

# Tadeusz Pietraszek



Alte Landstrasse 70  
8803 Rüslikon  
Switzerland  
+41 76 394 2998  
tadek@pietraszek.org  
<http://tadek.pietraszek.org>

*This resume is available online at <http://tadek.pietraszek.org/resume.pdf>*

- EDUCATION
- ◇ **Univeristy of Freiburg (exernal student)**, Freiburg, Germany (2004–2006)
    - Ph.D. in Computer Science (Dr. rer. nat.), Dec 2006.
    - Ph.D. Thesis: *Alert Classification to Reduce False Positives in Intrusion Detection*.
    - Advisor: Prof. Luc De Raedt
  - ◇ **Silesian Univeristy of Technology**, Gliwice, Poland (1997–2002)
    - M.Sc. Eng. in Computer Science (mgr inż.), June 2002.
    - M.Sc. Thesis: *Smart Sensor in Wide Area Network Environment (in Polish)*
    - Grade: very good with distinction
  - ◇ **The Nottingham Trent University**, Nottingham, U.K. (Jan–Jul 2000)
    - Socrates Erasmus Exchange Student
  - ◇ **Matriculation Exam**, 1997
    - Polish: 4—good, Maths: 6—excellent, English: 6—excellent.
- EXPERIENCE
- ◇ **Software Engineer**, Google, Zurich, Switzerland (Sept 2006–NOW)
    - Gmail Spam and Abuse Teams: Using security and machine-learning expertise to improve spam classification and abuse detection.
    - Search Quality: Improving Onebox quality.
  - ◇ **Doctoral Researcher**, Global Security Analysis Laboratory, IBM Zurich Research Laboratory, Zurich, Switzerland (Feb 2003–Sept 2006)
    - Worked towards PhD in the topic of the application of machine learning techniques to reduce false positives in intrusion detection
      - Research into false positives in intrusion detection.
      - Proposed a novel technique with an automatic classifier trained based on analyst’s feedback (see RAID’04 paper)
      - Research into background knowledge useful for intrusion detection.
      - Research into cost-sensitive metaclassification and abstaining classifiers using ROC analysis.
      - Proposed a novel and efficient algorithm for constructing optimal abstaining classifier (see ICML’05 and MLJ’07 paper)
      - Developed ALAC, a prototype alert classification system and validated it on numerous real and synthetic data sets.

- Working with an active Security Operations Center in Boulder, CO on the application of machine learning and existing data mining techniques in a two-stage alert classification to reduce analyst's load and ensure classification consistency.
- Defended my PhD at the University of Freiburg, Germany. Advisor: Prof. Dr. Luc De Raedt.
- Developed CSSE, a novel technique for preventing injection attacks in PHP based applications.
  - Performed an in-depth analysis and categorized the root causes of existing and future injection attacks.
  - Proposed CSSE, a novel technique based on precise tainting to prevent injection attacks.
  - Developed a prototype of CSSE by modifying PHP engine and validated in on real injection attacks.
  - Co-authored a paper on CSSE accepted to RAID2005.
  - Co-authored two patent applications based on ideas behind CSSE.
  - CSSE is currently in the process of being transferred to Zend.
- Worked on an undisclosed security product.
  - Participating in the high-level product design.
  - Responsible for the design on the database schemas and component (intrusion detection systems and vulnerability scanner) integration.
  - Designed, built and maintained the 'living lab', a secluded network for security testing. Managed vulnerabilities and scripted attacks.
  - In charge of automated system and installation tests.
- ◇ **Research Assistant/Doctoral Student**, Institute of Computer Science, Silesian Technical University, Gliwice, Poland (Oct 2002–Feb 2003)
  - Co-author of two publications on the security of web applications.
  - TA for a security of web applications course.
- ◇ **Extreme Blue Internship**, IBM Zurich Research Laboratory, Zurich, Switzerland (Jul 2002–Sep 2002)
  - A Booster Box Application for Floating Car Data.
  - Development of Java Application to demonstrate Booster Box operation with car telematics system and traffic prediction application.
- ◇ **Master Thesis: *Smart sensor in wide area network environment***, Silesian University of Technology and ATEST-Gaz, Gliwice, Poland (Feb 2002–Jun 2002)
  - Research into sensor networks and monitoring systems.
  - Design and implementation of real-time distributed monitoring system.
  - Application of embedded Java system and relational databases.
  - Based on thesis and developed software and hardware, system is currently manufactured and sold in Poland by company ATEST-Gaz.
- ◇ **Designer of electronic car security systems and other microprocessor driven projects**, company STER, Chorzów, Poland (Sep 2000–Feb 2002 (contracting))
  - Writing an assembler program for PIC processor, operating car security system. It has got insurance companies' certificates and is produced and sold in Poland (hundreds items/month).
- ◇ **Student Internship**, Technology Risk Consulting, Arthur Andersen, Warsaw, Poland (Feb 2002–Mar 2002)

- Taking part in Network Security Review project.
  - Dealing with CISCO routers and firewalls installation and configuration.
  - ◇ **Student Internship**, Hewlett-Packard, Warsaw, Poland (Sep 2001)
    - Analyzing and preparing the comparison of medium sized disk arrays.
  - ◇ **Network Administrator**, Amateur Computer Network “Albatros” (Oct 2000–Dec 2002)
    - Co-founder of Amateur Computer Network. Member of the Amateur Computer Networks Society.
    - Responsible for configuration and administration of Linux server.
    - Assistance in configuring and troubleshooting of client stations (40 computers).
  - ◇ **A research project *Investigation of microscopic traffic simulations***, RTTS and Modelling Group, The Nottingham Trent University, U.K. (Feb 2000–Jul 2000)
    - Investigation into traffic measurements and simulation techniques.
    - Analyzing and integrating existing simulation software with real-time data.
  - ◇ **Designer of an electronic gas detector**, Company ATEST-gaz, Gliwice, Poland (Sep 1999–Dec 1999 (contracting))
    - Research into methane and carbon monoxide sensors and writing an appropriate PIC software (PIC microcontroller)
- HONORS AWARDS
- ◇ Medal and award for the best of graduates “Omnium Studiosorum Optimo” (2002)
  - ◇ Polish Ministry of Education Scholarship (separate awards granted in the following years: 1999, 2000, 2001)
  - ◇ Hugo Kołłątaj Fund Scholarship (2001)
  - ◇ Good results in International Collegiate ACM Programming Contest, Prague, Czech Republic (1999, 2000)
  - ◇ Good results in National Collegiate Programming Contest, Warsaw, Poland (1999, 2000)
  - ◇ Dean’s prize (1998, 1999)
  - ◇ National Olympic in Maths—a finalist (1997)
  - ◇ Polish Children’s Fund Scholarship (1993-1995)
- SKILLS CERTIFICATES
- ◇ Languages: Polish (mother tongue), English (fluent), German (intermediate)
  - ◇ Computer languages: Java (fluent), C/C++ (fluent), R, PHP, Delphi, MFC, Perl, Python, Assembler PIC (embedded processor)
  - ◇ Network/System Administrator with focus on Security
  - ◇ CISSP (Certified Information Systems Security Professional)
  - ◇ Linux, OSX, Windows 2000/XP, Cisco IOS
- SELECTED PUBLICATIONS
- All publications can be downloaded from: <http://tadek.pietraszek.org/publications.html>
- ◇ **Conferences & Journals**
    - Tadeusz Pietraszek. *On the use of ROC analysis for the optimization of abstaining classifiers*. Machine Learning Journal, Volume 68(2), pages 137–169, 2007.
    - Tadeusz Pietraszek. *Classification of intrusion detection alerts using abstaining classifiers*. Intelligent Data Analysis Journal, Volume 11(3), pages 293–316, 2007.
    - Tadeusz Pietraszek, Axel Tanner. *Data Mining and Machine Learning—Towards Reducing False Positives in Intrusion Detection*. Information Security Technical Report Journal, Volume 10(3), pages 169–183, 2005.

Tadeusz Pietraszek, Chris Vanden Berghe. *Defending against Injection Attacks through Context-Sensitive String Evaluation*. In Recent Advances in Intrusion Detection (RAID 2005), volume 3858 of Lecture Notes in Computer Science, pages 124–145, Seattle, WA, 2005. Springer-Verlag.

Tadeusz Pietraszek. *Optimizing Abstaining Classifiers using ROC Analysis*. In Proceedings of 22nd International Conference in Machine Learning (ICML 2005), pages 665-672, Bonn, Germany, 2005.

Tadeusz Pietraszek. *Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection*. In Recent Advances in Intrusion Detection (RAID2004), volume 3324 of Lecture Notes in Computer Science, pages 102-124, Sophia Antipolis, France, 2004. Springer-Verlag.

◇ **PhD. Thesis**

Tadeusz Pietraszek. *Alert Classification to Reduce False Positives in Intrusion Detection*. PhD Thesis. University of Freiburg, 2006.

◇ **M.Sc. Thesis**

Tadeusz Pietraszek. *Inteligentny Czujnik w Strukturze Sieci Rozległej (in Polish)*. M.Sc. Thesis. Silesian University of Technology. Gliwice, 2002.

REFERENCES    On request.