# Cryptacus Newsletter

## April-May 2018 Cryptacus Newsletter

*Welcome to the April-May 2018 edition of the monthly Cryptacus.eu newsletter, offering a glimpse into recent developments in the cryptanalysis of IoT & related areas. Send your contributions, comments & feedback at cryptacus.newsletter@irisa.fr*

## News from the Chair

by GILDAS AVOINE

Dear Cryptacus Members,

April has been an important month for the Cryptacus community. Mainly because of the organization of two important events in São Miguel, namely the Cryptacus training school organized by Ricardo Chaves (PT), and a workshop on distance-bounding protocols (Cryptacus COST Action & Popstar ERC Grant) mostly organized by Ioana Boureanu (UK) and Stéphanie Delaune (FR).

More than 70 people have been funded to attend the events, which have been amazingly successful according to the feedback and comments I received from the attendees.

I would like to use this opportunity to kindly thank the organizers, including Ricardo's colleagues and students, who greatly contributed to make this event successful.

Looking now to the future, I can announce that the new Grant Period will start on time, namely on May 1st, 2018.

You can already apply for STSMs and ITC Grants, to be held between May 1st and December 11th, which is unfortunately already the end of our COST Action.

The number of applications we receive roughly doubled from one grant period to another one.

The last period may, consequently, be more competitive for applicants.

Last grant period also means we are now working on the organisation of the last conference. It will be held in Rennes (France) on September 18th-20th, 2018. The website is already up (`https://www.cryptacus.eu/en/conference/`) but programme and traveling information are not available yet. MC Members will likely receive their official invitation in May.

The list of speakers is not completed yet, but promises to be stellar. I can announce the confirmed ones: Lejla Batina, Milena Djukanovik, Orr Dunkelman, Aurélien Francillon, Kevin Fu, Flavio Garcia, Daniel Gruss, Claudio Orlandi, Bart Preneel, and Ingrid Verbauwhede.

The full list will be provided in the next newsletter.

Best regards,

**Gildas Avoine**

## Recommended reading: Practical Fault Injection on Deterministic Signatures: The Case of EdDSA

The recommending reading of the month is a joint work by Niels Samwel and Lejla Batina from Radboud University, Nijmegen.

It is particularly timely after recent vulnerabilities of popular implementations of deterministic signatures schemes such as EdDSA have been attacked, showing that the secure deployment of these algorithms will require more countermeasures than originally though.

The paper shows, in addition, that the realistic implementation of these additional countermeasures is far from trivial as the authors proposed certain checks as a countermeasure but the implementation under analysis remained vulnerable to fault injection attacks.

The authors present simple attacks against the EdDSA implementation in the lightweight cryptographic library WolfSSL on a 32-bit microcontroller, achieving success rates of almost 100% by voltage glitching and electromagnetic fault injection.


The paper was accepted to Africacrypt 2018, and can be accessed here `https://goo.gl/4ZPacb`.

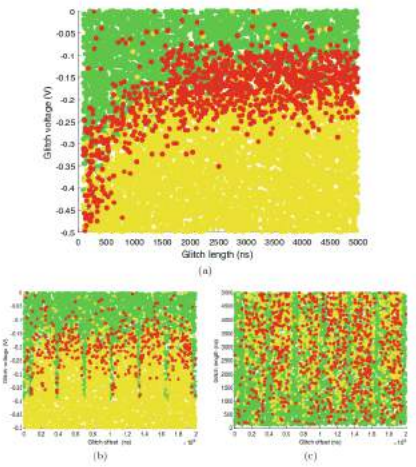
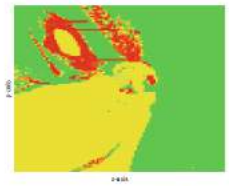



**Fig. 4.** Voltage fault injection results, Normal (green), Inconclusive (yellow), Successful (red). (Color figure online)

They conclude that, as only a single successful fault is needed to fully recover the key, this kind of implementation is a particularly easy target for the attackers.

(a) Target board



(b) Heat map with EMFI results

**Fig. 5.** This figure shows a picture of the board and it shows which locations are most effective to inject a glitch.

## Open Positions


Please send us any employment opportunities you may want to publicize in the newsletter.

- Chair in Computer Science at the University of Liverpool's Department of Computer Science. A permanent and full time position at the highest level. They mention in the ad security as one of their priority topics. The closing date for applications is the 11 May 2018. More info at `http://www.jobs.ac.uk/job/BIS200/chair-in-computer-science/`

UNIVERSITY OF LIVERPOOL Athena SWAN Silver Award

- A position as (full) professor of Computer Science is available as soon as possible at the Department of Computer Science, Aarhus University (`www.cs.au.dk`). The department has research groups within 'Algorithms and Data Structures', 'Data-Intensive Systems', 'Cryptography and Security', 'Mathematical Computer Science', 'Logic and Semantics', 'Ubiquitous Computing and Interaction', 'Computer-Mediated Activity', 'Use, Design and Innovation', and 'Programming Languages'. Moreover, they wish to build competencies within Machine Learning and Systems Security. The deadline is 03.05.2018. More information at `https://goo.gl/rnJYSh`.

AARHUS UNIVERSITY

- 50th Anniversary Readership (Associate Professor) in Cyber Security at the Lancaster University School of Computing & Communications.

  With a salary range of £50,618 to £56,950 this is a permanent and full time job offer, closing on the 31st May 2018. This is with the renowned Security Lancaster, the University's

cross-disciplinary research institute in Security and Protection Science.

Security Lancaster is one of four flagship Lancaster Research Institutes and amongst the current 14 Academic Centres of Excellence in Cyber Security Research (ACE-CSRs) recognised by the UK government.

For other interesting positions all across Europe, please check the recently revamped “Researchers in Motion” portal at `https://euraxess.ec.europa.eu/`. It currently has close to 60 open positions in computer security and related areas, including in Poland, the UK, Finland, Slovenia, Italy, Norway, Switzerland, and even in Spain!

Welcome

## Proposals for STSMs

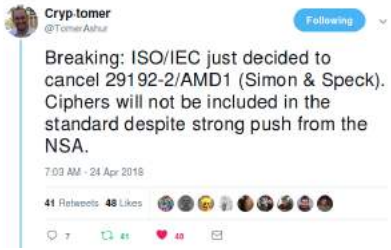
By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short) are. Please make your willingness to receive STSMs proposals known by sending me an email. Take into account that STSMs will be more competitive in this last period of the Action.
Until I do not have any more, I’ll just publish mine:

- I will be very happy to receive anyone interested in investigating randomness generation and testing, particularly on IoT devices.

## Blogs, posts and other recommended reads

**The End of the Road for SIMON and SPECK?**

Well done Tomer and Orr!




For more info, please check this aptly titled piece "ISO blocks NSA’s latest IoT encryption systems amid murky tales of backdoors and bullying" at `https://goo.gl/PkYcTD`.

**Other news**


**GravityRAT, state of the art in VM detection**

There is a continuous arms race between malware developers and analysts to detect (or, alternatively, hide) that a piece of malware is being run in a Virtual Machine. It is in the best interests of attackers to recognised when this is the case, so that they can stop their malware from running and hence being dynamically analysed by security experts. On the other hand, malware analysts want their VMs to replicate as accurately as possible real environments so that they can fully observe the behaviour of the malware under observation. A myriad of techniques have developed in this interesting area, but the recent GravityRAT seems to be various steps ahead of most current malware in spotting VMs. It uses no fewer than 7 different techniques to accomplish this. These include common techniques such as looking for traces of the hypervisor left on the virtual machine, checking the computer name, and checking the number of CPU cores.

But it also uses a novel technique where it requests the CPU temperature, a feature not commonly supported by hypervisors. These will then respond "not supported" thus revealing that the malware is probably not being run on a real machine.

More info at `https://goo.gl/15TN6x`, with the complete analyis by Cisco Talos researchers Warren Mercer and Paul Rascagnères.

## Event calendar

SSR 2018, The 4th Conference on Security Standards Research, will take place in Darmstadt Germany, on 3-4 December 2018.

The purpose of this conference is to discuss the many research problems deriving from studies of existing standards, the development of revisions to existing standards, and the exploration of completely new areas of standardisation.

**The deadline for submissions is 22 June 2018 (3pm UTC)**. The General Chair is Marc Fischlin. More

info at `https://ssr2018.net/`.


One of my preferred events in the European cybersecurity calendar is Nordsec.

It is one of the oldest events running, and although participants mostly come from European countries north of the 60th parallel, it is a magnificent event open to all. this year it runs its 23rd edition in Oslo, Norway, from the 28 to the 30 November.

The proceedings consist of peer-reviewed articles and are published in the Springer Lecture Notes in Computer Science series.

Some Cryptacus members are involved in the organisation or the program committee, such as Billy Brumley from Tampere University of Technology and Aikaterini Mitrokotsa from Chalmers University of Technology.

Prof. Audun Jøsang from UiO Norway is the General Chair this year.

**The deadline for paper submission is the 10th August**.


The 'IoT Autentication 2018' Conference will take place in Melbourne, Australia on November 28-30, 2018.

It will feature invited presentations from Auto-ID Labs, IoT Alliance Australia, IoT (Internet of Things) Security, Prof. Michael Sheng, Prof. Margreta Kuijper, Dr. Omid Kavahei, Prof. Seng Loke,and Prof. Lejla Batina.

The Keynote speaker is Dr. Veena Pureswaran from IBM. If you want to attend, check `http://www.authiot2018.conferences.academy/`.


The 14th International Conference on Information Security and Cryptology (Inscrypt) will be held in Fuzhou, Fujian, from December 14 to 16. Organized by the Fujian Provincial Key Laboratory of Network Security and Cryptology of Fujian Normal University.

It is an annual conference targeting the top research results in the related area.

Topics of interest encompass research advances in ALL areas of information security, cryptology, and their applications.

**Paper submissions close on August 14.**


FDTC 2018 is the Fourteenth Workshop on Fault Diagnosis and Tolerance in Cryptography, and will be held on the 13 of September 2018 in Amsterdam, co-located with CHES.

It is held in cooperation with the IACR and is interested in all aspects of fault injection.

**The submission deadline is May 25**, and Joan Daemen, now with Radboud University, is one of the Chairs. For more info, check `www.fdtc-workshop.eu`.


See you all back in June!

Best,
Julio Hernandez-Castro