Cryptacus Newsletter

June'17 Cryptacus Newsletter

Welcome to the latest edition of the monthly Cryptacus.eu newsletter, offering a glimpse into recent developments in the IoT cryptanalysis and related areas. We'd love to receive more of your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by GILDAS AVOINE

Dear Cryptacus Members,

I am glad to tell you that the new yearly Grant Period is now open, and STSMs can consequently be carried out again.

Cryptacus' Management Committee approved the organization of two events during this Grant Period, namely a workshop on Nov. 16-18, 2017 in Nijmegen (Netherlands) organized by Lejla Batina, and a training school on April 16-20, 2018 (tentative dates that might be modified) in Sao Miguel Island (Portugal) organized by Ricardo Chaves.

Thanks to both of them for their involvement in Cryptacus.

A Management Committee meeting will also take place jointly with these two events.

A web page will be set up soon to provide information about Nijmegen's workshop. Each Management Committee member will receive his/her official invitation letter before the summer break.

It is worth noting that the Nijmegen's event will be a 3-day workshop instead of the 2-day workshops we ran in the past. We aim to provide more free time to Cryptacus' participants for collaboration.

Activities to encourage and facilitate collaboration will be set up. Do not hesitate to contact me if you would like to share thoughts about such activities.

As we did in Sutomore (Montenegro), the workshop will mostly (but not only) consist of submitted presentations. The expenditures of the selected speakers will be fully reimbursed, which is a great opportunity - especially for young researchers - to attend a workshop and present their research results.

Best regards,
Gildas

Recommended reading

Table 11: A summary of the differences between ultra-lightweight and IoT cryptography.

	Ultra-Lightweight	IoT
Block size	64 bits	$\geq$ 128 bits
Security level	$\geq$ 80 bits	$\geq$ 128 bits
Relevant attacks	low data/time complexity	Same as "regular" crypto
Intended platform	dedicated circuit (ASIC, RFID...)	micro-controllers, low-end CPUs
SCA resilience	important	important
Functionality	one per device, e.g. authentication	encryption, authentication, hashing...
Connection	temporary, only to a given hub	permanent, to a global network

This month we will briefly cover an important paper just uploaded to e-print titled *State of the Art in Lightweight Symmetric Cryptography* by Alex Biryukov and Leo Perrin from the Luxembourg Security Group.

You can read a preliminary version of it at `https://eprint.iacr.org/2017/511.pdf`.

The authors present an extensive survey of all lightweight symmetric primitives they could get their hands on, including designs from the academic community, government agencies and even proprietary algorithms which were reverse-engineered or leaked.

More controversially, they argue that lightweight cryptography is too large a field that should be split into two related but distinct areas: ultra-lightweight and IoT cryptography.

They propose the former to deal only with the smallest of devices, for which a lower security level may be justified by the very harsh design constraints. They envision the latter to focus on low-power embedded processors for which the AES and modern hash function are too costly but which have nevertheless to provide a high level of security due to their greater connectivity.

Perhaps not all readers will agree with this proposal, but their division makes sense and provides good food for though.

As the authors say 'connecting a family of devices to a global network and protecting them with an 80-bit key is not a desirable situation, and yet it is what may happen if an ultra-lightweight algorithm is used where an IoT one is needed'. Indeed.

Funding News

We have been given early access to the next set of EU Horizon2020 draft work programmes.

These are important documents - describing all the EU research funding calls that will happen between 2018 and 2021.

This is a great opportunity to get ahead of the game, plan early and start talking to collaborators.

Although off-putting in size, these documents outline all the calls, budgets and deadlines for the next three years: 2018-2021 (with the exception of the ERC that publishes annually).

We cannot share these documents publicly, but will be happy to answer your questions on particular calls if you send them to me by email.

Use this opportunity to check calls in your area of interest and buy yourself months of extra time before the calls are published later in the year or in coming years.

As a brief taster, the areas most relevant to the Cryptacus aims are perhaps those covered in the Secure Societies. in particular we want to highlight the following calls: SU-INFRA02-2019 on 'Security for Smart Cities and soft targets in Smart cities'. Interestingly, subtopic 3 on 'Understanding the drivers of cybercriminality and new methods to prevent, investigate and mitigate cybercriminal behaviour' has a description around IoT and how it is an increasingly interested target for cybercriminals.

Open Positions

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

Interesting opportunities are lately arising in computer security with the transparent aim to attract talent willing to leave the UK after Brexit. New Zealand, Australia, Canada, China and Ireland are some of the firsts moving in this direction, as shown in the list below. When will France, the Netherlands and Germany follow? Asking for a friend...

- Lecturer in Digital Security. University of Auckland, New Zealand - Faculty of Science, Department of Computer Science. Deadline of 25th May 2017. They are particularly interested in experts on digital forensics, security testing, or software obfuscation, security or privacy for mobile devices, cyber-physical systems (esp. Internet of Things), machine-to-machine systems, and big data systems. More information at `https://goo.gl/Zb1tLJ`.

- Senior Lecturer in Secure Systems University of Surrey - Department of Computer Science. Deadline is the 25th May. Salary is from £39,324 to £57,674 per year. Two priority areas are *security through hardware and applied cryptography* and *secure systems and applications* `https://goo.gl/HUWh5F`. There is a similar position at the Lecturer level in the same institution with the same deadline, you can get more info at `https://goo.gl/xAaDbA`.

- Hamilton Professorships in Computer Science at Maynooth University. The areas of interest cover, between others, Cybersecurity and Privacy. Plenty of time to decide whether to apply, with a deadline on Friday 20th of October. Salary could be €110,060 to €139,501 p.a. for Professor A and €80,650 to €106,655 p.a. for the Professor B range. More info at `https://goo.gl/LSvKhM`.

- Senior Lecturer / Associate Professor in Security at The University of Sydney - School of Information Technologies, Faculty of Engineering and Information Technologies. Apparently housing prices in Sydney are astronomical, but the salary for the position, ranging from £88,332.30 to £117,175.50 may be good enough to cover for that. Deadline for applications is the 14th May. More info at `https://goo.gl/tTOUOX`.

- There is also an exceptional opportunity at the increasingly active and prestigious security group at the Vrije Universiteit Amsterdam. The post is for an Assistant or Associate Professor position in Systems Security, with a salary from €3605 to €6438. More info at `https://goo.gl/5bWHl8`.

  In addition, there are a good number of positions on the wrong side of the channel:

- Assistant/Associate Professor in Computer Science at Durham University. Deadline is the 30th May, salary up to £55,998. They mention in the job description both computer security and cryptographic analysis, whatever that may be. Apply at `https://goo.gl/pTPqwC`.

- Lecturer/Senior Lecturer in Cyber Security at De Montfort University - Faculty of Technology. De Montfort is recruiting heavily in recent times, and clearly is trying to attract talent and build a good cybersecurity team. Deadline for applications is the 2nd of July. More info at `https://goo.gl/0tK1AX`

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

Proposals for STSMs

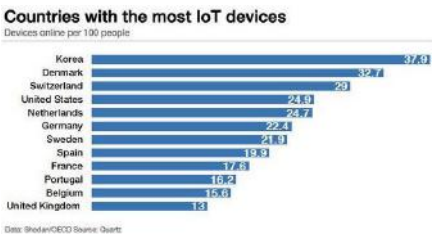
By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short) are, but we have a healthy budget for them within the Cryptacus project and not enough demand.

Until somebody sends more proposals, we will repeat the STSM offers of the past, including that of Aurélien Francillon and mine.

- "At Eurecom we are actively working on analyzing embedded devices software and building methodologies and tools for this. An example of that is ourvopen source Avatar Framework (see `http://s3.eurecom.fr/tools/avatar/`) which is aimed to reverse engineer devices and search for vulnerabilities. We are happy to receive visitors interested in the topic, for example to get help to start using the Avatar framework on a given device."

- I will be happy to receive anyone interested in investigating the many limitations and pitfalls of the PRNGs and the TRNGs currently in use on IoT devices.

Blogs, posts and other good reads



All over the news in recent times here in the UK has been a study by University of Twente that claims that smart meters are producing in some case readings that wrongly try to charge customers up to six times their right consumption.

An example of this, covered in The Telegraph, is at `https://goo.gl/RtDXL1`. This is, of course, not great for smart meter adoption and by extension also could affect other smart devices.

This is particularly worrisome in the uK, as the government is pushing for putting smart meters in every household by 2020, claiming it will improve the accuracy of people's energy bills.

The study points this is not always the case, and gives conspiracy theorists too worried about their privacy impact `https://goo.gl/mqoQVB` further fuel to vigorously oppose these measures.

Apparently the main culprits are 'green devices such as energy saving light bulbs, heaters, LED bulbs and dimmers that change the shape of electric currents which can result in a distorted reading'. Interesting but very troubling.

Another interesting piece of news is the publication of a very damming report by F-Secure regarding Chinese manufacturer Foscam.

The security cameras produced by Foscam are so plagued with security

issues that they can be easily compromised remotely so that attackers can get total control over them and heir video feeds.

Even worse, they responsibly disclosed their findings to the manufacturer months ago and they basically sit on them. More worrying, these serious vulnerabilities seem to exist in many other camera models manufactured by Foscam for other makes.

Hard-coded passwords that can't be changed by the user are just one of many issues. Foscam manufactures cameras for, between many others, Chacon, Thomson, 7links, Opticam, Netis, Turbox, Novodio, Ambientcam, Nexxt, etc.

More info here `https://goo.gl/YveuS2`.

Event calendar

The 17th Smart Card Research and Advanced Application (CARDIS) Conference will be held in Lugano, Switzerland, from November 13th to 15th 2017. The deadline is the 21st of July.

Indocrypt is this year in Chennai, with a paper submission deadline of August 20^{th} and notification on the 5^{th} of October. The conference will be from 10-13 December.

The 16th IMA International Conference on Cryptography and Coding will take place in St Catherine's College, University of Oxford from 12-14 December. The deadline for submission is the 14th of July. This is a prestigious and venerable conference with an excellent Program Committee. More info at `https://goo.gl/KejTXB`.

See you all very soon!

Best,
Julio Hernandez-Castro