Cryptacus Newsletter

January 2018
Cryptacus Newsletter

Welcome to the January 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,

Let me first of all wish you a happy new year 2018!

The year 2018 will actually be important for Cryptacus, with two major events, in April and September, respectively.

Also, we are on the home stretch now, given that Cryptacus will finish in December 2018.

In the meanwhile, let's meet in Sao Miguel island, Azores (Portugal) in April, where several Cryptacus' events are colocated. This is a brief schedule:

*** Saturday 14th / Sunday 15th: Workshop on Distance Bounding Protocols (co-organization by COST Action CRYPTACUS & ERC POPSTAR).

The workshop is free and open to every one. Both theory and practice of distance-bounding protocols will be considered.

Several great speakers already accepted the invitation, including S. Capkun (ETHZ, Switzerland), G. Hancke (University of Hong Kong), and M. Kuhn (University of Cambridge, UK), just to name a few.

*** Monday 16th: Working session on the CRYPTACUS' book. This session is free, open to everyone although mostly dedicated to people who submitted a chapter to the CRYPTACUS' book (if you plan to submit, but not done yet, let me know asap). Please, check the Cryptacus website if you are not aware of the call for chapters.

*** Tuesday 17th: MC Meeting (8:30–10:00 am). For MC Members only.

*** From Monday 16th to Friday 20th: Training School. Grants are available for trainees (e.g. PhD students, ECIs, etc.).

More information is available on the websites of the respective events:

- Workshop on Distance Bounding Protocols (co-organization CRYPTACUS & ERC POPSTAR): http://surrey.ac.uk/futureDB. Please contact Gildas (gildas.avoine@irisa.fr), Ioana (i.boureanu@surrey.ac.uk), Stephanie (stephanie.delaune@irisa.fr), or Cristina (cristina.onete@gmail.com)

- Training School (also information on Book session and MC Meeting): `https://goo.gl/w52ThM`. Contact Ricardo Chaves (Ricardo.Chaves@inesc-id.pt)

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

You still have time to apply for an STSM but you should send your request very soon.

Best regards,
Gildas Avoine

Recommended reading: On the dangers of speculation

I was lucky enough to attend the Real World Crypto in Zurich, Switzerland on January 10-12, 2018.

This highly recommended event took place in an amazing venue, the Volkshaus Zurich, which is normally a concert venue.

RWC2018 has been, by far, the largest event ever organised by the IACR, with more than 600 participants despite having a very average 36 presentation slots.

There was a lot of buzz in twitter, most of it under the hashtag #**realworldcrypto**, including a nice effort by @durumcrustulum to live tweet the event.

I enjoyed the event enormously, despite having been allocated only 5 minutes for my presentation, and some illness during day 2.

One of the cherries on the top was the invited talk by Jann Horn of Project Zero on the Meltdown and Specter bugs, that is recorded at `https://goo.gl/1PPqTp`.

Particularly interesting is the Q&A session, also accessible in the link above, that includes the very relevant disclosure process and some other interesting queries.

Meltdown and Spectre are certainly the vulnerabilities of the year so far, and can easily become those of the decade.

They have been widely reported on the media.

They exploit critical vulnerabilities in modern processors, allowing malicious programs to steal data that should be beyond their reach.

This allows to get hold of secrets stored in the memory of other running programs including passwords stored in a password manager or browser, photos, emails, or business-critical documents.

It is particularly damaging that Meltdown and Spectre affect personal computers, mobile devices, and cloud servers, allowing an attacker to steal data from other cloud customers.

An additional worry is that the available patches as of writing seem to seriously degrade the processor's performance.

More info about the attacks can be found at `https://meltdownattack.com/`.

It is really a pity that this event will only come to Europe every third year, as it alternates between Europe/East and West USA.

I have not run a proper poll on the topic, but my impression (though I may be suffering from confirmation bias) is that an increasingly large number of security researchers are reluctant to travel to the USA under the current political climate.

In addition, a TSA encounter of the third kind is not featured prominently in our bucket lits.

Funding News

SMI2G

The Security Mission Information & Innovation Group (SMI2G) is organising a two-day event in Brussels to exchange information on the 2018 Secure Societies calls and to stimulate networking for the creation of potential ideas and consortia.

This will take place on the 1st and 2nd of February 2018 at the Central Auditorium (Pierre Lacroix), of the Universite Catholique de Louvain (UCL) in Brussels.

This is heavily recommended to make contacts, meet colleagues, and start discussing ideas and building consortia for the security calls of this summer. More info at `https://www.tno.nl/smi2g/`.

If you plan to attend, drop me an email to meet there!

Open Positions

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

- Professor in Secure Systems at the University of Surrey,

Department of Computer Science. Salary from £67,970 to £91,001 per annum. Deadline for applications is the 5th March.

Suitable areas of expertise that complement current strengths of the group include (but are not limited to): anti-malware security, adversarial machine learning, risk management and threat modelling, trusted systems, verification, and distributed systems.

This is a full time, permanent job offer. For more info, visit the ad at `https://goo.gl/SGDf64`. The same employer is currently recruiting for a Senior Lecturer or Reader in Secure Systems, this time with a deadline of 23rd April. More info at `https://goo.gl/unyTQp`.

- Associate or Assistant Professor in Cyber Security at the Technical University of Denmark.

  The submission deadline is the 1st February. This is a full time, permanent position based in Lyngby.

  Topics of interest include access control, authentication and identity management systems, blockchains and distributed ledger technologies, malware analysis, digital forensics, and ethical hacking, privacy and privacy enhancing technologies, and security in pervasive computing systems.

  More info at `https://goo.gl/Spu76V`.

- Lecturer or Senior Lecturer/Professor positions in Cyber Security at the Queen's University Belfast Centre for Secure Information Technologies (CSIT).

  These positions are based in Belfast, with a salary of between £35,550 to £64,079 per annum.

  The deadline for submitting your application is 29th January. Their priority areas are Hardware Security, Software Security, and Embedded Systems Security. More info at `https://goo.gl/1enATh`.

- Lecturer in Computer Science (with a specialization in Security) at King's College London - Department of Informatics.

  This posts is based in London, with a salary of £41,212 to £49,149 plus an annual London allowance of £2,923.

  The deadline for application is 17th March. This is a full-time, permanent position. The successful candidate will be appointed to the Cybersecurity (CYS). More info at `https://goo.gl/dXPP7X`

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!

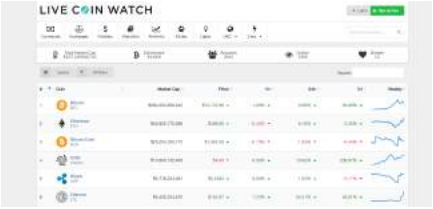
Proposals for STSMs

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. 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



IOTA: Wouldn't touch with a barge-pole

Very interesting developments around IOTA over the past weeks.

After a highly positive report on the cryptocurrency published on the 14th of December by the influential MIT Technology Review, titled "A Cryptocurrency Without a Blockchain Has Been Built to Outperform Bitcoin" there were many voices accusing the piece of being uncritical and too rosy.

It certainly had a positive impact on the cryptocurrency markets, but less than a week later Joichi Ito from the MIT Media Lab published a very critical response `https://goo.gl/C2Ca9K`.

This response was critical of both the currency and the previous bland article.

It was an inspired and well documented rebuttal of many of the assertions published as facts when in reality they were simply reflecting without much analysis on claims by the IOTA developers.

This response highlighted a number of serious issues with the project, notably that the much publicized IOTA relationships with top-tier companies such as Microsoft and Fujitsu were nebulous at best if not straight lies.

Also, it reasoned that it is not a fully decentralized project, and has suffered from availability issues as a result of this. More importantly, it analysed the total unconvincing answers to the security issues publicly reported.

This last point regarding security is possibly the most enlightening, so we will reproduce it in full:

"*Once the Digital Currency Initiative published the break in IOTA's curl hash function, its author, Sergey Ivancheglo, offered two conflicting explanations for the vulnerability. The first explanation was that the flaw was intentional - that it was meant to serve as a form of 'copy protection.' If anyone used this code in their own work, he said, the IOTA developers would be able to exploit the flaw and damage other systems that were using the hash function. However, later, he offered a conflicting explanation that he didn't write the curl at all, but that an AI wrote it. We do not find either of these explanations convincing, even in isolation. That they contradict each other makes them even less so.*"

We agree with this view.

Despite all this, at the time of writing IOTA is the 11th cryptocurrency for market capitalization, with a worth of 8.2 billion dollars.

If I were you, I will keep a safe distance from this project. I won't be surprised if it collapses as it recently did another cryptocurrency scam called BitConnect, which was a classical Ponzi scheme in a thin disguise.

For further reading, I would recommend the early (Sept 2017) post titled "Why I find IOTA deeply alarming" by Nick Johnson (an Ethereum core developer) at `https://goo.gl/HYyTtp`.

Be careful out there!

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.

The 16th International Conference on Applied Cryptography and Network Security (ACNS 2018) will take place in Leuven, Belgium from July 2 until July 4.

The **submission deadline is Jan 26**, 2018 AOE (Anytime on Earth).

The 23rd Australasian Conference on Information Security and Privacy (ACISP 2018) will be held in Wollongong, Australia on July 11-13, 2018.

It will, unsurprisingly, 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.

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.

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`.

The 21st 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.

The 13th International Conference on Availability, Reliability and Security (ARES 2018), will be held from August 27 to August 30, 2018 at the University of Hamburg, Germany.

The submission deadline is March 16, 2018. This conference is quickly becoming one of the largest security gatherings in Europe, with more than 12 associated workshops covering from 5G Networks to Information Hiding.

Of special interest to our audience is, possibly, the 2nd International Workshop on Security and Forensics of IoT.

SecureComm 2018, the 14th EAI International Conference on Security and Privacy in Communication Networks is taking place in Singapore, from August 8-10, 2018. **Deadline for submissions is 16 February.**

See you all back in February!

Best,
Julio Hernandez-Castro