marta Patio-Martínez. **STONE: a stream-based DDoS defense framework**. In *Proceedings of the ACM Symposium on Applied Computing (SAC)*, pages 807–812, March 2013.

Local copy: papers/callau-sac13.pdf

Online: http://syssec-project.eu/nNa#callau-sac13.pdf

[14] Shlomi Dolev, Omri Liba, and Elad M. Schiller. **Self-Stabilizing Byzantine Resilient Topology Discovery and Message Delivery**. In *Proceedings of the 2013 International Conference on Networked Systems (NETSYS)*, Marrakech, Morocco, May 2013.

Local copy: papers/dolev-netsys13.pdf

Online: http://syssec-project.eu/nNa#dolev-netsys13.pdf

[15] Federico Maggi, Alessandro Frossi, Stefano Zanero, Gianluca Stringhini, Brett Stone-Gross, Christopher Kruegel, and Giovanni Vigna. **Two Years of Short URLs Internet Measurement: Security Threats and Countermeasures**. In *Proceedings of the 22nd International World Wide Web Conference (WWW)*, Rio de Janeiro, Brazil, May 2013.

Local copy: papers/maggi-longshore-www13.pdf

Online: http://syssec-project.eu/nNa#maggi-longshore-www13.pdf

[16] Davide Canali, Davide Balzarotti, and Aurelien Francillon. **The Role of Web Hosting Providers in Detecting Compromised Websites**. In *Proceedings of the 22nd International World Wide Web Conference (WWW)*, Rio de Janeiro, Brazil, May 2013.

Local copy: papers/canali-www13.pdf

Online: http://syssec-project.eu/nNa#canali-www13.pdf

[17] Zlatogor Minchev, Luben Boyanov, and Stiliyan Georgiev. **Security of Future Smart Homes. Cyber-Physical Threats Identification Perspectives**. In *Proceedings of the National Conference with International Participation in Realization of the EU project "Development of Tools Needed to Coordinate Inter-sectorial Power and Transport CIP Activities at a Situation of Multilateral Terrorist Threat. Increase of the Capacity of Key CIP Objects in Bulgaria"*, Sofia, Bulgaria, June 2013.

Local copy: papers/zm-smart-home-security-cipbg13.pdf

Online: http://syssec-project.eu/nNa#zm-smart-home-security-cipbg13.pdf

[18] Zlatogor Minchev. **Security of Digital Society. Technological Perspectives & Challenges**. In *Proceedings of the Jubilee International Scientific Conference "Ten Years Security Education in New Bulgarian University: Position and Perspectives for the Education in a Dynamic and Hardly Predicted Environment"*, Sofia, Bulgaria, June 2013.

Local copy: papers/zm-digital-society-security-nbu13.pdf

Online: http://syssec-project.eu/nNa#zm-digital-society-security-nbu13.pdf

[19] Andrei Costin, Jelena Isacenkova, Marco Balduzzi, Aurelien Francillon, and Davide Balzarotti. **The Role of Phone Numbers in Understanding Cyber-Crime Schemes**. In *Proceedings of the Annual Conference on Privacy, Security and Trust (PST)*, Terragona, Spain, July 2013.

Local copy: papers/costin-phonenumbers.pdf

Online: http://syssec-project.eu/nNa#costin-phonenumbers.pdf

[20] Matthias Neugschwandtner, Martina Lindorfer, and Christian Platzer. **A view to a kill: Webview exploitation**. In *Proceedings of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, Washington, DC, USA, August 2013.

Online: USENIX website

[21] Istvan Haller, Asia Slowinska, Matthias Neugschwandtner, and Herbert Bos. **Dowsing for overflows: A guided fuzzer to find buffer boundary violations**. In *Proceedings of the 22nd USENIX Security Symposium (USENIX-SEC)*, Washington, DC, USA, August 2013.

Online: USENIX website

3 Talks, seminars and presentations

[1] Stefano Zanero. **Industrial impact of a NoE: the approach of SysSec**. At *EffectsPlus Workshop*, Padua, Italy, September 2012.

Local copy: talks/zanero-effectsplus-sep12.pdf
Online: http://syssec-project.eu/jNa#zanero-effectsplus-sep12.pdf

[2] Zlatogor Minchev. **Dynamics of Threats and Users Response as a Result of Entertainment Activities (An On-line Social Networks Case Study)**. At *IFIP TC14 Entertainment Computing Meeting*, Bremen, Germany, September 2012.

Local copy: talks/zm-ifip-tc14-sep12.pdf
Online: http://syssec-project.eu/jNa#zm-ifip-tc14-sep12.pdf

[3] Todor Tagarev, Zlatogor Minchev, and Nataliya Ivanova. **Academic Research on Cybersecurity**. At *6th Scientific Conference of the International Information Security Research Consortium*, Sofia, Bulgaria, October 2012.

Local copy: talks/ttzmni-cybersec-research-oct12.pdf
Online: http://syssec-project.eu/jNa#ttzmni-cybersec-research-oct12.pdf

[4] Zlatogor Minchev. **Social Networks Security Aspects: A Technological and User Based Perspectives**. At *20th National Jubilee Conference with International Participation (TELECOM2012)*, Sofia, Bulgaria, October 2012.

Local copy: talks/zm-telecom-oct12.pdf
Online: http://syssec-project.eu/jNa#zm-telecom-oct12.pdf

[5] Evangelos Markatos. **Managing Threats and Vulnerabilities in the Future Internet**. At *Joint EDA EC Workshop*, Brussels, Belgium, October 2012.

Local copy: talks/markatos-eda-ec-oct12.pdf
Online: http://syssec-project.eu/jNa#markatos-eda-ec-oct12.pdf

[6] Zlatogor Minchev. **Cybersecurity Academic Research Innovations**. At *Round Table "Conceptual Aspects of Cyberwarfare and Cyberdefence", Military Academy G.S. Rakovski*, Sofia, Bulgaria, October 2012.

Local copy: talks/zm-sofia-rakovski-nov12.pdf
Online: http://syssec-project.eu/jNa#zm-sofia-rakovski-nov12.pdf

[7] Zlatogor Minchev. **Integrated Border Security Aspects: Bulgarian Academic Experience and Development Perspectives**. At *International conference "The Eastern Partnership: Assessment of Past Achievements and Future Trends"*, Bucharest, Romania, November 2012.

Local copy: talks/zm-bucharest-nov12.pdf
Online: http://syssec-project.eu/jNa#zm-bucharest-nov12.pdf

[8] Asia Slowinska. **Body Armor for Binaries**. At *BeNeLux OWASP Day 2012 (invited talk)*, Leuven, Belgium, November 2012.

Local copy: talks/asia-owasp-nov12.pdf
Online: http://syssec-project.eu/jNa#asia-owasp-nov12.pdf

[9] Iasonas Polakis. **All your face are belong to us: Breaking Facebook's Social Authentication**. At *2012 Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

Local copy: talks/polakis-facebook-acsac-dec12.pdf
Online: http://syssec-project.eu/jNa#polakis-facebook-acsac-dec12.pdf

[10] Martina Lindorfer. **Lines of Malicious Code: Insights Into the Malicious Software Industry**. At *2012 Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

Local copy: talks/lindorfer-malicious-acsac-dec12.pdf
Online: http://syssec-project.eu/jNa#lindorfer-malicious-acsac-dec12.pdf

[11] Zlatogor Minchev. **Scenario Method Application**. At *University of National and World Economy (invited talk)*, Sofia, Bulgaria, March 2013.

Local copy: talks/minchev-scenario-method-unwe-mar13.pdf
Online: http://syssec-project.eu/jNa#minchev-scenario-method-unwe-mar13.pdf

[12] Evangelos Markatos. **Privacy-Preserving Social Plugins**. At *Boston University (invited talk)*, Boston, MA, USA, April 2013.

Local copy: talks/markatos-bu-apr13.pdf
Online: http://syssec-project.eu/jNa#markatos-bu-apr13.pdf

[13] Stefano Zanero. **All Your Face Are Belong to Us: Breaking Facebook's Social Authentication**. At *HackCon 2013*, Oslo, Norway, April 2013.

Local copy: talks/zanero-fb-hackcon-apr13.pdf
Online: http://syssec-project.eu/jNa#zanero-fb-hackcon-apr13.pdf

[14] Federico Maggi. **All Your Face Are Belong to Us: Breaking Facebook's Social Authentication**. At *Hek.si 2013*, Ljubljana, April 2013.

Local copy: talks/maggi-resa-heksi-apr13.pdf
Online: http://syssec-project.eu/jNa#maggi-resa-heksi-apr13.pdf

[15] Zlatogor Minchev. **New Challenges in the Academic Cybersecurity Studies**. At *National Conference "NATO & EU Defence Capabilities. The Contribution of the Republic of Bulgaria to Their Building and Development"*, Sofia, Bulgaria, April 2013.

Local copy: talks/minchev-cvk-apr13.pdf
Online: http://syssec-project.eu/jNa#minchev-cvk-apr13.pdf

[16] Evangelos Markatos. **SysSec: Emerging Threats and Vulnerabilites**. At *Cyber Security & Privacy EU Forum*, Brussels, Belgium, April 2013.

Local copy: talks/markatos-csp-track14-apr13.pdf
Online: http://syssec-project.eu/jNa#markatos-csp-track14-apr13.pdf

[17] Zlatogor Minchev. **Recent Bulgarian Academic Studies on Interactive Entertainment**. At *IFIP TC14 Annual Meeting*, Paris, France, May 2013.

Local copy: papers/zm-tc14-may13.pdf
Online: http://syssec-project.eu/nNa#zm-tc14-may13.pdf

[18] Stefano Zanero. **Behavior-based Methods for Automated, Scalable Malware Analysis**. At *MIT CSAIL-POLIMI Workshop (invited talk)*, Boston, MA, USA, May 2013.

Local copy: talks/zanero-auto-analysis-mit.pdf
Online: http://syssec-project.eu/jNa#zanero-auto-analysis-mit.pdf

[19] Federico Maggi. **AndroTotal A Scalable Framework for Android Antimalware Testing**. At *MIT CSAIL-POLIMI Workshop (invited talk)*, Boston, MA, USA, May 2013.

Local copy: talks/maggi-andrototal-mit-may13.pdf
Online: http://syssec-project.eu/jNa#maggi-andrototal-mit-may13.pdf

[20] Stefano Zanero. **Security of Cyber-Physical Systems**. At *Smau 2013 (invited talk)*, Bologna, Italy, June 2013.

Local copy: talks/zanero-smau13.pdf
Online: http://syssec-project.eu/jNa#zanero-smau13.pdf

[21] Luben Boyanov and Zlatogor Minchev. **Cyber Threats Identification Framework for Future Smart Homes**. At *NATO ARW "Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework"*, Ohrid, FYROM, June 2013.

Local copy: papers/lb-zm-smart-homes-nato-arw-jun13.pdf
Online: http://syssec-project.eu/nNa#lb-zm-smart-homes-nato-arw-jun13.pdf

[22] Zlatogor Minchev. **Security of Digital Society. Technological Perspectives & Challenges**. At *Jubilee International Scientific Conference "Ten Years Security Education in New Bulgarian University: Position and Perspectives for the Education in a Dynamic and Hardly Predicted Environment"*, Sofia, Bulgaria, June 2013.

Local copy: papers/zm-digital-society-security-talk-nbu13.pdf
Online: http://syssec-project.eu/nNa#zm-digital-society-security-talk-nbu13.pdf

[23] Zlatogor Minchev. **Cyberthreats and Challenges in the Digital Era**. At *XII Summer School on Mathematics and Informatics (LISH13)*, Varna, Bulgaria, August 2013.

Local copy: papers/zm-threats-challenges-lish13.pdf
Online: http://syssec-project.eu/nNa#zm-threats-challenges-lish13.pdf

4 Other Dissemination Activities

4.1 Cooperation with other projects and research institutes

SysSec made a conspicuous effort to integrate and cooperate with other projects funded by the EU and other entities. In particular:

- **SysSec in the Effects+/SecCord EU Yearbook**:
  During this reporting period we were contacted by Effects+/SecCord projects who are compiling a Yearbook for the EU Commission emphasizing the major achievements of different projects. They asked us to provide some input about the highlights of *SysSec* in 2012. In response, we gave them details on our successfull *1st SysSec Summer School*. More important, we arranged phone-interviews with several *SysSec* members in order to discuss the project research results and activities in detail.

  URL: http://cordis.europa.eu/projects/rcn/105977_en.html

- **Questionnaire for the Monitoring of the IST R&D Implementation in 2012**:
  At the DG's request, the consortium filled and submitted a questionnaire with the project's publications in 2012. Additionally, some publications from previous years which hadn't been successfully validated were re-submitted. The data will be used for the assessment of the overall progress made towards the achievement of the FP7 objectives.

  URL: http://ec.europa.eu/dgs/information_society/evaluation/rtd/indicators/index_en.htm

- **Cooperation with CRISALIS project**:
  CRISALIS[1] is an EU fundedaims project which aims at providing new means to secure critical infrastructure environments from targeted attacks. We invited the project to share their knowledge with the attendants of the 1st SysSec Summer School. They responded positively and we had **Damiano Bolzoni** (also a member of our Cyber-attacks Working Group) and **Dina Hadziosmanovic** joining us for the event.

[1] http://www.crisalis-project.eu

More details on their present in our Summer School can be found in Section 4.5.4.

URL: http://www.syssec-project.eu/events/summer-school-2012/program/

- **Cooperation with CCDCOE**:
  On January 22nd, Dr. Stefano Zanero (PoliMi - *SysSec* member) visited the *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE)[2] in Tallinn, Estonia. The visit comprised meetings with different key people at the Centre, including the Director, Colonel Artur Suzik, and the Chief of R&D Dr. Raimo Peterson.

  PoliMi contributed to the efforts of the Centre by providing support for the 2013 edition of the "Locked Shields" exercise (a military cyberdefense exercise). PoliMi will further this cooperation by providing technical analysis of the captured traffic/logfiles, and correlating it with the human reports from the exercise. For the next years it is foreseen the possibility of personnel from the *SysSec* institutions to participate in the Red teams of the exercise thanks to our demonstrated skills in systems security attacks.

  Additionally, as the Centre has a mandate to develop and keep up to date a portfolio of technical courses, personnel from the Centre will join as *SysSec Associate Member* to access and use our curriculum materials. Invitations to *SysSec* members for lectures at courses and seminars have also been discussed.

4.2 Presence in other events

During September 2012–August 2013 the *SysSec* consortium and its members participated in several events and conferences:

- **Effectsplus 3rd Clustering Workshop**:
  On September 6, 2012, Effectsplus organized their third clustering workshop in Padua, Italy. The workshop had subject: *Exploitation and Impact of results of FP7 Security and Trust Research Projects*.

  The focus for the workshop was on the exploitation and business models and the impact and transfer of research results coming from research projects. The event provided an opportunity for projects in the security and trust area to present their ideas and directions on their exploitation and impact activities.

  Stefano Zanero participated to the event on behalf of *SysSec*. Stefano's presentation [1] included some best practices for engaging industrial partners into research projects. The participants were also encouraged

[2] http://www.ccdcoe.org

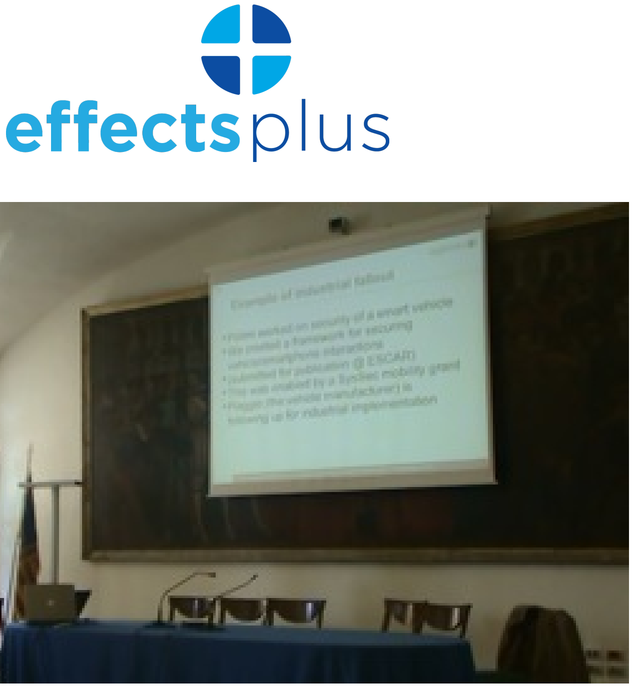


Figure 1: Stefano Zanero making a presentation in the 3rd Effectsplus Clustering Workshop.

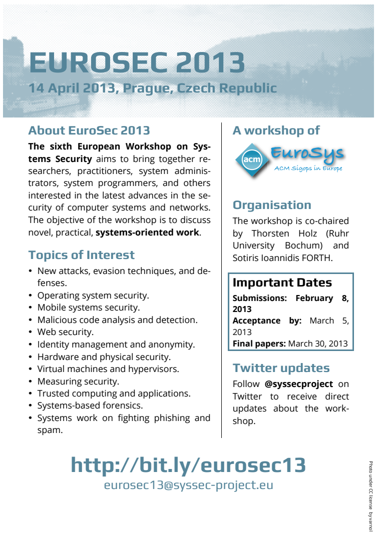
to provide feedback on the *SysSec* Research Roadmap and join the *SysSec* community as associate members.

URL: http://www.amiando.com/EffectsplusPadua.html

- **6th European Workshop on Systems Security**:
  The sixth European Workshop on Systems Security (EuroSec) was be held on April 14, 2012 in Prague, Czech Republic. The workshop (which is associated with the Annual ACM SIGOPS EuroSys conference[3]) focuses in discussion of novel, practical, systems-oriented work.

  For the **second consecutive year** *SysSec* contributed to the organization of the workshop. EuroSec 2013 is co-chaired by Sotiris Ioannidis (FORTH - *SysSec* member) and Thorsten Holz (Ruhr-University Bochum - *SysSec Associate Member*). Additionally, *SysSec* provided hosting and support for the workshop website and paper submission facility. We also used the communication channels of the project (*SysSec Constituency* mailing list and Twitter community) to promote the event. Furthermore, the call for submissions of the workshop was

[3] http://http://eurosys2013.tudos.org/



EUROSEC 2013

14 April 2013, Prague, Czech Republic

About EuroSec 2013

The sixth European Workshop on Systems Security aims to bring together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security of computer systems and networks. The objective of the workshop is to discuss novel, practical, **systems-oriented work**.

Topics of Interest

- New attacks, evasion techniques, and defenses.
- Operating system security.
- Mobile systems security.
- Malicious code analysis and detection.
- Web security.
- Identity management and anonymity.
- Hardware and physical security.
- Virtual machines and hypervisors.
- Measuring security.
- Trusted computing and applications.
- Systems-based forensics.
- Systems work on fighting phishing and spam.

A workshop of

Organisation

The workshop is co-chaired by Thorsten Holz (Ruhr University Bochum) and Sotiris Ioannidis FORTH.

Important Dates

Submissions: February 8, 2013
Acceptance by: March 5, 2013
Final papers: March 30, 2013

Twitter updates

Follow **@syssecproject** on Twitter to receive direct updates about the workshop.

http://bit.ly/eurosec13

eurosec13@syssec-project.eu

Photo under CC license by varnol

Figure 2: EuroSec 2013 promotional poster.

listed in the *Future Internet events page*[4] and sent to the *EffectsPlus project community*[5].

As a result of our efforts **a total of 27 submissions were received**, an increase of 7 compared to last year. The increase was significant, given the overlap in deadlines with other security conferences (e.g. DIMVA 2013). 8 papers were accepted for publication. There were also two invited talks by Boldizsár Bencsáth (*SysSec Associate Member*) and Christina Pöpper.

Around 30 people attended - which is a healthy number for small workshops like EuroSec. Overall, the feedback received from the attendees was positive. After the end of the workshop the chairs acknowledged and thanked *SysSec* members for their continued support to the workshop. On our part, we reaffirmed our support to the workshop and contributed to the discussions for the initial planning of EuroSec 2014.

URL: http://www.syssec-project.eu/eurosec-2013/

- **Cooperation with the European Internet Foundation**:
Stefano Zanero participated as a guest speaker and discussant in a workshop organized at the European Parliament by the European Internet Foundation[6] (EIF).

[4] http://bit.ly/14tiRTo

[5] http://www.effectsplus.eu/

[6] European Internet Foundation: http://www.eifonline.org/

The mission of the EIF is to help provide European political leadership for the development of European multilateral public policies responsive to the political, economic and social challenges of the world-wide digital revolution.

The workshop was organized to kickstart the "Digital World in 2030" report preparation. We contributed to the Socio-political Dimension Workshop, bringing to the table insights from the SysSec roadmap and Red Book.

URL: http://bit.ly/ZvbwED

4.3 Presence in the media

During September 2012–August 2013 we tracked the following references to *SysSec* by traditional and online media.

- **Mention on the Digital Agenda for Europe website**:

  Digital Agenda for Europe has added an article in their website titled **"Fighting cyberthreats, making the future more secure"**. *SysSec* is being mentioned in the article and also quote a statement from our ERCIM news article[7] which we covered in the previous reporting period:

  > For the last two years, the European Commission contributes EUR 2.5 million to establish *SysSec*, a European "Network of Excellence" (NoE) built on the age-old concept that prevention is better than cure. The NoE is focused on developing solutions for predicting threats and vulnerabilities before they occur, enabling potential victims of cyber-attacks to build defences before threats materialise.
  >
  > The SysSec "Network of Excellence" takes a game-changing approach to cyber security: instead of chasing the attackers after an attack has taken place, SysSec studies emerging threats and vulnerabilities ahead of time. The network's main thrusts are to identify a roadmap to work on threats and to build infrastructure to boost education in system security - to provide the expertise needed to deal with these emerging threats, Evangelos Markatos, the project coordinator, and Herbert Bos, a fellow Syssec researcher, note in a paper on the project.

  URL: http://ec.europa.eu/digital-agenda/

[7] http://syssec-project.eu/iTa

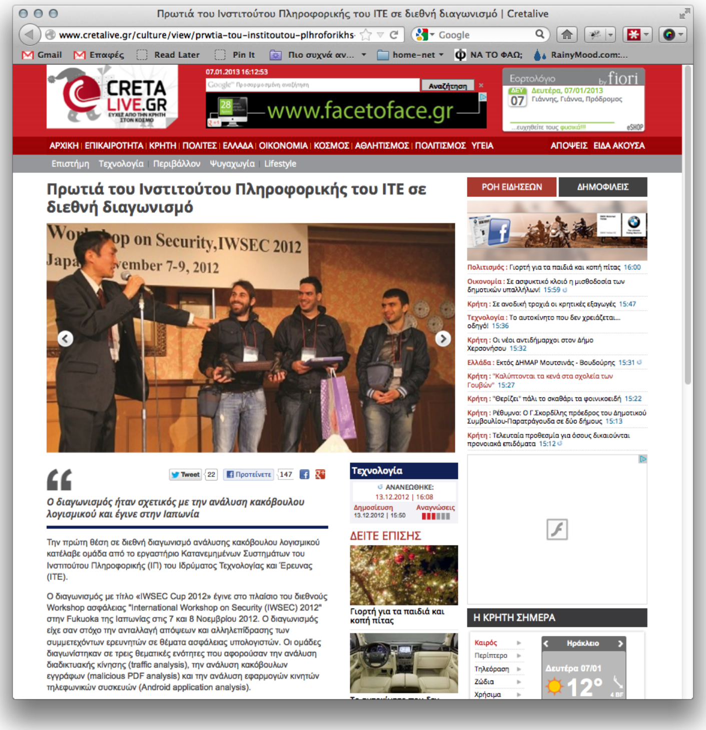
- **FORTH success at IWSEC Malware Analysis Competition**:
  On 7-8 November 2012, the team of Athanasios Petsas, Zacharias Tzermias, and Nikolaos Tsikoudis, from FORTH (the Foundation for Research and Technology Hellas) won the **Gold Prize at the malware competition analysis of the International Workshop on Security (IWSEC) Cup 2012**.

  Figure 3: Minotaurus Team in action.

  The winning team (see Figure 3), nicknamed **Minotaurus** - after the mythical half-bull/half-human creature from Crete, competed against two teams from Japan and one team from the USA. All the teams competed in three challenges involving, traffic analysis, malicious PDF analysis, and Android application analysis. To reach the winning prize, Minotaurus made extensive use of **MDScan**[8] which has been partly **developed in the context of SysSec**.

  MDScan is used to **detect polymorphic attacks masquerading themselves as ordinary data hidden inside PDF files**. Although PDF files are usually perceived as innocent “data” files, they may actually contain executable code that can pose a significant threat to anyone opening it. Despite the best efforts from several available PDF/antivirus tools, malicious PDF files remain a sizeable threat that may go undetected, especially when aggressors obfuscate their code in order to conceal it further. MDScan takes this into account and, by using a combination of different analysis techniques, tries to uncover and expose the obfuscated executable code and raise an alert before the malicious code manages to compromise the computer.

[8] http://syssec-project.eu/publications/#mdscan-eurosec11.pdf



Πρωτιά του Ινστιτούτου Πληροφορικής του ΙΤΕ σε διεθνή διαγωνισμό | Cretalive

www.cretalive.gr/culture/view/prwtia-tou-institoutou-plhroforikhs-

07.01.2013 16:12:53

Google™ Προσαρμοσμένη αναζήτηση

ΔΕΥ 07 Δευτέρα, 07/01/2013 Γιάννης, Γιάννα, Πρόδρομος

...ευχηθείτε τους φυσικά!!!

Πρωτιά του Ινστιτούτου Πληροφορικής του ΙΤΕ σε διεθνή διαγωνισμό

Ο διαγωνισμός ήταν σχετικός με την ανάλυση κακόβουλου λογισμικού και έγινε στην Ιαπωνία

Την πρώτη θέση σε διεθνή διαγωνισμό ανάλυσης κακόβουλου λογισμικού κατέλαβε ομάδα από το εργαστήριο Κατανεμημένων Συστημάτων του Ινστιτούτου Πληροφορικής (ΙΠ) του Ιδρύματος Τεχνολογίας και Έρευνας (ΙΤΕ).

Ο διαγωνισμός με τίτλο «IWSEC Cup 2012» έγινε στο πλαίσιο του διεθνούς Workshop ασφάλειας "International Workshop on Security (IWSEC) 2012" στην Fukuoka της Ιαπωνίας στις 7 και 8 Νοεμβρίου 2012. Ο διαγωνισμός είχε σαν στόχο την ανταλλαγή απόψεων και αλληλεπίδρασης των συμμετεχόντων ερευνητών σε θέματα ασφάλειας υπολογιστών. Οι ομάδες διαγωνίστηκαν σε τρεις θεματικές ενότητες που αφορούσαν την ανάλυση διαδικτυακής κίνησης (traffic analysis), την ανάλυση κακόβουλων εγγράφων (malicious PDF analysis) και την ανάλυση εφαρμογών κινητών τηλεφωνικών συσκευών (Android application analysis).

ΑΝΑΝΕΩΘΗΚΕ: 13.12.2012 | 16:08

Δημοσίευση 13.12.2012 | 15:50

Αναγνώσεις

Γιορτή για τα παιδιά και κοπή πίτας

Πολιτισμός : Γιορτή για τα παιδιά και κοπή πίτας 16:00

Οικονομία : Σε ασφυκτικό κλοιό η μισθοδοσία των δημοτικών υπαλλήλων! 15:59

Κρήτη : Σε ανοδική τροχιά οι κρητικές εξαγωγές 15:47

Τεχνολογία : Το αυτοκίνητο που δεν χρειάζεται... οδηγό! 15:36

Κρήτη : Οι νέοι αντιδήμαρχοι στον Δήμο Χερσονήσου 15:32

Ελλάδα : Εκτός ΔΗΜΑΡ Μουτσινάς - Βουδούρης 15:31

Κρήτη : "Καλύπτονται τα κενά στα σχολεία των Γουβών" 15:27

Κρήτη : "Θερίζει" πάλι το σκαθάρι τα φοινικοειδή 15:22

Κρήτη : Ρέθυμνο: Ο Γ.Σκορδίλης πρόεδρος του Δημοτικού Συμβουλίου-Παρατράγουδα σε δύο δήμους 15:13

Κρήτη : Τελευταία προθεσμία για όσους δικαιούνται προνοιακά επιδόματα 15:12

Figure 4: Local news portal CretaLive.gr covered the success of Minotaurus Team.

The success was covered by the local media (see Figure 4).

The e-zine of the Greek *General Secretariat for Research and Technology*[9] covered FORTH's success[10] in the 2012 Malware Analysis Competition of the International Workshop on Security (IWSEC) in its January issue (see Figure 5). The article mentions that the winning team used the *SysSec*-developed **MDScan**[11] tool.

URL: http://www.syssec-project.eu/TUa

- **Computerworld blog reports on SysSec paper**: Computerworld featured a blog post on (see Figure 6) Iasonas Polakis' et al. paper [5] on Breaking Facebook's Social Authentication. The post includes commentary by Stefano Zanero (co-author of the paper), who stressed that the results of this research are not applicable

[9] http://www.gsrt.gr/

[10] The success has been covered in the previous report. It is also covered on the website news section: http://www.syssec-project.eu/TUa

[11] http://syssec-project.eu/publications/#mdscan-eurosec11.pdf

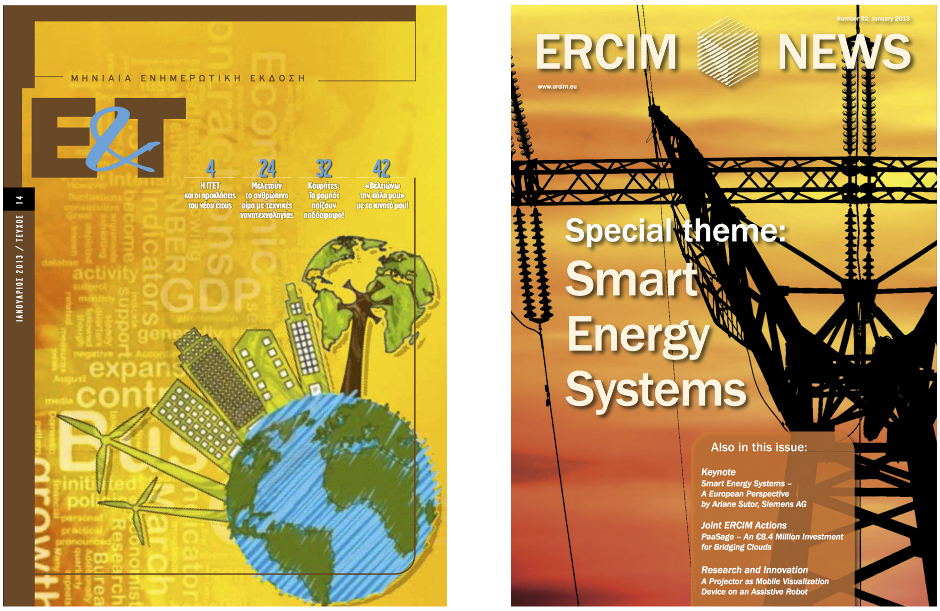

ΜΗΝΙΑΙΑ ΕΝΗΜΕΡΩΤΙΚΗ ΕΚΔΟΣΗ
E&T
ΙΑΝΟΥΑΡΙΟΣ 2013 / ΤΕΥΧΟΣ 14
4
24
32
42
ERCIM NEWS
Number 92, January 2013
www.ercim.eu
Special theme:
Smart Energy Systems
Also in this issue:
Keynote
Smart Energy Systems – A European Perspective by Ariane Sutor, Siemens AG
Joint ERCIM Actions
PaaSage – An €8.4 Million Investment for Bridging Clouds
Research and Innovation
A Projector as Mobile Visualization Device on an Assistive Robot

Figure 5: The January issues of *E&T Online* and *ERCIM News* featured *SysSec* related articles.

to the broader area of Social Authentication and not only Facebook's implementation of the concept.

URL: http://shar.es/465Lg

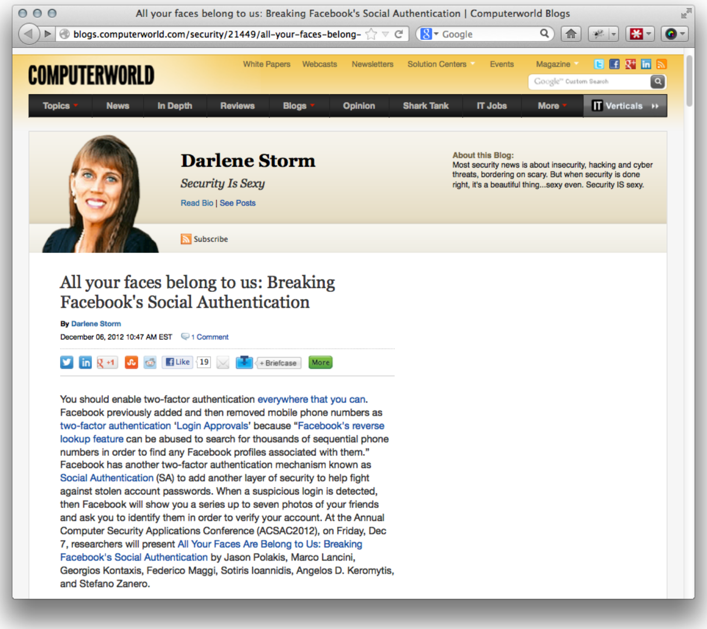
- **Opinion article in NRC newspaper**:
Herbert Bos, Maarten van Steen, Dennis Andriesse and Christian Rossow authored an opinion article on the Dutch minister's proposal to fight cybercrime by "hacking back". The article, titled *"Het Virusdilemma"* was published in *NRC Handelsblad*[12] (Dutch national newspaper) on November 24, 2012.

  URL: http://syssec-project.eu/oNa#het-virusdilemma.pdf

- January's issue of ERCIM News[13] had a special theme on Smart Energy Systems (see Figure 5). *SysSec* contributed to the edition with an article titled *"Cybersecurity in the Smart Grid"* authored by Magnus Almgren (Chalmers), Davide Balzarotti (Eurécom), Marina Papatriantafilou (Chalmers) and Valentin Tudor (Chalmers). The article argues on the importance of transferring knowledge from the domain of ICT security to the domain of Smart Grids. It points that efforts like

[12] http://www.nrc.nl/

[13] http://ercim-news.ercim.eu/



Darlene Storm

Security Is Sexy

About this Blog:
Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

All your faces belong to us: Breaking Facebook's Social Authentication

By Darlene Storm
December 06, 2012 10:47 AM EST 1 Comment

You should enable two-factor authentication everywhere that you can. Facebook previously added and then removed mobile phone numbers as two-factor authentication 'Login Approvals' because "Facebook's reverse lookup feature can be abused to search for thousands of sequential phone numbers in order to find any Facebook profiles associated with them." Facebook has another two-factor authentication mechanism known as Social Authentication (SA) to add another layer of security to help fight against stolen account passwords. When a suspicious login is detected, then Facebook will show you a series up to seven photos of your friends and ask you to identify them in order to verify your account. At the Annual Computer Security Applications Conference (ACSAC2012), on Friday, Dec 7, researchers will present All Your Faces Are Belong to Us: Breaking Facebook's Social Authentication by Jason Polakis, Marco Lancini, Georgios Kontaxis, Federico Maggi, Sotiris Ioannidis, Angelos D. Keromytis, and Stefano Zanero.

Figure 6: Darlene Storm's blog post about *SysSec* paper on Facebook's Social Authentication.

SysSec and CRISALIS[14] could play an important role in developing cross-domain expertise in ICT security and power engineering.

URL: http://ercim-news.ercim.eu/en92/special/cybersecurity-in-the-smart-grid

- In January 2013, IT4Sec[15] published a report authored by Zlatogor Minchev (IICT-BAS) with title *Cyber Threats in Social Networks and Users' Response Dynamics*. The report makes several references to *SysSec*.

  URL: http://www.it4sec.org/node/5643

- **VU interviews on the Dutch media**:
  Through April 2013 Herbert Bos (VU) has been interviewed by the Dutch media in several occasions for issues related to the wider IT-security area. Specifically:

  - On April 10 several regional papers interviewed Herbert about the DDoS attack on Dutch banks.
  - On the same date he was also interviewed by the national news (*RTL Nieuws*) on the same subject.

[14] http://www.crisalis-project.eu/
[15] http://it4sec.org/

- On April 23 Herbert gave an interview on national radio *BNR*[16].
- On April 24 there was an interview on the *Hoe?Zo!* national radio[17].

4.4 SysSec Industrial Advisory Board

Two new members joined the *SysSec* IAB after being contacted by Chalmers. We now have **8 IAB members** who are listed below. The new members appear in bold.

- **Göran Ericsson (Swedish National Grid)**
- **Håkan Kvarnström (Telia)**
- Leif Axelsson (VTEC - Volvo)
- Marc Dacier (Symantec)
- John Ioannidis (Google)
- Jean-Pierre Faye (Thales)
- George Danezis (Microsoft)
- Julio Canto (Hispasec)

The 2nd physical[18] *SysSec* Industrial Advisory Board meeting took place on March 27 2013, following the project's plenary meeting, and co-located with the 3rd workgroup meetings.

4.5 1st Summer School

4.5.1 Overview

The 1st *SysSec* Summer School[19] took place at Vrije Universiteit (VU) Amsterdam (see Figure 7), Thursday October 10 to Friday October 11, 2012. Its main topic was System Security and **malware reverse engineering** with a special focus on **critical infrastructure protection**.

One of the goals of the 2012 SysSec Summer School was to have a hands-on approach. We wanted the students to **develop a skill** but also **learn from experts** that have analyzed recent threats partly targeting critical infrastructures. For that reason, the first day focused on general reverse engineering

[16] BNR interview is available on: http://bit.ly/1204e8F.

[17] Hoe?Zo! interview is available on: http://bit.ly/11K81s4. Relevant part starts on 13'50".

[18] An online IAB meeting has also been held in fall 2012.

[19] http://www.syssec-project.eu/events/summer-school-2012/

Figure 7: Entrance to VU, venue of the Summer School.

with lectures and practical exercises, while the second day focused on lectures highlighting the structure of new advanced malware and how it was analyzed.

The materials produced for the Summer School have become part of the Common Curriculum (WP4) thus further incrementing the impact of this experience.

4.5.2 Attendance

The registration for the Summer School opened on September 4 (Tuesday) with announcements sent to a few mailing lists in the following couple of days. The registration stayed open for less than a week, because by September 10 (Monday) we had already been overwhelmed with applications. The number of applications exceeded the capacity of the rooms available for the event, so we had to close the registration and create a waiting list.

In this period a total of about **65 participants expressed their interest to participate**. After changing the arrangements for the rooms, managed to admit 50 of these to the Summer School, out of who **49 students participated**.

The school was free for students affiliated with an academic institution while others paid a nominal fee of €200. 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 topics so interesting and useful for their future. Mostly Europeans participated but we also had a student from Brazil, for example.

It should be mentioned that many people who had declared their interest but in the end couldn't be admitted contacted us after the Summer School, asking for the material so that they could run a similar school on their own premises for their own students. We are currently exploring possibilities in how to share the material.

4.5.3 Speakers & Programme

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

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

The topics covered in the two days can be seen in Table 1. As we have already mentioned, the first day focused on general reverse engineering with lectures and practical exercises, while the second day focused on lectures highlighting the structure of new advanced malware and how it was analyzed.

4.5.4 Covered Topics

Day 1: The tutorials and lectures the first day covered the process of reverse engineering and the tools often used. For example, Davide Balzarotti explained the use of gdb and IDA Pro (see Figure 8). After the tutorials and lectures the first day, the students were given two challenges to reverse engineer (Figure 9). Among other tools, they used IDA Pro as Hex-Rays had generously sponsored the Summer School with a set of licenses for the students.

Before the school, we sent out a questionnaire to tune the exercises to the participants. They differed a bit in their knowledge so each challenge was offered in two versions, one normal and one advanced version. The

Day 1: Introduction to reverse engineering

Welcome and VM installation	$30'$
Session I *Herbert Bos*	$90'$
Session II *Davide Balzarotti*	$90'$
Practical Exercise	$3h30'$
Industry Perspective: Security in a changing DSO infrastructure *Erwin Kooi (Alliander)*	$60'$

Day 2: Advanced Malware and recent attacks against critical infrastructures

Critical Systems and their special constraints *Damiano Bolzoni (UTwente & CRISALIS), Dina Hadziosmanovic (UTwente)*	$60'$
Description and detailed analysis of Stuxnet *Heiko Patzlaff (Siemens CERT)*	$120'$
Analysis of Duqu/Flame *Boldizsár Bencsáth (CrySyS Lab)*	$120'$
Hooks and code injection in Duqu and Flame *Gábor Pék (CrySyS Lab)*	$30'$
Role of the DNO in Smartgrid security presentation *Frans Campfens (Alliander)*	$30'$

Table 1: Programme of the 1st SysSec Summer School

Figure 8: Davide Balzarrotti teaching the introduction to Tracing & Deguggging.

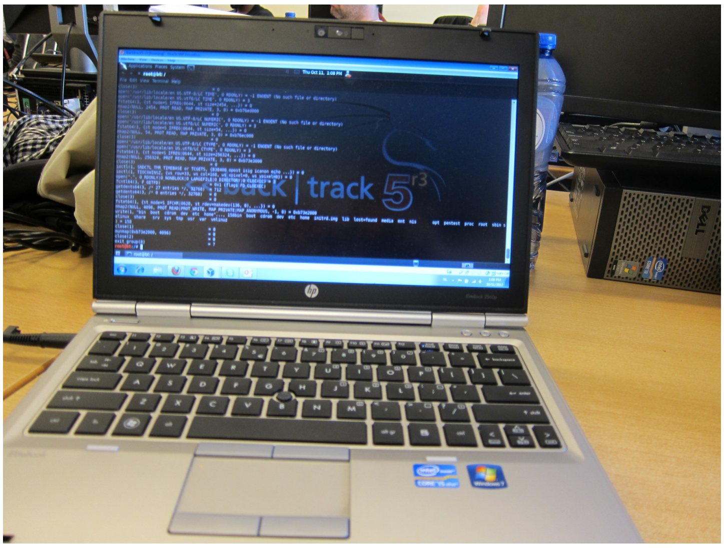


Figure 9: Backtrack linux tracing malware system calls during the hands-on practice.

challenges also had an associated hint sheet that was released after the students had had a change to look at the challenge, and finally the solutions were released.

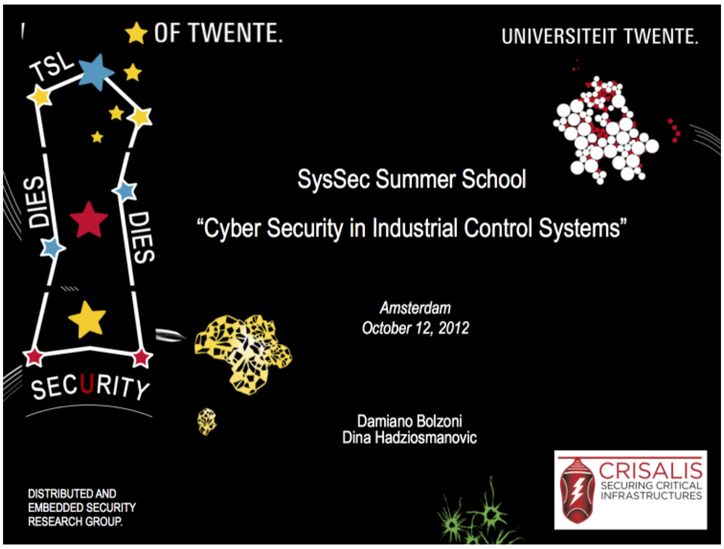
Figure 10: Herbert Bos helping students during the hands-on practice.

We also had a walk through to explain how the solution should be implemented. During the practical hands-on exercises, both Herbert Bos (Figure 10) and Davide Balzarotti walked around and helped students, and also several experts from VU were available if the students had questions. Even though we had many more students than envisioned, there was enough support available to help even the ones that did not know much before the start of the school.

In the evening of the first day, a social event with a dinner in the *Restaurant Café In de Waag Amsterdam*.

Day 2: The second day focused on lectures highlighting the structure of new advanced malware and how it was analyzed. We should note the presence of Damiano Bolzoni and Dina Hadziosmanovic from the **EU CRISALIS project**[20] who shared their knowledge on attacks on Industrial Control Systems (see Figure 11).

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


OF TWENTE.

UNIVERSITEIT TWENTE.

SysSec Summer School

“Cyber Security in Industrial Control Systems”

Amsterdam
October 12, 2012

Damiano Bolzoni
Dina Hadziosmanovic

CRISALIS
SECURING CRITICAL INFRASTRUCTURES

DISTRIBUTED AND
EMBEDDED SECURITY
RESEARCH GROUP.

TSL
DIES
DIES
SECURITY

Figure 11: Damiano Bolzoni and Dina Hadziosmanovic from CRISALIS Project discussed security in Industrial Control Systems.

Take-home challenges: Partly to minimize the cost of the students for the Summer School, the school only took place over two days. However, the students could take home the challenges and solve the more difficult ones on their own. Also, two weeks after the end of the physical school, we sent out an additional challenge to be solved by the students themselves, with the support of fellow students and teachers through an email list.

[20] http://www.crisalis-project.eu/

4.5.5 Evaluation of the Summer School

Overall, the impression we got was that the students liked the Summer School. After the end of the school we asked the students to fill an evaluation survey to get a more accurate picture of what they thought about the event.

So far[21], **the students have rated the Summer School with an average of** $4.3/5$. The lowest score, given by two students, was 3. When rating the individual days, students seem to appreciated more the hands on approach of the first day. The average score for the first day was $4.6/5$, with all responses being 4s and 5s. For the second day the average score was $4/5$, with 10 people giving it a mark of 3.

Most students actually seemed to want a longer Summer School, with maybe one full day of exercise. To envisage this wish, we created a mailing list in order to enable interactions between the students on the subjects covered in the Summer-School as well as the take-home challenges. We also used the list to release an additional challenge after the end of the Summer School (as described above), to be solved by the students by themselves (with the help of teachers and/or fellow students through the email list).

4.6 SysSec "Red Book"

Responding to a comment from the Reviewers and the Project Officer, we discussed how to make the revised *SysSec* Research Roadmap more captivating and increase its potential impact to future research in Europe. We concluded that it would be a good idea to write and release the updated Research Roadmap as a printed book rather than an electronic-only publication.

In the recent past, this approach had been successfully employed by FORWARD [22], the project that preceded *SysSec*. The FORWARD roadmap was labeled the *"White Book on Emerging ICT Threats"*. In order to convey a sense of continuation, we decided to release deliverable D4.3 under as *"The SysSec Red Book"*.

More important than the format and title change, we decided to assembly a *Task Force* of young security researchers with proven track record, to team-up with *SysSec* senior members and contribute to the publication. The following researchers were invited (and accepted):

- Asia Slowinska (VU University Amsterdam)
- Michalis Polychronakis (Columbia University)
- Elias Athanasopoulos (Columbia University)

[21] At the time of writing of this report we haven't yet received responses from all students.
[22] http://www.ict-forward.eu/

- Federico Maggi (Politecnico di Milano)
- Lorenzo Cavallaro (Royal Holloway, University of London)

Besides remote collaboration over email/teleconference, the Task Force members joined the Working Groups meeting in Amsterdam along with experts from the States and Europe (and IAB members).

The process started from teleconference brainstorming sessions on threats. ubsequently, in order to rank the threats identified during these sessions, we created an online questionnaire. On each page of the questionnaire, the Task Force members are asked to rank the threats along a different dimension. The dimensions include impact, likelihood, research need, time scale, target size, etc.

Based on their input, we restructured the questionnaire in order to make it simpler to fill, and presented it to *SysSec* consortium members and *Associate Members*. Then, in a subsequent iteration, it was sent to the members of related projects and the rest of our community.

The results of the questionnaire were used to guide the creation of the Red Book, and the structure of the output produced by the task force reflects the overall perception of our community with respect to upcoming threats and needed research.

In the end we believe that we will achieve producing a high quality roadmap document that will be equally useful to the EC (e.g. to use in the Horizon 2020 program) and the scientific community.

4.7 2nd SysSec Workshop

Our 2nd Workshop was co-located with the *2013 UbiCrypt Summer School on Reverse Engineering*[23], organized by Ruhr-University Bochum within the group of **Prof. Thorsten Holz**[24] (also a *SysSec Associate Member*).

The main benefit from this co-location was the opportunity to network with more young researchers and involve them in our network. Additionally, the co-location allowed us to free-up resources (both time and budget) for other activities, as Ruhr-University Bochum took care of the local arrangements.

The outcome was very satisfactory, with a full room for the whole day of the workshop (see Figure 12). Approximately 70 students enrolled to the whole of the Summer School (which we promoted), and approximately 30 people joined just for the SysSec event.

The workshop was laid out in 3 sessions:

- **Session 1:** Invited presentations of a selection of the best European papers in the systems security area.

[23] http://www.ubicrypt.hgi.rub.de/veranstaltungen/summerschool2013/

[24] http://www.ei.rub.de/fakultaet/professuren/tho/

Figure 12: The audience of the 2nd SysSec Workshop.

- **Session 2:** A session with a selection of "best rejected" papers, i.e., papers that contained quality researched but were at first rejected before being accepted in a top tier venue. The emphasis here was on the lessons learned from the rejections and the "secrets" of publishing in top-tier conferences.

- **Session 3:** Projects session, where security related EU projects were given the opportunity to present their best recent paper(s).

To conclude the workshop, we organized a social event with a poster session, allowing young researchers to present for informal discussion their most recent research results (see Figure 13).

The full workshop program is available at the following URL: http://syssec-project.eu/wks2p

The collection of the presentations will be made publicly available as Deliverable 2.3.

4.8 Dialogue with Standardization bodies

Acting upon recommendations of the reviewer, the partners are exploring ways to interact with relevant standardization bodies.

POLIMI met with Dr. Paul Nikolich, IEEE-SA chair of the 802 working groups, and he suggested to connect with the "Industry Connections Security Group", which is developing shared services and standards that benefit the anti-virus community. We are now in touch with Dr. James Wendorf of the IEEE Standards Association to interact with this group. We might help

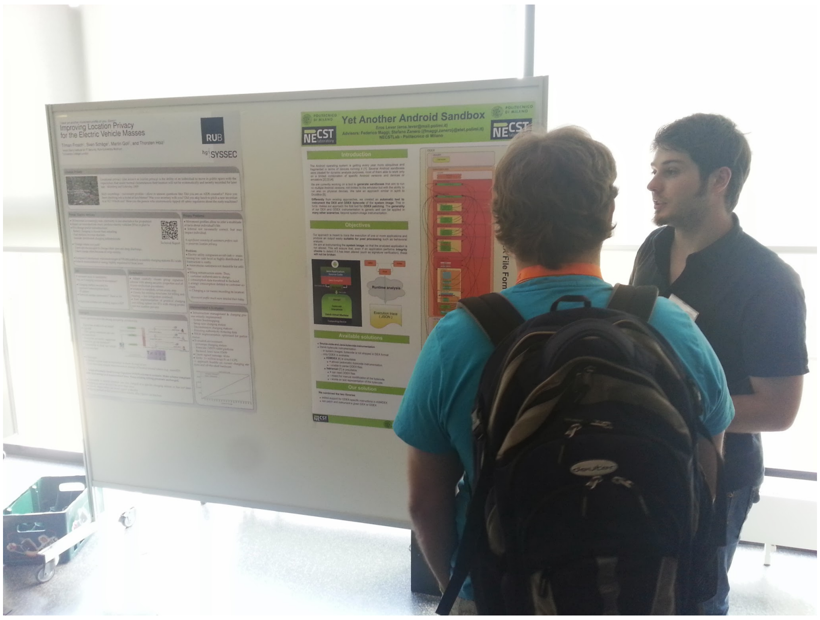

Improving Location Privacy for the Electric Vehicle Masses
RUB
SYSSEC
Yet Another Android Sandbox
NECST

Figure 13: Poster session at the 2$^{\text{nd}}$ SysSec Workshop.

transition the proposed Malware MetaData Exchange Format (MMDEF) into a formal standard.

EURECOM met with with Marco Obiso, cybersecurity coordinator for the International Telecommunications Union (ITU), the United Nations specialized agency for standardization in information and communication technologies, presenting him the SysSec project and discussing how we can contribute to the standardization process. Mr. Obiso will be our liaison if we identify some standards-related work to present to the standardization committee. He also expressed interest in the common curriculum.

TUBITAK is sending a representative to the next IETF meeting, and will seek ways to liaise our community with that body.

4.9 SysSec Constituency

During the third year, we kept expanding our dissemination base (which we call the SysSec "Constituency"). This is not just a mailing list, but a list of people with which we have direct connections, and who specifically wished to be informed of our activities.

At the end of this reporting period, we had a total of **240 people subscribed**[25].

So far, the dissemination list has a pivotal role in the promotion of both *SysSec* scientific output as well as the promotion of events and activities.

[25] This figure excludes the *SysSec* partners and Working Group members.

Some of the ocassions where we used the list include, the kickstarting our associate members program (see Section 4.10), the promotion of our workshops and hosted events and most important the announcment of the *SysSec* Red Book.

4.10 SysSec Associate Members

At the end of the second year of *SysSec*, we had announced our *Associate Members* (AMs) initiative with the goal to strengthen and expand our community. We see this initiative as an opportunity which would allow *SysSec* to evolve from a community of loosely related members to a *scientific association of affiliated members*.

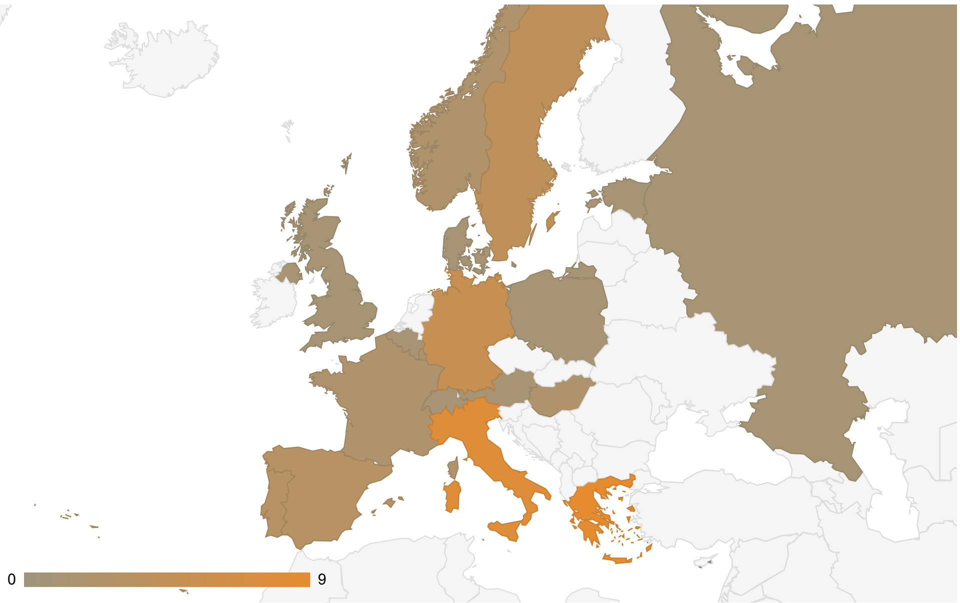


Figure 14: *SysSec Associate Members* across Europe. We have covered the major part of the continent and we hope to be able to expand further in the next year.

Applications for new *SysSec Associate Members* are received through our website. In order to strengthen our ties with the Associate Members and encourage people to apply, we came up with several incentives for them:

- Being eligible for *SysSec* scholarships.
- Access to the *SysSec* course repository and will be able to contribute course material as well.
- First who will receive hard copies of the *SysSec* Red Book (see Section 4.6).

- Invitations to online consultations related to *SysSec* roadmapping efforts.
- Invitations to meetings (such as workshops and summer schools) and the travel expenses of some of them may be covered by the project.

Applications to become an AM are evaluated on a bimonthly basis. The first round of evaluations took place early in this reporting period. After several such rounds, **our AM community currently lists 58 members** from around the world. Figure 14 shows the number of members we have across Europe[26].

5 SysSec website and social media

5.1 Mobile Layout Imrovements

Responding to comments received during conferences, we decided we should make our website more friendly to mobile devices such as tablets and phones. Towards this end we replaced the *960.gs* framework which we had initially used with the *Bootstrap* framework. Both frameworks layout the website content on a *grid*, so transition was straightforward. However Bootstrap comes loaded with a lot more components for common use cases. The most important of these is the *responsive layout* component, which automatically reflows the page contents to fit the display of the visitor's device (see Figure 15).

5.2 New and updated website sections

During the course of this third project year, besides the continuing updates and posting of news and documents from the project, we added or changed a few sections in the website which we will briefly outline in this section.

5.2.1 SysSec Organized Events

1st SysSec Summer School: On October 11-12, 2012, the *1st SysSec Summer School* was held in Amsterdam. We had already added information about the event to the *SysSec* website since late August 2012. The period preceding and following the event we added to the pages any information that was missing, including the final summer school programme. Detailed coverage of the event can be found in Section 4.5.

[26] A world map which also includes AMs from outside Europe is featured on our website: http://www.syssec-project.eu/community/members/.

2nd SysSec Workshop: Our 2nd was held on July 24, 2013 in Bochum, Germany. We added the programme and all other necessary information. Local arrangements were made by Ruhr-University Bochum, so we didn't have to provide extensive travel information etc. for the workshop but only pointers to their respective pages. More details on the 2nd SysSec Workshop can be found in Section 4.7.

5.2.2 Hosted Conference

During the third year of the project, we contributed to the organization of EuroSec 2013 conference. This is detailed in Section 4.2. One of our contributions to the event was the design, hosting and support of its website and paper submission facility. The website is hosted under the main *SysSec* websites, but uses a different theme from the main *SysSec* website. This year, we preserved the same colorscheme we had used for EuroSec 2012, but added a stylized photo from Prague in the page header in order to be able to easily distinguish the two. A screenshot can be seen in Figure 16.

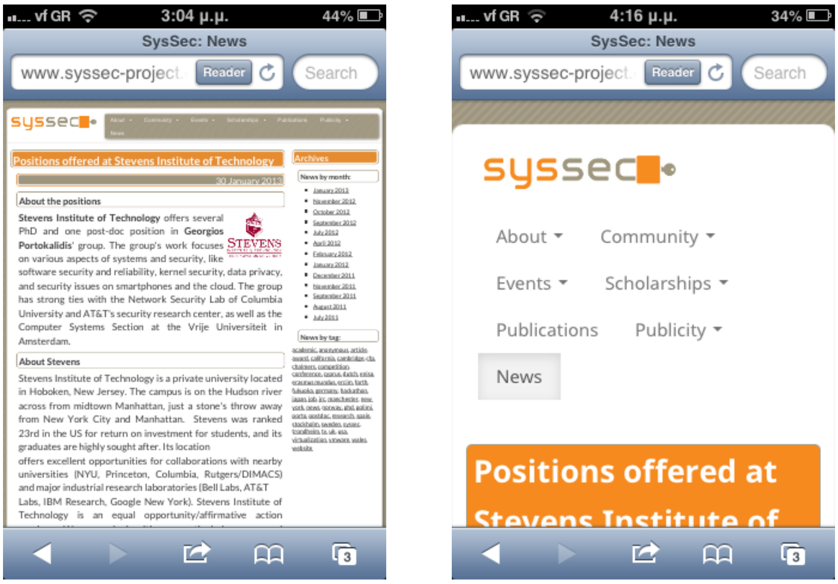
5.2.3 Community Section

The *Community* section was added late in August 2012, in order to host information about the *SysSec Associate Members*. Initially, it contained the form for applying to be a member and the list of accepted associate members. This year we also added a page presenting the benefits of being a *SysSec Associate Member*. Additionally, we show a world map showing in which countries we have associate members. In order to stress our focus on strengthening the Systems Security community in Europe, the default map view shows Europe. A world map view is also available by clicking the respective link.

5.3 Visitors & Trends

During this third year of the project, we received a total *11,600 visits* to our website. This represents a small increase (by 1%) compared to the second year. However the number *unique visitors increased by 7.34%*, a considerable increase. A detailed comparison of the website visitors during the second and third years can be seen in Figure 18.

In Figure 18 we can also see that the number of page views on the website dropped from the second to the third year. This may seem alarming on the first look, but after three years of SysSec it is expected that many visitors know what they are looking for on our website, which results in fewer pageviews. This case is also supported by the 100% increase in the number of downloaded documents (see Section 5.4 below).



Positions offered at Stevens Institute of Technology

30 January 2013

About the positions

Stevens Institute of Technology offers several PhD and one post-doc position in **Georgios Portokalidis**' group. The group's work focuses on various aspects of systems and security, like software security and reliability, kernel security, data privacy, and security issues on smartphones and the cloud. The group has strong ties with the Network Security Lab of Columbia University and AT&T's security research center, as well as the Computer Systems Section at the Vrije Universiteit in Amsterdam.

About Stevens

Stevens Institute of Technology is a private university located in Hoboken, New Jersey. The campus is on the Hudson river across from midtown Manhattan, just a stone's throw away from New York City and Manhattan. Stevens was ranked 23rd in the US for return on investment for students, and its graduates are highly sought after. Its location

offers excellent opportunities for collaborations with nearby universities (NYU, Princeton, Columbia, Rutgers/DIMACS) and major industrial research laboratories (Bell Labs, AT&T Labs, IBM Research, Google New York). Stevens Institute of Technology is an equal opportunity/affirmative action

Archives

News by month:

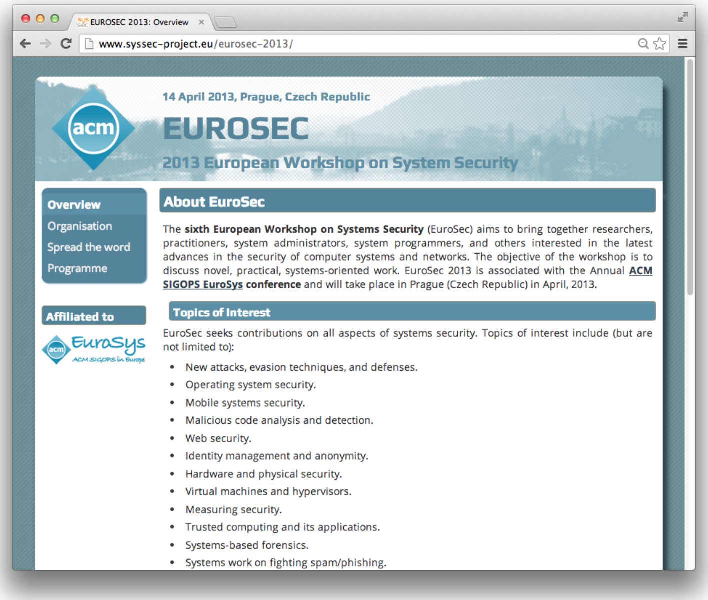
- January 2013
- November 2012
- October 2012
- September 2012
- July 2012
- April 2012
- February 2012
- January 2012
- December 2011
- November 2011
- September 2011
- August 2011
- July 2011

News by tag:

academic, anonymous, article, award, california, cambridge, cfp, chalmers, competition, conference, cyprus, dutch, enisa, erasmus mundus, ercim, forth, fukuoka, germany, hackathon, japan, job, jrc, manchester, new york, news, norway, phd, polimi, porto, postdoc, research, spain, stockholm, sweden, syssec, trondheim, tu, uk, usa, virtualization, vmware, wales, website

Positions offered at Stevens Institute of

Figure 15: Default iPhone view of the *SysSec* website news section when using the *960.gs* (left) and *Bootstrap* (right) frameworks. We can see that with Bootstrap the contents are automatically scaled to a size comfortable for reading without the user having to zoom-in manually.



14 April 2013, Prague, Czech Republic

EUROSEC

2013 European Workshop on System Security

About EuroSec

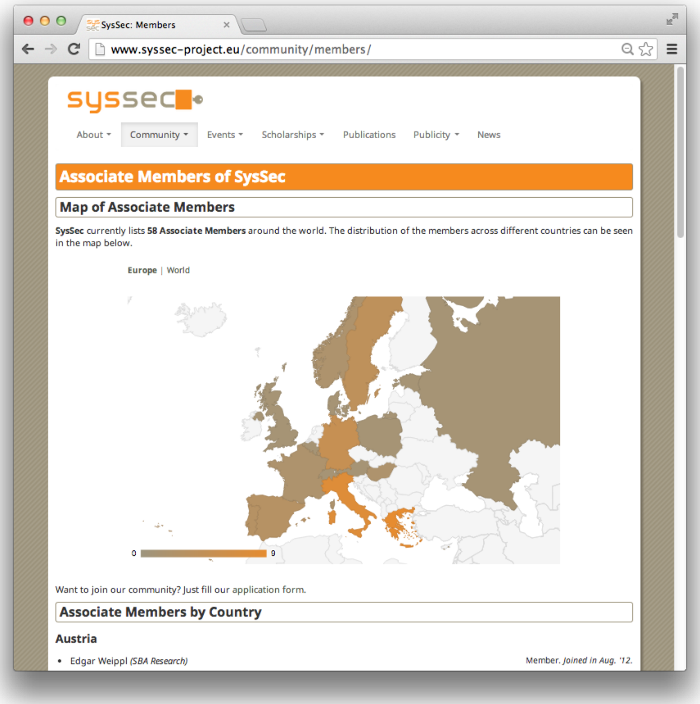
The **sixth European Workshop on Systems Security** (EuroSec) aims to bring together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security of computer systems and networks. The objective of the workshop is to discuss novel, practical, systems-oriented work. EuroSec 2013 is associated with the Annual **ACM SIGOPS EuroSys conference** and will take place in Prague (Czech Republic) in April, 2013.

Topics of Interest

EuroSec seeks contributions on all aspects of systems security. Topics of interest include (but are not limited to):

- New attacks, evasion techniques, and defenses.
- Operating system security.
- Mobile systems security.
- Malicious code analysis and detection.
- Web security.
- Identity management and anonymity.
- Hardware and physical security.
- Virtual machines and hypervisors.
- Measuring security.
- Trusted computing and its applications.
- Systems-based forensics.
- Systems work on fighting spam/phishing.

Figure 16: EuroSec 2013 website was hosted under www.syssec-project.eu.



Associate Members of SysSec

Map of Associate Members

SysSec currently lists **58 Associate Members** around the world. The distribution of the members across different countries can be seen in the map below.

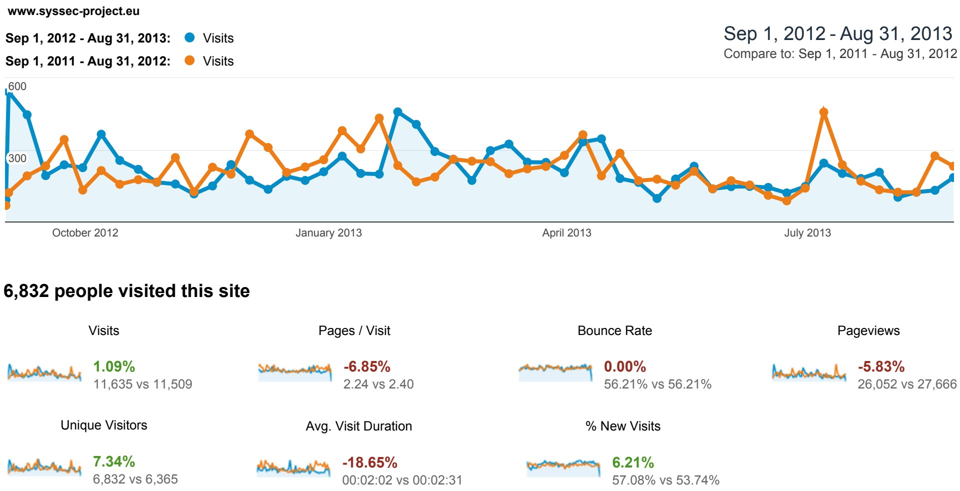
Want to join our community? Just fill our application form.

Associate Members by Country

Austria

- Edgar Weippl *(SBA Research)* Member. *Joined in Aug. '12.*

Figure 17: Community Section: List of *SysSec Associate Members*.


www.syssec-project.eu
Sep 1, 2012 - Aug 31, 2013: ● Visits
Sep 1, 2011 - Aug 31, 2012: ● Visits
Sep 1, 2012 - Aug 31, 2013
Compare to: Sep 1, 2011 - Aug 31, 2012
600
300
October 2012
January 2013
April 2013
July 2013

6,832 people visited this site

Visits
1.09%
11,635 vs 11,509

Pages / Visit
-6.85%
2.24 vs 2.40

Bounce Rate
0.00%
56.21% vs 56.21%

Pageviews
-5.83%
26,052 vs 27,666

Unique Visitors
7.34%
6,832 vs 6,365

Avg. Visit Duration
-18.65%
00:02:02 vs 00:02:31

% New Visits
6.21%
57.08% vs 53.74%

Figure 18: Visits to the *SysSec* website.

Specifically, in Figure 19, we can see that for the unique pageviews we can see that we had a small drop of around 3%. Again the pages that dominated the pageviews were the *Publications* and *Presentations* sections. We also see much interest for the *1st SysSec Summer School*. More important, our *Associate Members* initiative was also very popular among the content.

5.4 Documents downloads

The visits to the website is a good metric for how much “visible” the project is. But it is not a very good metric to measure the overall impact of the project. A more suitable metric for this purpose would be the number of documents downloaded from the website.

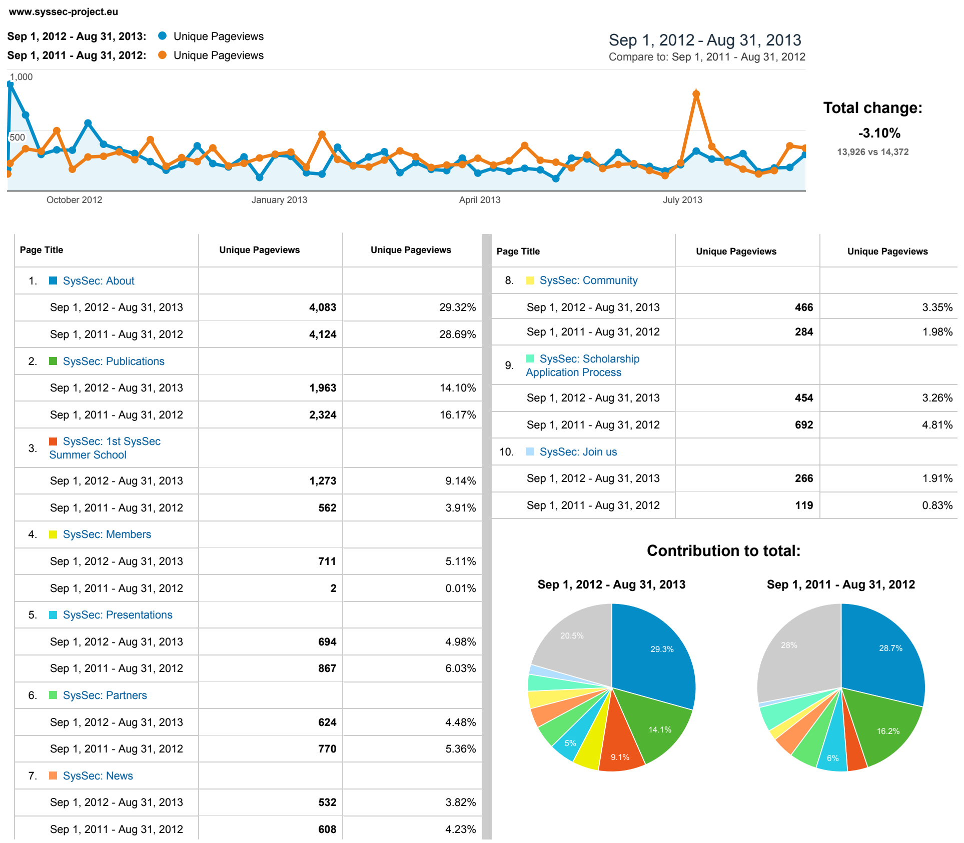
During the second year of the project a total of **42708 copies of documents were downloaded** from the *SysSec* website, out of a total of **265 published documents**. This represents **more than twice the number of downloads** we had in the second year of the project and three times the number of downloads we had in the first year.[27]

5.4.1 Downloads per document category

To gain some insight on the preferences of our website visitors we categorized the documents we made available to the following categories:

- *Publications*: *SysSec* sponsored papers published by the consortium in peer reviewed conferences and journals.

[27] All figures have been calculated using a $150min$ timeout and after having aggressively filtered out potential bots and web spiders.


www.syssec-project.eu
Sep 1, 2012 - Aug 31, 2013: ● Unique Pageviews
Sep 1, 2011 - Aug 31, 2012: ● Unique Pageviews
Sep 1, 2012 - Aug 31, 2013
Compare to: Sep 1, 2011 - Aug 31, 2012
1,000
500
October 2012
January 2013
April 2013
July 2013
Total change:
-3.10%
13,926 vs 14,372

Page Title	Unique Pageviews	Unique Pageviews
1. ■ SysSec: About		
Sep 1, 2012 - Aug 31, 2013	4,083	29.32%
Sep 1, 2011 - Aug 31, 2012	4,124	28.69%
2. ■ SysSec: Publications		
Sep 1, 2012 - Aug 31, 2013	1,963	14.10%
Sep 1, 2011 - Aug 31, 2012	2,324	16.17%
3. ■ SysSec: 1st SysSec Summer School		
Sep 1, 2012 - Aug 31, 2013	1,273	9.14%
Sep 1, 2011 - Aug 31, 2012	562	3.91%
4. ■ SysSec: Members		
Sep 1, 2012 - Aug 31, 2013	711	5.11%
Sep 1, 2011 - Aug 31, 2012	2	0.01%
5. ■ SysSec: Presentations		
Sep 1, 2012 - Aug 31, 2013	694	4.98%
Sep 1, 2011 - Aug 31, 2012	867	6.03%
6. ■ SysSec: Partners		
Sep 1, 2012 - Aug 31, 2013	624	4.48%
Sep 1, 2011 - Aug 31, 2012	770	5.36%
7. ■ SysSec: News		
Sep 1, 2012 - Aug 31, 2013	532	3.82%
Sep 1, 2011 - Aug 31, 2012	608	4.23%
8. ■ SysSec: Community		
Sep 1, 2012 - Aug 31, 2013	466	3.35%
Sep 1, 2011 - Aug 31, 2012	284	1.98%
9. ■ SysSec: Scholarship Application Process		
Sep 1, 2012 - Aug 31, 2013	454	3.26%
Sep 1, 2011 - Aug 31, 2012	692	4.81%
10. ■ SysSec: Join us		
Sep 1, 2012 - Aug 31, 2013	266	1.91%
Sep 1, 2011 - Aug 31, 2012	119	0.83%

Figure 19: Unique pageviews of the website content.

- *Presentations*: Presentations made by the consortium in events related to the project.
- *Deliverables*: The deliverables produced by the project, as outlined in the description of work document.
- *SysSec events material*: Papers, presentations as well as organization information from events organized by *SysSec*. This includes the *SysSec* summer school and workshops.
- *Other*: Everything else. This includes material from hosted events (EuroSec, DIMVA 2012, etc.), clippings from *SysSec* related articles in magazines etc.

Figure 20 shows how many documents were downloaded from each category. Again, the publications downloads are dominant, as it has happened in all the previous years. The downloads of deliverables are also going on strong, with 4545 downloads - around double the number of deliverable

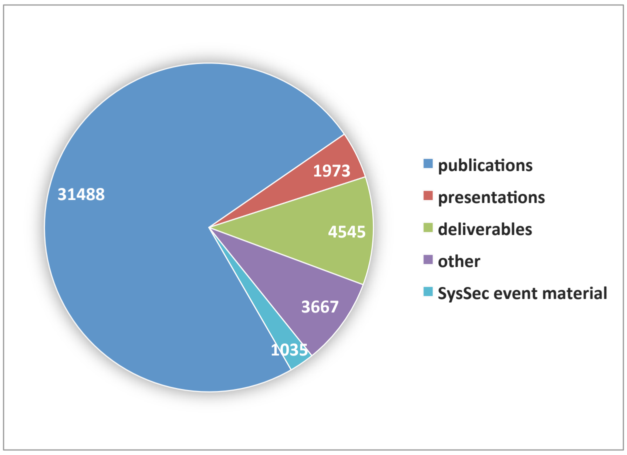


Figure 20: Downloads per document category.

downloads we had during the second year of *SysSec*. In the following figures (21, 22, 23, 24) we present the top-5 downloaded documents for each of the first four categories.

5.5 Twitter and Facebook

From the begining of the project, the consortium embraced social media as an important tool for disseminating the results of the project and building a community around the project.

During the second project year, we continued utilizing the *SysSec* Facebook page and a Twitter account[28] to disseminate event notifications, published papers and news related to the project.

The SysSec Facebook page has 191 “Likes”, whereas the Twitter feed is followed by 300 users - an increase of around 50% since last year. These figures indicate a preference amont the *SysSec* community towards the Twitter platform. In the third year of the project, we pushed *60 tweets* through these channels.

Finally, we should note that due to changes in the Twitter API there was an intermission in mirroring our tweets on our Facebook page. We have fixed this issue but in the meantime our Facebook page appeared as inactive for a while.

[28] http://twitter.com/#!/syssecproject

#	Document
1	Manuel Egele, Christopher Kruegel, Engin Kirda, Giovanni Vigna. PiOS: Detecting Privacy Leaks in iOS Applications.
2	Leyla Bilge, Engin Kirda, Christopher Kruegel, Marco Balduzzi. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis.
3	Marco Balduzzi, Jonas Zaddach, Davide Balzarotti, Engin Kirda, Sergio Loureiro. A Security Analysis of Amazon's Elastic Compute Cloud Service.
4	Christian J. Dietrich, Christian Rossow, Felix C. Freiling, Herbert Bos, Maarten van Steen, Norbert Pohlmann. On Botnets that use DNS for Command and Control.
5	Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, Herbert Bos. Paranoid Android: Versatile Protection For Smartphones.

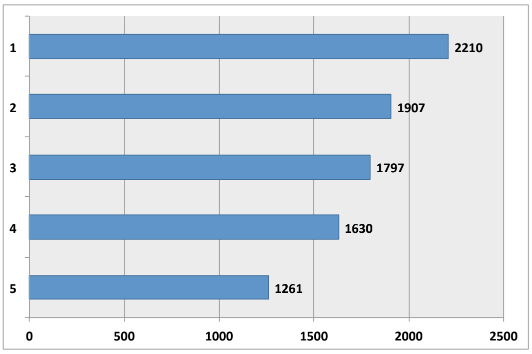


Figure 21: Top-5 downloaded *SysSec* publications.

#	Document
1	Evangelos Markatos. Managing Threats and Vulnerabilities in the Future Internet.
2	Martina Lindorfer. Lines of Malicious Code: Insights Into the Malicious Software Industry.
3	Todor Tagarev, Zlatogor Minchev, Nataliya Ivanova. Academic Research on Cybersecurity.
4	Zlatogor Minchev. Social Networks.
5	Herbert Bos. Towards Better Protection in Reverse.

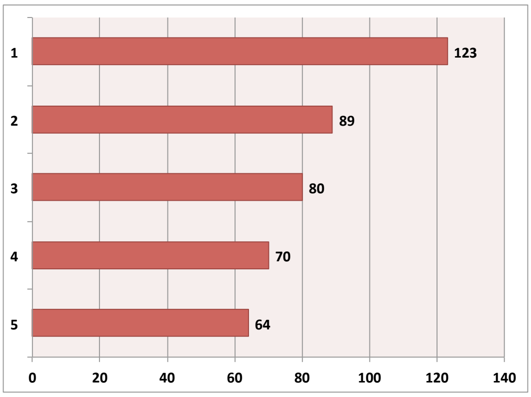


Figure 22: Top-5 downloaded *SysSec* presentations.

#	Document
1	D2.3: First Public Workshop Proceedings
2	D7.1: Review of the State-of-the-Art in Cyberattacks
3	D5.3: Case Study: Malicious Activity in the Turkish Network
4	D4.2: Second Report on Threats on the Future Internet and Research Roadmap
5	D5.2: Preliminary Report on Social Networks Security

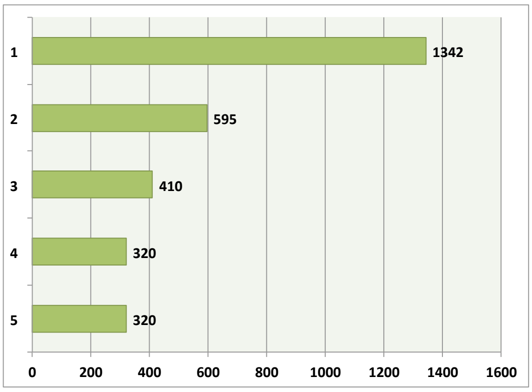


Figure 23: Top-5 downloaded *SysSec* deliverables.

#	Document
1	George Noseevich, Andrew Petukhov. Detecting Insufficient Access Control in Web Applications.
2	Angelos D. Keromytis, Salvatore J. Stolfo, Junfeng Yang, Angelos Stavrou, Anup Ghosh, Dawson Engler, Marc Dacier, Matthew Elder, Darrell Kienzle. The MINESTRONE Architecture: Combining Static and Dynamic Analysis Techniques for Software Security.
3	Jan Loeschner, Ioannis Kounelis, Vincent Mahieu, Jean-Pierre Nordvik, Pasquale Striparo, Sead Muftic. Towards a better understanding of the impact of emerging ICT on the safety and security of the Citizen.
4	Birhanu Eshete, Adolfo Villafiorita, Komminist Weldemariam. Malicious Website Detection: Effectiveness and Efficiency Issues.
5	Fernand Lone Sang, Vincent Nicomette, Yves Deswart. I/O Attacks in Intel PC-based Architectures and Countermeasures.

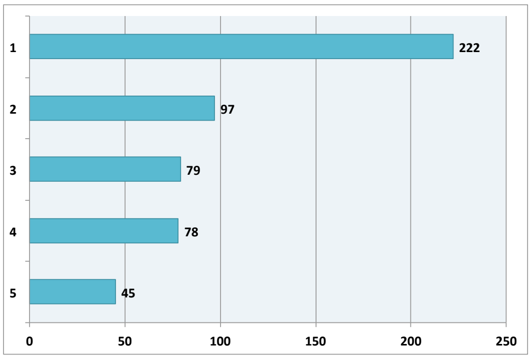


Figure 24: Top-5 downloaded documents from *SysSec* organized events.