

Johannes Schlumberger

Education

- September 2011–May 2013 **PhD Student**, *University of California Santa Barbara*, Santa Barbara, GPA: 3.98.
At the security lab with Christopher Kruegel and Giovanni Vigna. Courses in: Cloud computing, Distributed Systems, Cryptography, Program Analysis, Computer Architecture, Operating Systems, Approximative Algorithms and Security.
- October 2010–September 2011 **Visiting Researcher**, *University of California Santa Barbara*, Santa Barbara.
- 2004–October 2010 **Diploma (Master eqv.)**, *Friedrich-Alexander-Universität*, Erlangen, Grade 1.1 (excellent).
Computer Science major (specialized in Computer Architecture, Compiler Construction, Operating Systems and System Security), Astrophysics minor
- 2004–2008 **Intermediate Diploma**, *Friedrich-Alexander-Universität*, Erlangen.
Computer Science major, Medical Computer Science minor

Vocational

- 2016– **Staff Software Engineer**, *Appfolio Inc.*, Santa Barbara.
- 2013–2016 **Sr. Software Engineer**, *Appfolio Inc.*, Santa Barbara.
- 2010–2013 **Research Assistant**, *UCSB Security lab.*, Santa Barbara.
Main focus on anonymity networks, malware analysis and detection as well as analyzing Android applications.
- 2005–2010 **System Administrator**, *Friedrich-Alexander-Universität*, Erlangen.
As a system administrator at the computer science department I was part of a small team of students responsible for the hard- and software in the computer rooms. The roughly 170 workstations and thin clients are mostly Linux-based as are the dozen servers. These machines are used by roughly 4700 users. I was responsible for all the services and installation as well as network operations and user support. Multiple administration tools were programmed by me during this time. Planning the purchase of new hardware was our responsibility, too.

Academic activities

- I2P attacks Paper on practical attacks on the I2P anonymity system. (in submission).
- Jarhead Paper on analyzing and detecting malicious Java applets. (accepted ACSAC'12).
- BacaTec Grant 2012/13 EUR 7000 (~\$10 000) grant for research on distributed anonymity systems.
- Parallelizing MD5 Student paper exploiting SSE Instructions to recover MD5-digested pass-phrases.
- Defcon CTF Participation Finalist at the Defcon capture the flag competition 2011 and 2012.
- iCTF Organization Co-organizer of the iCTF capture the flag competition (largest life IT-security exercise in the world) 2010 and 2011.

- Appointment committee In 2007 I was the student representative in an appointment committee.
- Lectures On several occasions I gave lectures as a stand-in. The topics were partly prepared by me.
- Mentor I acted as a mentor for beginning students and helped with various introductory courses.
- Private lessons For four years I have been giving private lessons in computer science and math.

Student research project

- Title *Breaking MIFARE security in real world applications*
- Supervisors Wolfgang Schröder-Preikschat, Michael Gernoth
- Description I showed that today's real world MIFARE applications are susceptible to a broad range of attacks. I developed and documented these attacks and partly executed them in practice. Targeted applications ranged from train tickets or payment systems to an access control system.

Diploma thesis

- Title *Implementing the Phantom Protocol*
- Supervisors Wolfgang Schröder-Preikschat, Michael Gernoth
- Description I have implemented a prototype for the Phantom Anonymity Protocol. The Phantom Anonymity Protocol was developed by Magnus Bråding to provide anonymity optimized for the current conditions and needs of the average Internet user.

Computer skills

System security and Cryptography	research experience, professional knowledge and practical experience	Operating Systems	professional knowledge and practical experience implementing a small operating system on x86
Compiler Construction	theoretical knowledge and practical experience implementing a compiler with basic optimization techniques for a Pascal-like language	Computer Architecture	professional theoretical background
Virtual Machines	professional theoretical knowledge and practical experience implementing a basic x86 emulator	Linux Administration	professional knowledge and 5 years work experience
Programming Languages	very good knowledge of C, Ruby, Java, Bash, Assembly, sound knowledge of Scala, Python, C++, Perl, basic knowledge of Scheme, Prolog, Fortran. Research experience in static analysis, professional theoretical background in abstract interpretation.	Cloud Computing	professional theoretical background and some practical experience building a toy scalable web application and deploying it using Rightscale.

Languages

- German native language, text and speech
- English fluent, text and speech
- Russian basic knowledge, text and speech