Cryptacus Newsletter

November 2017
Cryptacus Newsletter

Welcome to the November 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,

Next week, we will meet in Nijmegen, the Netherlands, for our biannual event.
The scientific program is now available on the web site at `https://cryptacus.cs.ru.nl/`.
Lejla Batina, Veelasha Moonsamy, and Irma Haerkens, the local organizers, did a great job to prepare this event.
We will have 29 talks, including an introduction by our COST Science Officer, Karina Marcus, and 4 invited talks by Clémentine Maurice, Johann Heyszl, Francesco Regazzoni, and Léo Perrin.
It is worth noting that Thursday afternoon will be devoted to collaborations. We will organize small scientific and informal meetings/brainstormings (in parallel) about any topic you are interested in.
Please, think about topics you would like to work on with other people. We will install a white board such that everyone will be able to suggest topics and people will be able to register to any topic.
We will also allow you to present your topic(s) during a couple of minutes on Wednesday. You can so prepare 1 or 2 slides. This activity will be fruitful only if we are proactive in suggesting topics. Private lounges are also possible if you want to pursue an ongoing collaboration.

During our event in Nijmegen, we will also take time to discuss about the book we plan to write on the cryptanalysis in ubiquitous computing systems. The call for chapters, prepared with the collaboration of the working group leaders, is now online on Cryptacus' website at: www.cryptacus.eu
Julio Hernandez-Castro will organize a session on Thursday afternoon for members who are interested in submitting a chapter. We will also look for a couple of volunteers to participate to the selection committee.
Last but not least, if not already done, please register to our Nijmegen's workshop at cryptacus.cs.ru.nl/registration.shtml in order to make the life of the organizers easier. Many thanks.

See you there!

Gildas Avoine

Opportunities

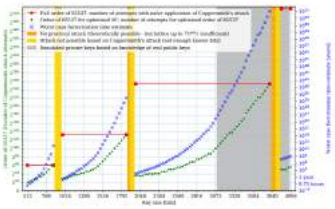
ENISA Call for IoT Experts

I had the opportunity to attend the ENISA/Europol IoT Security Conference and expert meeting group in the Hague in October 18-20 at Europol Headquarters. It was a very lively event, with lots of interesting

presentations by some of the major actors and vendors in the discipline. At the expert meeting there was a notable lack of representatives from academia, which in my view is very problematic. The group discussed a draft tentatively titled 'Baseline Security Measures for IoT' that is expected to be published and made publicly available before the end of the year. We will report on it in future newsletters.

In the meantime, please seriously consider to at least try to join the group, as there will be more meetings in the near future and more joint work on standardisation and IoT security that may have a profound effect on the security of Europe. Read more about the IoTSEC group at `https://goo.gl/uS1o4S` and join it by filling the form at `https://goo.gl/tzEJkC`.

Recommended reading



In a month with no shortage of new vulnerabilities, I have to confess that on a personal level my favorite one is the ROCA Attack.

The associated paper title is 'The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli'. This work by Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec and Vashek Matyas was accepted and presented a ACM CCS 2017, in Dallas, and describes a serious vulnerability in generation of RSA keys as implemented in a software library widely adopted in cryptographic smartcards, security tokens and other secure hardware chips manufactured by Infineon.

The attacker can compute the private part of an RSA key with significant less effort than the theoretical/expected one making the attack feasible for commonly used key lengths, such as 512 bits but also for 1024 and in some cases 2048 bits. For example, for some 512 bit keys just 2 CPU hours at a cost of $0.06 will suffice, or 97 CPU days (costing $40-$80) for some 1024 bit RSA keys. The authors provided a series of tools to verify online whether keys in use where affected. Major vendors including Microsoft, Google, HP, Lenovo, Fujitsu etc. have released software updates and guidelines for mitigation.

The authors stated that the currently confirmed number of vulnerable keys found is about 760,000 and the vulnerable chips are pervasive and not necessarily sold directly by Infineon, as the chips can be embedded inside devices by other manufacturers.

Estonia abruptly canceled roughly half its national ID cards used for voting, filing taxes, and encrypting sensitive documents as a direct result of the discovery. These results are particularly relevant for IoT aficionados, and affected electronic identity documents across Europe, including ePassports, eDriving licenses, national ID cards, etc. Problems have been reported with some of the ID documents in Estonia and Slovakia but rumors abound that other countries might be affected too. You can read more about this issue at `https://goo.gl/RMYU6L`.

All in all, an awesome piece of work that will probably continue to be relevant for years to come, as similar vulnerabilities will most likely crop up in other products.

Funding News

The European Commission has pre-published the draft 2018-2020 work programme part for the Marie Sklodowska-Curie Actions (MSCA). You can find it here `https://goo.gl/ngkbES`. It contains many changes, mostly improvements in my opinion, over the past rules for Marie Curie Actions.

The European Commission has pre-published the draft 2018-2020 work programme part for Societal Challenge 6 - "Europe in a changing world - Inclusive, innovative and reflective societies". You can access it at `https://goo.gl/jk91TS`.

The European Commission recently published its tenth progress report 'Towards an effective and genuine Security Union', which discusses progress over the last years and planned actions to improve security, including systematic checks and a revamping of the EU entry/exit system, the establishment of an 'European Travel Information and Authorisation System (ETIAS)', reinforce Europol, approving a new directive on combating terrorism and firearms trafficking, as well as explosives-precursors to combat home-made explosives, etc. It's a good read, that you can access at `https://goo.gl/Heb5de`.

The European Commission, and in particular the DG for Research & Innovation has launched a prize on online security as part of H2020 Industrial Leadership pillar. This Horizon prize aims to significantly improve citizen's overall experience on online authentication, looking for a solution enabling citizens to seamless authenticate across a wide

range of applications and devices. The ultimate objective is to foster the widespread adoption of services and products provided within the Digital Single Market of the European Union. The call is a single stage and has an estimated budget of 4 Million EUR. The deadline for the submission of proposals is 27 September 2018. You can get more info at `https://goo.gl/JWr1h9`.

Open Positions

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

- What in the UK is called 'the other UCL', that is, Universite catholique de Louvain, is searching for a full-time professor in Software Security. If you are interested in this permanent position, you have to hurry up because the deadline for submitting applications in the 15th of November. You can get more information and even start your application at `https://goo.gl/nMwzAY`.

UCL
Université catholique de Louvain

- 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/`

AARHUS UNIVERSITY

- 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.

University of Kent

- 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

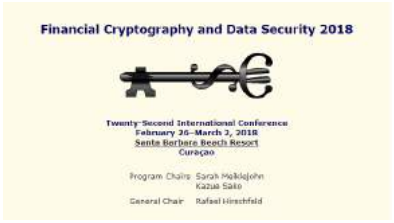
New and potentially more dangerous IoT botnet
News of a new botnet, more sophisticated than the infamous Mirai, are making the rounds. The new malware goes by the name of Reaper, and is way more powerful than the already quite damaging Mirai which limited itself to try a list of frequent usernames and passwords and primarily victimised IP cameras and routers. Reaper, on the other hand, is capable of exploiting known vulnerbilities in the targets it encounters,hacking its way in with an array of tools and spreading itself further. If Mirai was capable of causing such havoc by imply abusing default credentials, researchers fear what can happen with Reaper and its bag of

nine exploits targeting products from D-Link, Netgear, Linksys, Vacron, GoAhead, and AVTech. While many of the targeted products have patches available, unfortunately a significant number of users are not commonly applying those. This is another palpable example of the need for better solutions regarding updating policies in the IoT ecosystem, as Reaper is for sure not the last malware taking advantage of the current limitations in this area. Some researchers estimate Mirai controlled, at its peak, 2.5m devices and the latest estimates for Reaper are around 10 million. Even more worryingly, CheckPoint has noticed worm capabilites in Reaper, as infected devices contribute to spread the threat to new targets. Although not DDoS activity has been noticed at the time of this writing, it seems its authors are still adding machines to the botnet and that any attack target will really have a bad time defending itself from For more info, check `https://goo.gl/eDYKWq` or the very interesting study by CheckPoint at `https://goo.gl/qRPvfx` or, alternatively, an in-depth analysis by F-Secure at `https://goo.gl/XjWt2g`.

Event calendar

Eurocrypt 2018 will take place in Tel Aviv, Israel, from April 29 to May 3. The notification is on the 15 January. Orr Dunkelman is the General Chair.

Financial Cryptography and Data Security 2018 (FC18) is taking place, as usual, in an exotic location. This time in Nieuwpoort in Curacao, from February 26 to March 2. The notification will arrive on the 17 November.



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.

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.

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 18th Central European Conference on Cryptology will take place from June 6 to 8, 2018 in Smolenice, Slovakia. The venue will be the Smolenice Castle. Submission deadline is March 31st and notification is on Apr 30th.

See you all back in December!

Best,
Julio Hernandez-Castro