Resumé
Till Stegers

Personal Data

Born in 1979 in Dortmund, Germany.

Education and Research Experience

A German grading scale is provided at the end of this document.

since 09/2005	PhD Candidate Dept. of Computer Science, University of California, Davis. Advisor: Phillip Rogaway. Research topics: Relating formal and computational cryptography; practical and provably-secure cryptographic protocols. GPA 3.93 on a 4.00 scale.
10/2003–09/2005	*Diplom-Mathematiker (Mathematics with Computer Science)* Technische Universität Darmstadt, Darmstadt, Germany. Graduated with distinction. GPA 1.07. Advisor: Johannes Buchmann. Topic: Analysis and implementation of Faugère's F_5 algorithm for computing Gröbner bases
07/2002–08/2003	*Master of Science (Mathematics)* Tulane University, New Orleans, LA. GPA 3.91 on a 4.00 scale. Advisor: Michael W. Mislove. Topic: Survey of degeneracy results for models of the untyped lambda calculus.
10/1999–07/2002	*Bachelor of Science (Mathematics with Computer Science)* Technische Universität Darmstadt. Grade 1,0 (A) in both exams. Advisor: Michael Wüstner. Topic: Discussion of several state-of-the-art algorithms for discrete logarithms.

Publications

12/2006 — *Computational Soundness of Formal Indistinguishability and Static Equivalence*, with Gergei Bana and Payman Mohassel. 11th Annual Asian Computing Science Conference, Tokyo, Japan, December 2006. To appear in the Lecture Notes in Computer Science series, Springer-Verlag.

11–12/2005 — *Security Analysis of the eVACS Open-Source Voting System* Security audit of the open-source e-voting software eVACS (with A. Das, Y. Niu). Utilized the static analysis toolkits *Flawfinder* and *Fortify Source Code Analysis Suite*. No compromising vulnerabilities were found, but a number of flaws in the engineering process identified. Manuscript, 2005.

Professional Experience

06/2006–09/2006 — Engineering Intern at *Coverity, Inc.*, San Francisco. Extended Coverity's static analysis tool for Java by a specification miner that extracts design contracts from source code to enable static checking of custom protocols. Also implemented models for Coverity's C/C++ checker and helped test its alpha release.

11/2003–09/2004 — Developer for *Danet GmbH* (Weiterstadt, Germany) in TU Darmstadt's Software Engineering practicum. Worked in a team of seven students to develop a highly reliable J2EE application for the transfer of billing data from telecommunication providers. Responsibilities included design, Java programming, testing, documentation, and project management. Product is expected to be deployed in mission-critical systems according to *Danet* officials.

09/2005–06/2006
10/2003–09/2004
08/2002–05/2003 — Teaching Assistant at UC Davis, (Dept. of Computer Science), TU Darmstadt (Dept. of Mathematics), and Tulane University (Department of Mathematics) . Taught discussion sessions for undergraduate classes such as *Computer Security, Discrete Mathematics, Calculus.* Graded exams. Held office hours. Lectured occasionally.

Programming Languages & Computer Skills

- Java and J2EE, Magma, C, Matlab, LISP, Scheme, Python, ObjectPascal
- Software engineering techniques and methodologies, security audits, static analysis
- UNIX (esp. Linux), Windows, and Mac OS environments; Subversion, BitKeeper, Eclipse, JUnit, Cactus, Clover, Cruise Control, Ant, XML, ...
- LaTeX, MS Office, InDesign, Illustrator, Photoshop

Scholarships, Honors, Activities

Merit-based Scholarships: Department Block Grant (UC Davis, Winter 2007), Tulane University (2002/2003), *Stiftung der Deutschen Wirtschaft* (Foundation of the German Economy, 2001–2005), *e-fellows.net* (since 2001).

Academic activities: Former Member of both Academic Senate and Student Parliament of TU Darmstadt; Member of Faculty Hiring Committee, Dept. of Mathematics, TU Darmstadt.

German Grading Scale

German numeric	1,0	1,3	1,7	2,0	2,3	2,7	3,0	3,3	3,7	4,0	5
German verbal	excellent		good			satisfactory			passed		fail
4.0 scale	4.00	3.67	3.33	3.00	2.67	2.33	2.00	1.67	1.33	1.00	0.00