December 2017, No 14

Cryptacus Newsletter

December 2017 Cryptacus Newsletter

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

News from the Chair

by Gildas Avoine

Dear Cryptacus Members,

I would like to start this newsletter by thanking Lejla Batina, Veelasha Moonsamy, and Irma Haerkens for the organization of our workshop in Nijmegen last month.

It was a very successful workshop, and greatly organized.

The slides of the presentations will be available on the Cryptacus' website soon.

The next event will be at São Miguel Island, in the Portuguese archipelago of the Azores, in April.

Precise venue, dates, and program will be communicated by the end of the year.

In the meanwhile, we will progress on the book that we plan to publish on the cryptanalysis in ubiquitous computing systems.

We indeed recently announced the call for chapters (available at: `www.cryptacus.eu`), which you can distribute to colleagues involved in our research field.

You should also have received a few days ago my email containing the minutes of the book-related working session we organized in Nijmegen.

Again, if you know that you will submit a proposal, please send us a mail of intent without waiting for the deadline, so we will be able to early detect gaps in the covered topics.

Please, use the address cryptacus.editors@irisa.fr to contact Julio and myself about matters regarding the book.

Finally, I would like to remind you that the current grant period will end on April 30th, 2018.

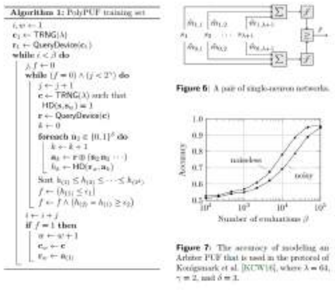
You still have time to apply for an STSM or an Inclusiveness Target Countries (ITC) Conference Grant.

In a few words, this tool allows PhD Students and Early Career Investigators from ITCs to attend conferences, if they give a talk (or present a poster).

Best regards,

Gildas Avoine

Recommended reading


Algorithm 1: PolyPUF training set
Figure 6: A pair of single-neuron networks.
Accuracy
noiseless
noisy
Number of evaluations β
Figure 7: The accuracy of modeling an Arbiter PUF that is used in the protocol of Konigsmark et al. [KCW16], where λ = 64, γ = 2, and δ = 3.

This month we are going to focus on a paper by Jeroen Delvaux, from KU Leuven, that presents a string of attacks against popular PUF-based authentication schemes.

The work is titled "Attacks on Three PUF-Based Authentication Protocols: PolyPUF, RPUF and PUF-FSM".

The author presents efficient impersonation attacks based on the use of machine learning that exploit the poor diffusion and confusion properties of many PUF-based protocols.

In fact, this work is a continuation of the author's recent PhD Thesis, where he analyzed the security of 21 PUF-based authentication protocols and found numerous issues to the extent that only 6 proposals survived this cryptanalysis effort.

It is particularly relevant that the 3 protocols broken in this work have been designed to be resistant to machine learning attacks by using some obfuscation logic, admittedly not very strong because it ought to be lightweight.

That makes feasible that, by using a relatively low number of challenge-response pairs, one can establish a relatively accurate model of the PUF and predict its response to unseen challenges employing artificial neural networks or support vector machines, to mention just a couple of machine learning approaches that generally produce good results.

I particularly like the author's analysis presented in the Aftermath section, where he discusses the underlying reasons for the vulnerabilities found, and makes suggestions to avoid similar attacks that everybody working in this area should consider and implement in future proposals.

A very interesting work by a very promising early career researcher that casts a serious doubt on the security of many of the existing, including some very recent, PUF-based authentication protocols. A must-read for anybody working in the field.

The original paper can be accessed at `https://eprint.iacr.org/2017/1134.pdf`

Funding News

A recent workshop on the future of security research in Europe, organised by the German Federal Ministry of Education and Research (BMBF), highlighted a number of priority policies, and stressed that security and defence research is still a priority area in Framework Programme 9 (FP9).

The participants agreed that a coordinated approach is needed in response to recent security events across Europe and that, while defence and civil security research activities have different objectives and stakeholders, the required solutions will often be very similar if not the same.

It seemed clear that civil security research and defence research should continue to be funded from separate pots and not be merged into a single strand. Also, there was apparent the need to better engage with industry and to promote, disseminate and exploit the results in Europe.

The participants at the workshop made a number of recommendations for FP9, and stressed the importance of covering, in the security calls of the following two years, the topics below:

- Consider elections as critical infrastructure, and protect them accordingly
- Fight against fake news
- Fight against the fragmentation of societies
- Artificial intelligence, block chain technology and bitcoin
- Dematerialised borders

The recommendations from the audience were:

- Ensure that the defence research programme and activities of the European Defence Agency do not undermine each other.
- Improve dissemination and exploitation; make better use of end-user networks; allow for greater flexibility to face urgent end-users' needs
- Standardise and harmonise to overcome market fragmentation
- Combine digital and physical security research
- Security has both technological and societal challenges, cover them all in future calls
- Ensure that key agencies are engaged - Interpol, Europol, border agencies, police force, fire and rescue services, etc.

The Commission is planning to hold a public hearing in December 2017 before the adoption of the Multiannual Financial Framework (MFF) in May 2018. The Commission's proposal for the ninth framework programme is to be published in early summer 2018.

MSCA: 2018 RISE Call Open

On the 23 November, the European Commission opened the call for proposals for the Marie Sklodowska-Curie Actions (MSCA) European Research and Innovation Staff Exchange (RISE).

The deadline is 21 March 2018. The available budget is 80 million, and the call-related documents, including the guide for applicants, and the link to the online submission are available on the Participant Portal.

Many national contact points are holding events for organisations interested in applying to the call in early January. Contact the one in your country for further details.

Open Positions

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

- If you want to join the excellent team at Birmingham University, with such strong researchers as Flavio Garcia and David Oswald, there is an interesting opening right now for a Research Fellow in Cyber Security, with a Hardware focus. The deadline for applications is January 3rd, 2018 and the contract is for 48 months, in the context of the EPSRC project 'User-controlled hardware security anchors: evaluation and designs'. In addition to a relevant PhD, applicants should have expertise in one or more of the following: cryptographic protocols; side-channel and fault attacks; implementation of cryptographic protocols using hardware features. More information on this highly recommended opportunity at `https://goo.gl/vzQWJA`.

- Sheffield is another prestigious UK university avidly recruiting in Cyber Security, trying to create a top group in the near future. They are offering 6 positions in cyber security and closely related areas, including positions that are open to recruit at the Reader, Senior Lecturer or Lecturer level. The earliest closing date for these positions is 5th January 2018. More information at `https://www.sheffield.ac.uk/dcs/jobs/index`

- Aarhus University, in Denmark is also offering positions at the Assistant Professor (tenure-track) and Associate Professor level. This is part of an ambitious expansion program, so there will probably be more job opportunities in the future.

  Applicants within all areas of computer science are welcome, but they are strong on crypto and computer security and candidates in these areas will likely be particularly welcomed. The deadline for applications is the 5th of January, 2018. More information at `http://www.au.dk/en/about/vacant-positions/scientific-positions/stillinger/Vacancy/show/934877/5283/`

- Lecturer or Senior Lecturer at the University of Cambridge - Department of Computer Science and Technology. This is a full time and permanent positions located at Aston. The deadline is the 10th January 2018. The Lecturer position `https://goo.gl/zDhzhk` has a salary range of £53,691 to £56,950. Interviews will be held on 19-20th March 2018.

For other interesting positions all across Europe, please check the recently revamped "Researchers in Motion" portal `https://euraxess.ec.europa.eu/`.

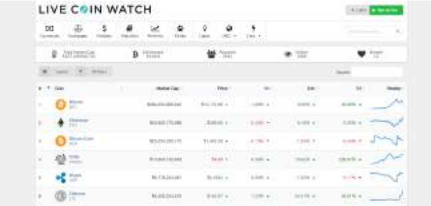
Proposals for STSMs

By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short) are, but we have a healthy budget for them within the Cryptacus project and not enough demand.

Please send your willingness to receive STSMs proposal to me for publishing here. 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.

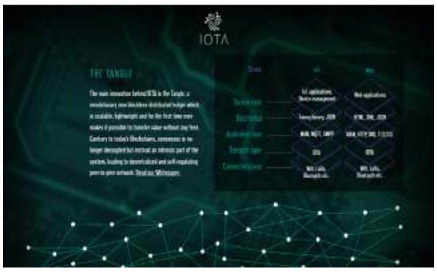
Blogs, posts and other good reads



IOTA

At the end of a very good year for crypto currencies, where bitcoin has had a prominent presence even in generalist media and many early players have multiplied their investments ten-fold or more, there is a curious project that has attracted massive support in the community and is IoT related, hence my coverage here.

For full disclosure, I have to say I have not invested in this project and, to be perfectly frank, I don't have it in very high regard. So my opinions below could be wrong but are at least not aimed to make a quick buck.


IOTA

THE TANGLE

There are possibly two reasons for this surprising success, one is that IOTA is not based on a classical blockchain but on an alternaive structure called 'The Tangle'. Iota is created to be as lightweight as possible, for connected IoT devices to be able to automatically pay minuscule amounts to one another (micropayments) in a frictionless manner without having to compromise on product design by introducing additional hardware.

The tangle is an Directed Acyclic Graph (DAG) linking devices with each other, that solves some of the perceived issues with blockchains, in particular the centralization of control, inability to conduct micropayments and their scalability limits.

All that is good, but what really changed the appreciation towards this project, and increased its value as a cryptocurrency, was the recent announcement that Microsoft, Samsung and Volkswagen will launch a secure data marketplace based on the IOTA technology. For more info, check `https://goo.gl/BaCcXx` or the white paper, at `https://iota.org/IOTA_Whitepaper.pdf`.

Event calendar

The 17th Annual Workshop on the Economics of Information Security (WEIS) will take place next year in Innsbruck, Austria. The submission deadline is February 18, with a notification of acceptance by March 31. Rainer Böhme is the conference chair.

WEIS 2018

17th Annual Workshop on the Economics of Information Security

The 10th International Conference on Cryptology, AFRICACRYPT 2018, will take place in Marrakesh, Morocco on 7-9 May. The submission deadline is on January 7, and the notification on February 20th.

Springer

جامعة الأخوين
AL AKHAWAYN UNIVERSITY

10th International Conference on Cryptology, AFRICACRYPT

The 23rd Australasian Conference on Information Security and Privacy (ACISP 2018) will be held in Wollongong, Australia on July 11-13, 2018. It will be organized by the University of Wollongong. The submission deadline is the 25 February 2018 at 11:59pm AEST and the notification will be on the 8th April.

UNIVERSITY OF WOLLONGONG AUSTRALIA

23rd Australasian Conference on Information Security and Privacy
July 11-13, 2018, Wollongong, Australia

Welcome to ACISP 2018

Springer

The 3rd International Workshop on Boolean Functions and their Applications (BFA) is organized by the Selmer Center of the University of Bergen.

It will take place at the Alexandra Hotel, Loen, in Norway during June 17-22, 2018. The deadline for submission is April 1st, 2018 (no kidding) and the notification will be one week later, on April 7th.

The 3rd International Workshop on
Boolean Functions and their Applications (BFA)

This workshop occurs immediately after a related one called WAIFI (International Workshop on the Arithmetic of Finite Fields 2018) in Bergen, which is on June 14-16, with a deadline on April 1st, and acceptance notification on May 11th, 2018. More info at `http://waifi.org`.

International Workshop on the Arithmetic of Finite Fields
WAIFI 2018

The 21^{st} Information Security Conference (ISC 2018), will take place in London (Guildford), from September 9 to September 12, 2018. The submission deadline is 16 April, with notification on the 18 June. The General Chair will be Steve Schneider.

21st Information Security Conference

9-12 September 2018, London (Guildford), UK

ISC 2018

See you all back in January!

Best,
Julio Hernandez-Castro