July 2018, No 19

Cryptacus Newsletter

June-July 2018 Cryptacus Newsletter

Welcome to the June-July 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,

The final grant period of Cryptacus is now running, and it will finish on December 14th.

You still have time to apply for a STSM Grant or an ITC Conference Grant.

We will be very happy to receive your applications

Given that the final period is shorter than the previous ones, the budget is shorter as well, but we can still fund around 4 or 5 STSM Grants.

As usual, the procedure to apply is described on our website, www.cryptacus.eu and very lightweight.

Our major event during this final grant period is, of course, the conference in Rennes (France) on September 18-20, 2018.

The program consists of 16 invited speakers for 45-minute talks, and 13 speakers who will present their book chapter in 5 minutes.

These short talks will be recorded, and made available on the cryptacus website and possibly as well in the Springer book web.

The website of the conference is up, and available at http://www.cryptacus.eu/en/conference/

We will organize a social event at Mont-Saint-Michel, a famous rocky tidal island located in Normandy.

Do not hesitate to spread the URL in your labs.

The other running task is the Cryptacus book, to be published by Springer.

Everything goes well so far.

A call for chapters was published in 2017, and additional authors were lated invited to fill thematic gaps.

The chapters have been received by the editors, and the cross-review step started last week. The book will likely be sent to the publisher in October 2018, aiming for a publication date in early 2019.

Have a great summer break!

Best regards,

Gildas Avoine

Open Positions

Please send us any employment

opportunities you may want to publicize in the newsletter.

- Professor of Cybersecurity (includes a Lectureship appointment) at the Department of Computer Science, University of York. This is an excellent opportunity to lead a small but growing cybersecurity group at York, that comes with the infrequent possibility for the successful candidate to almost immediately recruit a Lecturer. York is one of the UK's best Universities, and one of the best places to live. Both positions are permanent and full time. The salary starts around £65,585 but can be higher based on experience. The only caveat is the very short deadline on the 5^{th} of July, which has been extended from the original 24^{th} June. More info at `https://goo.gl/hkwyb3`.

- Senior Research Fellow of Information Security and Privacy at the University of Tartu. With a salary of €3-3.5K per month, depending on qualification and experience. Deadline for applications is the 2^{nd} August. More info on the post and instrictions on how to apply at `https://goo.gl/ibfjin`.I was recently in Tartu, for NordSec'17, and liked the city a lot, it seemed like a very nice, calm and relatively inexpensive place to live.

- Full Professor of Ubiquitous Computing at TU Wien (Vienna University of Technology). For a start in October 2019, and with a deadline of 22 October 2018, this is an excellent opportunity at the Faculty of Informatics. They want somebody working on "next generation ubiquitous computing systems and their application in authentic real world settings. Particular research topics of interest include sensor-rich environments; interactive and smart spaces; new interaction paradigms; Internet of Things; mobile and context-aware computing; awareness and privacy; and tangible, situated and embodied interaction." Salary starts at €70K. For more info, check `https://goo.gl/5FUzSt`

- Tenure Track Assistant/Associate/Full Professor Innovative Computer Architectures at The Faculty of Science and Engineering of Groningen University. You may apply for this position until 14 August 23:59h. More info at `https://goo.gl/CFVqvP`

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!

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.

Event calendar

CARDIS 2018 will take place on November 12-14th in Montpelier, France. The submission deadline is July 13, 23:59:59 Anywhere on Earth (AoE). More info at `https://cardis2018.sciencesconf.org`.

The Sixth International Workshop on Lightweight Cryptography for Security & Privacy (LightSec 2018, In Cooperation with IACR) will take place on September 10-12, in Cardiff, together with the 11th International Conference On Security Of Information and Networks. The submission deadline is the 20^{th} July. The general chair is Atilla Elci and the PC chair is Koray Karabina. For more info, check `http://www.sinconf.org/sin2018/lightsec.php`.

Indocrypt 2018 will take place on 9-12 December in New Delhi. The submission deadline is 25 August 2018, 11:59 AM, GMT. Tutorials will take place on the 9 December and the conference properly on 10-12 December. It's the 19^{th} edition of the event. More info at `https://www.isical.ac.in/~indocrypt/`

Indocrypt 2018

9-12 December
NEW DELHI

Introduction

Sponsors/Co-organizers

Indocrypt 2018 is the 19th International Conference on Cryptology in India. The conference will take place during 9-12 December 2018 in New Delhi. Indocrypt 2018 is part of the Indocrypt series organized under the aegis of the Cryptology Research Society of India.

Important Dates

- Submission deadline: 25 August 2018, 11:59 AM, GMT
- Notification to authors: 12 October 2018
- Final versions of accepted papers: 22 October 2018
- Tutorials: 9 December 2018
- Conference: 10-12 December 2018

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 has been postponed to the 6^{th} July (3pm UTC), so hurry up!. The General Chair is Marc Fischlin. More info at `https://ssr2018.net/`.

SSR 2018: Security Standardisation Research

[illegible]

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.

NordSec 2018

Welcome to NordSec 2018

The 23rd Nordic Conference on Secure IT Systems

[illegible]

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/`.

IoT Autentication 2018

AUTHENTICATION FOR THE FUTURE INTERNET OF THINGS

Date: November 28 – 30, 2018, Melbourne, Australia

Location: [illegible]

URL: [illegible]

Significance

[illegible]

Organizers

[illegible]

Flyer

[illegible]

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.

Inscrypt 2018

[illegible]

About INSCRYPT 2018

[illegible]

See you all back in September!

Best,
Julio Hernandez-Castro