Seventeenth Workshop on Fault Diagnosis and Tolerance in Cryptography

Sept 13-th, 2020 • Virtual Workshop

(co-located with CHES 2020)

FDTC 2020 is held in cooperation with IACR

Fault injection is one of the most exploited means for extracting confidential information from embedded devices and for compromising their intended operation. Therefore, research on established as well as upcoming methodologies, and techniques for fault injection, architectures and design tools for the design of robust and protected cryptographic systems and embedded devices (both hardware and software), are essential. Fault injection case studies on popular categories of embedded devices like mobile phones, industrial control devices, hardware wallets for cryptocurrencies, security tokens, etc., are of high interest to improve the understanding of the implications on realistic applications.

FDTC is the reference event in the field of fault injection appliances, fault attacks and countermeasures

Topics of interest include but are not limited to:

- Fault injection setups and praxis:
  - novel and improved mechanisms for fault injection, e.g., using lasers, electromagnetic induction, or clock / power supply manipulation
  - practical issues in fault injection setups and validation results
  - practical limitations of attacks and implications for security
- Case studies:
  - attacks on cryptographic implementations
  - attacks on embedded devices like mobile phones, industrial control devices, hardware wallets for cryptocurrencies, security tokens, smartcards, etc.
  - validation of earlier results
- Related highly-invasive attacks on device security:
  - setups and practical results from invasive attacks, such as photonic emission analysis, laser thermal imaging, laser-voltage imaging, etc.
  - practical issues, limitations and potential
- Countermeasures (detection, resistance and tolerance):
  - countermeasures for cryptographic implementations
  - countermeasures for firmware of embedded devices, e.g., for bootloaders
  - detection countermeasures, e.g., control flow integrity
  - HW/SW co-design countermeasures for CPU architectures
- Design tools for analysis of fault attacks and countermeasures:
  - early estimation of fault attack robustness
  - automatic applications of fault countermeasures

Instructions for authors

Submissions must not substantially duplicate work that any of the authors have published elsewhere or that has been submitted in parallel to any other conference or workshop. Submissions should be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Papers should be up to 8 pages (including the bibliography and appendices), and must be formatted following the instructions in the provided template.

Authors may opt for an early submission with rebuttal. See the important dates.

The submission of final papers will be managed by Conference Publishing Services (CPS). CPS will directly contact the authors with instructions and will send links for uploading the manuscripts.

Accepted papers will be published in an archival proceedings volume by CPS and will be distributed at the time of the workshop.

At least one author of each accepted paper must register for the workshop and present the paper in order to be included in the proceedings. Additional submission instructions and further information can be found at:

`fdtc-workshop.eu`

Program chairs

Tim Güneysu *Ruhr-Uni. Bochum & DFKI*
Colin O'Flynn *NewAE & Dalhousie Uni.*

Program committee

Michel Agoyan *ST Microelectronics*
Josep Balasch *KU Leuven*
Lejla Batina *Radboud University*
Guido Bertoni *Security Patterns*
Shivam Bhasin *NTU Singapore*
Luca Breveglieri *Politecnico di Milano*
Ileana Buhan *Riscure*
Fabrizio De Santis *SIEMENS AG*
Jean-Max Dutertre *ENS Mines S. Etienne*
Junfeng Fan *Open Security Research*
Wieland Fischer *Infineon AG*
Jorge Guajardo *Bosch US*
Sylvain Guilley *Telecom ParisTech*
Johann Heyszl *Fraunhofer Institute*
Mehran M. Kermani *University of South Florida*
Osnat Keren *Bar Ilan University*
Israel Koren *University of Massachusetts*
Heiko Lohrke *TU Berlin*
Philippe Loubet Moundi *Gemalto*
Debdeep Mukhopadhyay *IIT Kharagpur*
Dmitry Nedospasov *Keylabs*
David Oswald *University of Birmingham*
Gerardo Pelosi *Politecnico di Milano*
Ilia Polian *University of Passau*
Robert Primas *TU Graz*
Falk Schellenberg *Ruhr-Universität Bochum*
Sergei Skorobogatov *University of Cambridge*
Takeshi Sugawara *UEC Tokyo*
Junko Takahashi *NTT*
Shahin Tajik *University of Florida*
Hugues Thiebeauld *eShard*
Michael Tunstall *Cryptography Research*
Vincent Verneuil *NXP Semiconductors*
Fan Zhang *Zhejiang University*

Chairs (general, publication, finance)

Guido Marco Bertoni *Security Pattern*
Luca Breveglieri *Politecnico di Milano*
Israel Koren *University of Massachusetts*

Steering committee

Luca Breveglieri *Politecnico di Milano*
Israel Koren *University of Massachusetts*
David Naccache (chair) *ENS Paris*
Jean-Pierre Seifert *TU Berlin & T-Labs*

Important dates (2020)

Submission with rebuttal:	June 1
Submission without rebuttal:	June 22
Resubmission after rebuttal:	July 6
Notification final acceptance:	July 31
Final version (camera-ready):	Aug. 14
Workshop:	Sept. 13