

# Federico Maggi

UPDATED ON JANUARY 10, 2012

Politecnico di Milano  
Dipartimento di Elettronica e Informazione  
Room T.16, Building 23  
Via Ponzio 34/5  
20133 Milano- Italy

T +39 02 2399 3564  
F +39 02 2399 3411

email: [fmaggi@elet.polimi.it](mailto:fmaggi@elet.polimi.it)  
www: <http://home.dei.polimi.it/fmaggi/>

Born: June 13, 1982 in Vimercate, Milano - Italy  
Nationality: Italian



## Synopsis

I am a Post-doctorate Research Assistant at **Dipartimento di Elettronica e Informazione, Politecnico di Milano** in Italy, working at the **VPLAB** [14] with Prof. Stefano Zanero. Specifically, my current research interests are in security visualization of large-scale, malicious activity on the Internet, new security aspects of cloud-computing, malware naming inconsistencies, and automatic shoulder surfing against mobile touchscreen devices.

During my Doctorate, in the same University, I studied and made contributions in the field of *intrusion detection*: I developed and tested anomaly-based tools to mitigate Internet threats by (1) avoiding their spread via vulnerable *web applications*, (2) detecting unexpected activities in the *operating system's kernel* (sing of malware infections or compromised processes), and (3) dealing with high number of alerts using *alert correlation*.

At **Politecnico di Milano** I have been involved in teaching since I received a Bachelor Degree. During my Master of Science, I was TA for undergraduate-level courses on computer programming, I thought classes in graduate-level courses of computer and network security, as well as non-security courses, on topics such as computer system performance evaluation and information systems.

## Position and Education

### RECORD OF EMPLOYMENT

*Jan 2010 – present*

Post-doctorate Research Assistant at **Dipartimento di Elettronica e Informazione, Politecnico di Milano**.

### EDUCATION

- Doctorate *cum laude* in Information Technology at Politecnico di Milano. Jan, 2010.  
Thesis: *Integrated Detection of Anomalous Behavior of Computer Infrastructures*  
Advisor: *Prof. S. Zanero*  
Reviewer: *Prof. H. J. Bos*
- Master of Science in Computer Science Engineering. Oct 2006.  
Grade: 110/110 *cum laude*.  
Thesis: *Efficacia ed integrazione di sistemi di anomaly detection* (in Italian)  
Advisor: *Prof. G. Serazzi*  
Co-advisor: *Prof. S. Zanero*

## VISITING EXPERIENCES

- Visiting research scholar at [Department of Computer Science, University of California, Santa Barbara](#) (Sep 2008 - Jul 2009).

## SCHOOL PARTICIPATION

2008

SWING 2008 [Third Ph.D. and Researchers International School on Security for Wireless Networking](#). Bertinoro, Italy.

2007

EWSCS [13th Estonian Winter School in Computer Science](#). Palmse, Estonia.

SWING 2007 [Second Ph.D. and Researchers International School on Security for Wireless Networking](#). Bertinoro, Italy.

## SCHOLARSHIPS

- Ph.D. scholarship from M.I.U.R (Jan 2007 - Jan 2010).
- Research scholarship from Department of Computer Science (Prof. G. Vigna), University of California, Santa Barbara (Sep 2008 - Jul 2009)

## AWARDS

- AW.1. [Dimitri N. Chorafas PhD Thesis Award](#) (USD 4,000), 2010.
- AW.2. Best M.Sc. Thesis Candidate at “Premio laurea Accenture”, 2007
- AW.3. Best M.Sc. Thesis Nominee at “Premio tesi ClusIT”, 2007

# Research Statement

My research focuses on *computer security*. In particular, during my Ph.D. I studied and made contributions in the field of *intrusion detection*. More precisely, I developed and tested anomaly-based tools to mitigate Internet threats by (1) avoiding their spread via vulnerable *web applications*, (2) detecting unexpected activities in the *operating system's kernel* (sing of malware infections or compromised processes), and (3) dealing with high number of alerts using *alert correlation*. The results of such work are summarized in [10].

In the past, I also did some studies the field of theoretical computer science and contributed with the definition and implementation of a recognizer for rational *trace languages* [3, 6].

## CURRENT INTERESTS

My current research interests focus on future threats that are gaining the miscreants' attention, and thus need to be studied pro-actively. In particular, given the spread of rough anti-malware campaigns, I am studying the different malware naming schemes adopted by anti-malware software, toward creating a global map of the current knowledge about malware [2011\_maggi\_bellini\_salvaneschi\_zanero\_avnaming\_tr, 19]. Secondly, given the variety and significance of Internet threats (e.g., botnets, phishing, malware), I did contributions in the fields of security visualization, with the twofold goal of increasing user awareness and providing experts with usable investigation tools [23] (received best paper award). Then, given the spread of mobile devices, I am studying the extent to which automated shoulder surfing attacks may be used to circumvent software protections, especially against mobile touchscreen devices that expose sensitive information during typing<sup>1</sup> [2010\_maggi\_volpatto\_gasparini\_boracchi\_zanero\_clearshot]. An extended abstract describing the automated attack has been accepted for publication in the proceedings [16, 20] of the ACM CCS 2011, a top-tier security conference.

## ANOMALY-BASED INTRUSION DETECTION

Learning-based anomaly detection techniques strive to automatically construct mathematical models that characterize the canonical behavior of a computer infrastructure. The goal of such systems is to accurately detect violations as deviations from the modeled behavior. I contributed to this field with a host-based *Intrusion Detection System* (IDS) [2, 7] to detect anomalies in the sequence of operating system calls invoked by a process. In addition, I showed how the same techniques can be applied to forensic investigation and are effective even if the attacker adopted anti-forensic tools [15]. Also, I demonstrated that similar techniques can be used for detecting attacks against the web browser, the web application and the database [1, 24]. By leveraging cooperative negotiation to compute the anomaly score, as opposed to naive methods such as a weighted average, I showed that this system is resilient to attacks in the training dataset and avoids false positives caused by naive model-aggregation strategies [24]. I also showed that such tools can be trained dynamically [21]. This is particularly important for modern web applications, as they are subject to frequent changes and for which training data is often absent [22].

Future directions of this research line departs from the observations summarized in a recent study I did on the validity of the assumption that the semantic of HTTP is sufficient to detect the attacks against web applications that rely on different formats than pure HTTP (e.g., JSON, SOAP, or other RPC messages) [11, 13]. In the Web 2.0 and cloud computing era, such assumption appears to be less realistic and must be therefore relaxed to devise effective countermeasures. Indeed, the changes that brought to life the concept of “utility computing”, where network boundaries — the typical “observation point” for setting defense tools — are extremely shallow and porous today. I observed how current countermeasures (e.g., intrusion detection systems, malware detectors, anti-virus) to mitigate well-known Internet security threats, might in turn be immature for defending future infrastructures with the aforesaid characteristics.

## ALERT CORRELATION

The integration of both information sources (i.e., observed activities) and revealed anomalies (i.e., alerts), is the first step toward the development of enhanced anomaly detection techniques. Apparently trivial, the integration and the correlation of the alerts produced by heterogeneous sensors is of paramount importance for practical applications, yet is an open research problems in intrusion detection.

I have studied this topic during my Ph.D. and proposed an unsupervised approach based on a set of statistical tests, and proved that such criteria work well on a simplified correlation task, without requiring complex configuration parameters. More precisely, I developed a prototype system that treats alert streams produced by sensors as time series. In [12],

---

<sup>1</sup>I published a video demonstration of an automated shoulder surfing attack against the Apple iPhone: <http://www.youtube.com/playlist?list=PL81F91E404B928833>

I demonstrated that a Fisher statistic estimated from the samples of such time series can be effectively exploited in a hypothesis test to decide whether or not two alert streams are correlated (without prior knowledge).

Also, I focused on the aggregation of intrusion alerts, an important component of the alert correlation process. I proposed to exploit fuzzy measures and fuzzy sets to design simple and robust alert aggregation algorithms. In particular, I have studied the problem of deciding whether or not two alerts are sufficiently near (in time) so to be considered as correlated. In this decision process, constructing a sound model of the time series that represents the alerts is crucial. Instead of representing alerts as events in time, I proposed to encode them as fuzzy sets in the time domain. This simple assumption allows to exploit fuzzy measures to calculate the degree of overlapping between two fuzzy sets (i.e., the degree of correlation between two alerts). In [8], I showed that this mechanism can be applied in practice, and allows to decrease the number of alerts of several order of magnitude at the price of negligible detection errors.

I believe that alert correlation will be gaining new attention in the near future because, as explained in the previous section (and observed in [13]), attacks against global-scale infrastructures are likely to pass undetected by local protection tools. Thus, such tools will benefit from correlation mechanisms to offer an adequate level of protection.

## PHONE FRAUDS AND VOICE PHISHING

Phishing is the practice of eliciting a person's confidential information such as the name, date of birth or credit card details. Typically, phishers exploit a mixture of technologies and simple social engineering stratagems to persuade the victims into voluntarily disclose sensitive data. Phishing based on e-mail and Web technologies is certainly the most popular form. It has indeed received ample attention and some mitigation measures have been implemented. Notably, spam and phishing e-mail filters, blacklists.

I studied the *vishing* (voice phishing) phenomenon, a form of phishing where the miscreants exploit the phone channel rather than sending e-mails and cloning trustworthy websites. In [5, 9] I showed that vishing, albeit less known, is a relevant form of phishing recently on the raise. I detailed my analysis of a real-world database of vishing attacks reported by victims through a publicly-available web application that I build for this purpose. First, my preliminary analysis reveals that the vast majority of vishing activity that has been registered is targeted against U.S. customers. Second, I analyzed to what extent the criminals rely on automated responders to streamline the vishing campaigns. Third, I analyzed the content of the conversations and found that words such as "credit", "press" (a key) or "account" are fairly popular. In addition, I described the data collection infrastructure and motivate why gathering data about vishing is more difficult than for regular e-mail phishing.

## Teaching Statement

I have been involved in teaching before being awarded a Master of Science. During my master studies, I tutored undergraduate students in computer programming courses (Informatica 1) between 2005 and 2007. In what follows, this activity is referred to as Lab. Tutor as it involved guiding students in problem-solving tasks during their programming assignment in laboratory classes. Such classes are thought by Lab. *Teaching Assistants* (TAs). I was Lab. TA between 2007 and 2010 for the same computer programming courses and this required me to prepare, solve and test computer programming problems of increasing difficulty (in the ANSI C language), assign them to students, coordinate the activity of one or two Lab. Tutors, and evaluate solutions produced by students in the lab.

Since 2008 I am TA for other courses. In particular, I thought classes in computer and network security, graduate-level courses, and prepared and graded exams for such courses. I also prepared and demonstrated practical tutorial lessons (e.g., live penetration tests on testbed virtual systems) to illustrate security competitions (e.g., Capture The Flag) to the students. Also, I was TA for non-security courses on topics such as computer system performance evaluation and information systems. For these courses I was required to teach how to solve practical exercises, prepare and grade exams, and also to prepare homework and small web application for students to request assignments, submit their solutions and automate grading as much as possible.

As part of my teaching activity, I also organized a series of security-related events for students, researchers and practitioners, called "Young Hackers, Successful Security Specialists". Besides disseminating the importance of applied information security to mitigate today's Internet threats, the main aim of these events are to motivate undergraduate and graduate students. Selected Politecnico di Milano alumni with a brilliant career are invited to give technical talks about their contributions to the worldwide information security community.

In the future, my plans are to introduce cybercrime and cyber warfare as background topics in computer and network security courses. I believe this is important to spread security-awareness among students, make them understand the

economical reasons that drive the miscreants on the Internet, and, more importantly, to motivate brilliant students to do research in security.

## Publication list

### Selected publications

- [7] Federico Maggi, Matteo Matteucci, and Stefano Zanero. “Detecting Intrusions through System Call Sequence and Argument Analysis.” In: *IEEE Transactions on Dependable and Secure Computing (TODS)* 7.4 (2008), pp. 381–395. ISSN: 1545-5971. DOI: [10.1109/TDSC.2008.69](https://doi.org/10.1109/TDSC.2008.69).
- [21] Federico Maggi et al. “Protecting a Moving Target: Addressing Web Application Concept Drift.” In: *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*. (St Malo, Brittany, France). Sept. 23–25, 2009. DOI: [10.1007/978-3-642-04342-0\\_2](https://doi.org/10.1007/978-3-642-04342-0_2).
- [22] William Robertson et al. “Effective Anomaly Detection with Scarce Training Data.” In: *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. (San Diego, California, United States). Feb. 28–Mar. 3, 2010.

### Refereed international conferences

- [1] Claudio Criscione et al. “Integrated Detection of Attacks Against Browsers, Web Applications and Databases.” In: *Proceedings of the European Conference on Network Defense (EC2ND)*. (Milano, Italy). IEEE Computer Society, Nov. 9–10, 2009. ISBN: 978-0-7695-3983-6. DOI: [10.1109/EC2ND.2009.13](https://doi.org/10.1109/EC2ND.2009.13).
- [2] Alessandro Frossi et al. “Selecting and Improving System Call Models for Anomaly Detection.” In: *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*. (Como, Italy). July 9–10, 2009. DOI: [10.1007/978-3-642-02918-9\\_13](https://doi.org/10.1007/978-3-642-02918-9_13).
- [3] Federico Maggi. “A Recognizer of Rational Trace Languages.” In: *Proceedings of the International Conference on Computer and Information Technology (CIT)*. (Bradford, West Yorkshire, UK). IEEE Computer Society, June 29–July 1, 2010, pp. 257–264. ISBN: 978-0-7695-4108-2. DOI: [10.1109/CIT.2010.77](https://doi.org/10.1109/CIT.2010.77).
- [5] Federico Maggi. “Are the Con Artists Back? A Preliminary Analysis of Modern Phone Frauds.” In: *Proceedings of the International Conference on Computer and Information Technology (CIT)*. (Bradford, West Yorkshire, UK). IEEE Computer Society, June 29–July 1, 2010, pp. 824–831. ISBN: 978-0-7695-4108-2. DOI: [10.1109/CIT.2010.156](https://doi.org/10.1109/CIT.2010.156).
- [9] Federico Maggi, Alessandro Sisto, and Stefano Zanero. “A social-engineering-centric data collection initiative to study phishing.” In: *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. (Salzburg, Austria). ACM Digital Library, Apr. 10, 2011.
- [10] Federico Maggi and Stefano Zanero. “Integrated Detection of Anomalous Behavior of Computer Infrastructures.” In: *Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS)*. (Maui, Hawaii, US). Vol. (to appear). IEEE, Apr. 16–20, 2012.
- [11] Federico Maggi and Stefano Zanero. “Is the future Web more insecure? Distractions and solutions of new-old security issues and measures.” In: *Proceedings of the Worldwide Cybersecurity Summit*. (London, UK). Vol. (to appear). EWI, July 1–2, 2011.
- [12] Federico Maggi and Stefano Zanero. “On the Use of Different Statistical Tests for Alert Correlation - Short Paper.” In: *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*. (Surfer’s Paradise, Queensland, Australia). Sept. 5–7, 2007, pp. 167–177. DOI: [10.1007/978-3-540-74320-0\\_9](https://doi.org/10.1007/978-3-540-74320-0_9).
- [14] Federico Maggi and Stefano Zanero. “System Security research at Politecnico di Milano.” In: *Proceedings of the 1st SysSec Workshop (SysSec)*. (Amsterdam, The Netherlands). Vol. (to appear). IEEE Computer Society, July 6, 2011.
- [16] Federico Maggi et al. “A Fast Eavesdropping Attack Against Touchscreens.” In: *7th International Conference on Information Assurance and Security (IAS)*. (Melaka, Malaysia). Vol. (to appear). Dec. 5–Aug. 2011.
- [19] Federico Maggi et al. “Finding Non-trivial Malware Naming Inconsistencies.” In: *Proceedings of the 7th International Conference on Information Systems Security (ICISS)*. (Kolkata, India). Vol. 7093. Lecture Notes in Computer Science. Springer-Verlag, Dec. 15–19, 2011, pp. 144–159.
- [20] Federico Maggi et al. “POSTER: Fast, Automatic iPhone Shoulder Surfing.” In: *Proceedings of the 18th Conference on Computer and Communication Security (CCS)*. (Chicago, IL, US). Vol. (to appear). ACM, Oct. 15–21, 2011.

- [21] Federico Maggi et al. “Protecting a Moving Target: Addressing Web Application Concept Drift.” In: *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*. (St Malo, Brittany, France). Sept. 23–25, 2009. DOI: [10.1007/978-3-642-04342-0\\_2](https://doi.org/10.1007/978-3-642-04342-0_2).
- [22] William Robertson et al. “Effective Anomaly Detection with Scarce Training Data.” In: *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. (San Diego, California, United States). Feb. 28–Mar. 3, 2010.
- [23] Francesco Roveta et al. “BURN: Baring Unknown Rogue Networks.” In: *Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec)*. (Pittsburg, PA, US). **BEST PAPER AWARD**. New York, NY, USA: ACM, July 20, 2011, 6:1–6:10. ISBN: 978-1-4503-0679-9. DOI: [10.1145/2016904.2016910](https://doi.org/10.1145/2016904.2016910).
- [24] Alberto Volpato, Federico Maggi, and Stefano Zanero. “Effective multimodel anomaly detection using cooperative negotiation.” In: *Proceedings of the First international conference on Decision and game theory for security (GameSec)*. (Berlin, Germany). Vol. 6442. GameSec’10. Springer-Verlag, Oct. 22–23, 2010, pp. 180–191. ISBN: 3-642-17196-6, 978-3-642-17196-3.

### Refereed international journals

- [7] Federico Maggi, Matteo Matteucci, and Stefano Zanero. “Detecting Intrusions through System Call Sequence and Argument Analysis.” In: *IEEE Transactions on Dependable and Secure Computing (TODS)* 7.4 (2008), pp. 381–395. ISSN: 1545-5971. DOI: [10.1109/TDSC.2008.69](https://doi.org/10.1109/TDSC.2008.69).
- [8] Federico Maggi, Matteo Matteucci, and Stefano Zanero. “Reducing false positives in anomaly detectors through fuzzy alert aggregation.” In: *Inf. Fusion* 10 (4 2009), pp. 300–311. ISSN: 1566-2535. DOI: [10.1016/j.inffus.2009.01.004](https://doi.org/10.1016/j.inffus.2009.01.004).
- [15] Federico Maggi, Stefano Zanero, and Vincenzo Iozzo. “Seeing the invisible: forensic uses of anomaly detection and machine learning.” In: *Operating Systems Review of the ACM Special Interest Group on Operating Systems (SIGOPS)* 42.3 (2008), pp. 51–58. ISSN: 0163-5980. DOI: [10.1145/1368506.1368514](https://doi.org/10.1145/1368506.1368514).

### Technical Reports

- [4] Federico Maggi. *A Survey of Probabilistic Record Matching Models, Techniques and Tools*. TR-2008-22. Politecnico di Milano, 2008.
- [6] Federico Maggi. *Specification and Evaluation of an Efficient Recognizer for Rational Trace Languages*. TR-2008-23. Politecnico di Milano, 2008.
- [13] Federico Maggi and Stefano Zanero. *Rethinking security in a cloudy world*. TR-2010-11. Politecnico di Milano, 2010.
- [17] Federico Maggi et al. *Don't touch a word! A practical input eavesdropping attack against mobile touchscreen devices*. Tech. rep. TR-2010-59. Politecnico di Milano, 2010.
- [18] Federico Maggi et al. *Finding Non-trivial Malware Naming Inconsistencies*. Tech. rep. TR-2011-19. Politecnico di Milano, 2011.

## Teaching activities

Unless differently stated, what follows refers to undergraduate-level courses thought at the **5th School of Engineering (Ingegneria dell'Informazione)** of Politecnico di Milano.

### 2010–2011

- TA for *Dimensionamento degli Impianti Informatici (Computer Systems Performance Evaluation: Techniques and Applications)*
- TA for *Sistemi Informativi (Information Systems)*. Undergraduate-level course thought at the **2nd School of Engineering (Ingegneria dei Sistemi)** of Politecnico di

### 2009–2010

- TA for *Sicurezza delle Applicazioni (Computer Security)*. Graduate-level course thought at the **5th School of Engineering (Ingegneria dell'Informazione)** of Politecnico di Milano.
- Lab. TA<sup>2</sup> for *Informatica B (Computer Science)*. Undergraduate-level course thought at the **4th School of Engineering (Ingegneria Industriale)** of Politecnico di Milano.
- TA for *Sistemi Informativi (Information Systems)*. Undergraduate-level course thought at the **2nd School of Engineering (Ingegneria dei Sistemi)** of Politecnico di

2008-2009

- TA for *Impianti di Elaborazione (Information Systems)*. Undergraduate-level course thought at the **2nd School of Engineering (Ingegneria dei Sistemi)** of Politecnico di

2007-2008

- Lab. TA for *Informatica 1 (Computer Science)*.
- TA for *Impianti Informativi (Enterprise Digital Infrastructures)*.
- TA for *Sicurezza degli Impianti Informativi (Network Security)*. Graduate-level course thought at the **5th School of Engineering (Ingegneria dell'Informazione)** of Politecnico di Milano.

2006-2007

- Lab. Tutor for *Informatica 1 (Computer Science)*.

2005-2006

- Lab. Tutor for *Informatica 1 (Computer Science)*.

## STUDENTS' SUPERVISION

As part of my academic activities at the **5th School of Engineering (Ingegneria dell'Informazione)** of Politecnico di Milano, I supervised graduate and undergraduate students during their master and bachelor theses, respectively.

### Graduate Students Co-Advisor

- *Luca Di Mario* 2010–2011, “BURN: Baring Unknown Rogue Networks” (related paper received best paper award).
- *Andrea Bellini* 2010–2011, “Uno studio sistematico delle inconsistenze nei nomi dei malware”
- *Manuel Fossemò* 2010–2011, “Automated Collection and Analysis of Runtime-Generated Strings in a Web Browser”
- *Alberto Volpatto* 2009–2010, “Negoziazione cooperativa e meccanismi adattativi per mitigare gli attacchi contro le applicazioni web”
- *Lorenzo Peri* 2009–2010, “Metodi K-nearest-neighbor per la rilevazione automatica di attacchi informatici”
- *Matteo Debiassi, Matteo Falsitta* 2006–2007, “Reingegnerizzazione ed ottimizzazione di un sistema di anomaly detection host based”

### Undergraduate Students Co-Advisor

- *Luca Visentin, Stefano Todisco* 2009–2010, “Pcapstat: un sistema per supportare l'analisi del traffico di rete”
- *Marco Clerici, Mattia Sasso* 2009–2010, “Analisi Sperimentale delle vulnerabilità di Google reCAPTCHA”
- *Marco Lancini* 2009–2010, “FacePrivacy”
- *Eros Lever* 2009–2010, “Un sistema di raccolta dati per lo studio delle minacce celate dagli URL brevi”
- *Alessandro Rizzi, Stefano Schiavoni* 2009–2010, “WebLorica: Un framework per lo sviluppo di anomaly detection system per applicazioni web”

---

<sup>2</sup>Lab. TA refers to teaching assistantship for laboratory activities (e.g., computer programming).

- *Simone Benefico, Andrea Colombo* 2009–2010, “Reingegnerizzazione di un riconoscitore automatico di attacchi di rete”
- *Erika Gressi* 2008–2009, “Apprendimento e simulazione dell’attività di un utente mediante l’utilizzo di modelli semi-markoviani nascosti”
- *Matteo Michellini* 2007–2008, “Kernel auditing su Linuxn 2.6 in formato OpenBSM”
- *Pietro Testa* 2006–2007, “Valutazione automatica delle performance di sistemi di anomaly detection”
- *Claudio Magni* 2006–2007, “Analisi e test automatizzati di sistemi di anomaly detection network-based”

## Talks

- “Are the con artists back? Some thoughts about phone scams” at the IEEE Symposium on Security and Privacy, Berkeley/Oakland, California, United States. May, 2010. ([Slides](#))

### INVITED TALKS

- “SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet.” at Effectsplus informal session in FIA Ghent, Ghent, Belgium, December 2010. ([Slides](#))
- “Detecting Anomalous Behaviors in Computer Infrastructures” at Fondazione Bruno Kessler, Trento, Italy. Feb 25, 2010 ([Slides](#))
- “Just-in-Time Training of Anomaly Detectors” at the Computer Systems Seminar, Vrije Universiteit Amsterdam, The Netherlands. Jan 21, 2010 ([Slides](#))

## Service

### TECHNICAL PROGRAM COMMITTEE

- 7th ENISA European Conference on Network Defense (EC2ND 2011).
- First SysSec Workshop (SysSec 2011).
- Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2011).

### REFEREE SERVICES

I have served for the following conferences and journals as a reviewer (or external reviewer).

- Journal in Computer Virology (Springer)
- IEEE Intl. Conf. on Complexity in Engineering (COMPENG 2010)
- 5th ENISA European Conf. on Network Defense (EC2ND 2009)
- Fifth Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2008)
- International Journal of Information Security
- ACM Transactions on Information and System Security

## CONFERENCE AND WORKSHOP ORGANIZATION

- Publication and Publicity Chair for the 7th ENISA European Conference on Network Defense (EC2ND 2011).
- Publication and Publicity Chair for the First SysSec Workshop (SysSec 2011).
- Publication Chair for the International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2011).
- Publicity Chair for the IEEE Intl. Conf. on Complexity in Engineering (COMPENG 2010).
- Publicity Chair for the 5th ENISA European Conference on Network Defense (EC2ND 2009).

## FUNDED RESEARCH PROJECTS

My research has been supported by the following EU-sponsored projects, in which I am actively involved under the supervision of Prof. S. Zanero and Prof. G. Serazzi.

- *WOMBAT*, EU STREP FP-7 - <http://www.wombat-project.eu>
- *SysSec*, EU NoE FP-7 - <http://www.syssec-project.eu>
- *i-Code*, CIPS - <http://www.icode-project.eu/>
- *SCADA-NG*, NATO SCIENCE FOR PEACE - [http://www.fer.hr/NATO\\_SNG/](http://www.fer.hr/NATO_SNG/)

## References

**Professor Christopher Krügel** <[chris@cs.ucsb.edu](mailto:chris@cs.ucsb.edu)>

1117 Engineering I  
Department of Computer Science  
University of California, Santa Barbara  
Santa Barbara, CA 93106, United States

**Professor Giovanni Vigna** <[vigna@cs.ucsb.edu](mailto:vigna@cs.ucsb.edu)>

2159 Engineering I  
Department of Computer Science  
University of California, Santa Barbara  
Santa Barbara, CA 93106, United States

**Professor Herbert Bos** <[herbertb@cs.vu.nl](mailto:herbertb@cs.vu.nl)>

Computer Systems Section  
Vrije Universiteit Amsterdam  
De Boelelaan 1081  
1081 HV Amsterdam