



26th Crypto-Day

June 01 and 02, 2017

Maxfeldstr. 5, Eingang Rollnerstraße, Nuremberg, Germany

On June 01 and 02, 2017, the interest group “Angewandte Kryptographie” of Gesellschaft für Informatik e. V. will host the twenty-sixth *Crypto-Day*.

Ambition and Program: The Crypto-Day aims at providing an opportunity for early-stage researchers in the field of cryptography and IT-security to exchange knowledge and establish networks to universities as well as to industry (e.g. for collaboration across Germany, or to find out about research internships and post-doc positions). Therefore, we invite students, doctoral candidates, and experienced researchers to present their research results or research ideas in the form of 20 minute presentations on this upcoming Crypto-Day.

Schedule (tentative)

Thu 13:00-17:00 Talks
Thu 17:10-17:55 GI Fachgruppentreffen
“Angewandte Kryptographie”
Thu 18:00-22:00 Excursion and dinner
Fri 09:00-13:00 Talks

Host: SUSE will host the event and provide insights into the security challenges of developing and maintaining software solutions used by other companies worldwide to run mission critical deployments. For that the SUSE security team stays on top of current security threats and provides our

customers with security updates even for very old code.

OpenSSL is a critical piece of software that SUSE maintains for its customers. As part of the Crypto-Day we will explain the challenges of maintaining such a crucial software component for a long time (up to 13 years).

Topics: The presented talks shall cover a broad spectrum from the field of cryptography or IT-security. We invite presentations of work-in-progress, contributions, which may be submitted to a conference, or summarize findings from a thesis or dissertation.

Submitted articles corresponding to the presentations will be arranged in a technical report. Therefore, submissions will be quotable publications and will be published on the web page. Observe that this does not forbid the publication of the result at other conferences or journals.

Attendance: There are **no participation fees**.

Submission: Please submit an abstract of your talk (**one DIN A4 page**). To simplify generation of the technical report, we request you to only use the LaTeX template of the cryptography group and to provide the PDF file additionally to the LaTeX sources.

Further Information (Program, Venue, LaTeX-template): <http://www.kryptotag.de/>

Submission/Registration: Until **May 22, 2017** per email: kryptotag@lists.bit.uni-bonn.de

Organisation: Johannes Segitz, SUSE
Michael Nüsken, Universität Bonn
Frederik Armknecht, Universität Mannheim