DECEMBER 2016, NO 4

Cryptacus Newsletter

December'16 Cryptacus Newsletter

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

News from the Chair

by GILDAS AVOINE

Cryptacus organized its biannual meeting on November 6^{th}-7^{th} in Sophia-Antipolis, in the French Riviera.

More than 35 people attended the working group meetings. Very exciting talks were arranged by the WG leaders, including the ones by the two invited speakers: Takanori Isobe (SONY Corporation), who spoke about "Security of Block Ciphers Beyond Blackbox Model", and Cristiano Giuffrida (Vrije Universiteit Amsterdam) whose talk was entitled "Imagine a World without Software Bugs".

An interesting and very active discussion about the concept of "lightweight cryptography" was also initiated by Working Group 2 (WG2: Cryptanalysis of protocols and primitives).

The Management Committee meeting was organized jointly with the Working Groups meetings.

An important point discussed during the meeting was about the organization of a workshop around March 2017.

The workshop will cover the topics considered in Cryptacus, and will consist of talks given by researchers who are not necessarily members of the COST Action.

A call for presentations will be published soon. Speakers of selected presentations will be invited to the workshop and fully financially supported by the COST Action.

The location of the workshop will be announced in December 2016.

Finally, I would like to thank those who sent information to cryptacus.newsletter@irisa.fr to feed December's newsletter.

Do not hesitate to use this information channel to announce news about your own work and spread important information for the community, including relevant call for papers, job opportunities, etc.

Recommended reading

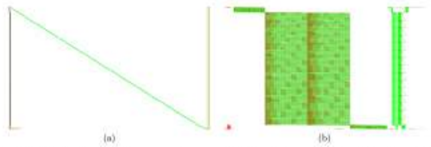


Fig. 3. (a) Visualization of a software execution trace of the binary Wyseur white-box challenge showing the entire accessed address range. (b) A zoom on the stack address space from the software trace shown in (a). The 16 rounds of the DES algorithm are clearly visible.

This month we will start and end our recommended reading section with a paper that perhaps many of you have already read titled *"Differential Computation Analysis: Hiding Your White-Box Designs is Not Enough"*, by Joppe W. Bos, Charles Hubain, Wil Michiels and the great Philippe Teuwen.

It was published at the last CHES conference, and it received the best paper award.

You can access it and, more interestingly, a video of their presentation, at http://iacr.org/cryptodb/data/paper.php?pubkey=27856.

Please send your contributions and suggestions for future issues of this newsletter.

Funding News

As we have shown in the last issues of this newsletter, there is no shortage of European calls for H2020 projects in our area of interest or closely related ones. We will try, from within Cryptacus, to facilitate the build up of consortia to successfully apply to several of these opportunities.

One additional opportunity we would like to highlight and will probably discussed in more detail over future issues is the Marie Curie Individual Fellowship scheme.

It is a prestigious and highly competitive scheme that basically allow you to bring to your University or Research Center a foreign researcher (not necessarily an EU citizen) for up to three years.

This is a golden opportunity to convince like-minded colleagues in other countries to come and stay working with you for one to three years, with all expenses covered by the scheme. Particularly recommended for early career researchers that want to establish their careers on firmer ground.

It is frequently the case, at least in the UK, that many of the Marie Curie Fellows are offered a Lectureship at the end of it, if everything has gone according to plan. Much more info at https://goo.gl/WHrwCU.

Open Positions

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

There are still 2 open positions at Eurecom in the security domain, at assistant professor level:

- System and software security: More info at https://goo.gl/WpW8cG
- Security and privacy for cloud computing: More info at https://goo.gl/KqNmuq The screening will start on November 1st, and applications will be accepted until the position is filled.

Other interesting positions are:

- Lecturer/Senior Lecturer in Cyber-Physical Systems, University of Cambridge. Deadline is 10th January 2017. Salary in the range £39,324 to £55,998 per year. Full time, permanent position. More info at https://goo.gl/oQMRZo. They explicitly mention Internet-of-Things/IoT, wearable technologies and security & privacy.

- Lecturer/SL/Reader/Professor in Secure Information Technologies. Queen's University Belfast - Global Research Institute of Electronics, Communications and Information Technology (ECIT). https://goo.gl/sbVPsm. £34,956 to £63,008 per annum. Full time, permanent positions. They explicitly mention in the job description "security of Smart Cities and the Internet of Things". Deadline is 12th December.

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.

We will repeat the STSM offer of Aurélien Francillon from last month:

'At Eurecom we are actively working on analyzing embedded devices software and building methodologies and tools for this.
An example of that is our open source Avatar Framework (see http://s3.eurecom.fr/tools/avatar/) which is aimed to reverse engineer devices and search for vulnerabilities.

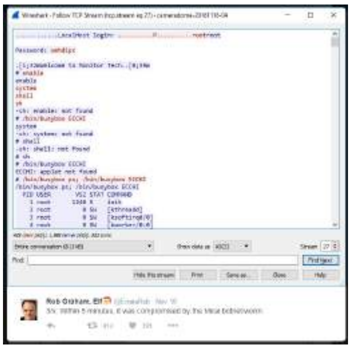
We are happy to receive visitors interested in the topic, for example to get help to start using the Avatar framework on a given device.'

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.

If you want to see what kind of work I'll be interested in carrying out, check my paper at RFIDSec'16 or the preliminary presentation at the WG4 meeting.

Contact me at jch27@kent.ac.uk if interested and/or for further info.

Blogs and posts to read



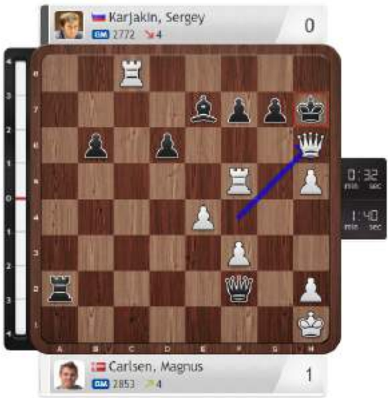
```
..........LocalHost login: ..........R..........root
Password: xmhdipc
.[1;32mWelcome to Monitor Tech.[0;39m
# enable
enable
system
shell
sh
-sh: enable: not found
# /bin/busybox ECCHI
system
-sh: system: not found
# shell
-sh: shell: not found
# sh
# /bin/busybox ECCHI
ECCHI: applet not found
# /bin/busybox ps; /bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
  PID USER       VSZ STAT COMMAND
    1 root      1368 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [ksoftirqd/0]
    4 root         0 SW   [kworker/0:0]
```

Rob Graham, Elf @ErrataRob · Nov 16
5/ Within 5 minutes, it was compromised by the Mirai botnet/worm

In https://goo.gl/gtwHgm we find a very popular piece of news that fits perfectly within the Cryptacus remit: A security researcher (@ErrataRob) plugs (with caution, he's a paranoid security researcher after all) his newly acquired smart camera into his WiFi network at home and checks that all is nice and sound, only to witness how just 98 seconds later it gets compromised by a variant of the infamous Mirai malware (again recently in the news due to crippling internet access for nearly 1 million home users in Germany). Admittedly, the camera is a cheap model https://goo.gl/L91jZJ with a default username/password of root/xmhdipc. This is the sorrow state of affairs right now. By the way, the blog of this researcher, Robert Graham, is highly recommended, and you can find it at http://blog.erratasec.com/.

Another non-academic but still interesting reading can be found at https://goo.gl/KwiPHT were the author comments on "19 Internet of Things IoT Security Startups". It is relevant to be familiar with what the industry is doing in IoT security, but there are many promising start-ups popping around and it's easy not to know what type of technologies they are working on. The selection is heavily based towards USA companies, but still useful. It is curious to see so many small companies working on automotive IoT security.

Lastly, there is another potentially interesting piece discussing the usage of blockchain to help in securing the IoT. I'm not fully convinced by all the proposed ideas, but in any case they are worth knowing, and could even be inspiring for some of you to develop new applications. More info at https://goo.gl/39AMbQ



And now for something completely different https://goo.gl/mn6qsS, as good old John Cleese used to say. I couldn't help but add the final position of the last game of the Carlsen-Karjakin match for the World Chess Championship that just finished moments ago while yours truly was writing this newsletter. It is an extremely beautiful and not so common mate pattern that I'm sure many of you will appreciate. Congrats to Magnus for retaining the title on his birthday!

Event calendar

As I finish this newsletter many of you will probably be in Hong Kong, attending RFIDSec. For those who missed it, there are still some interesting events on the horizon to keep us happy and hopeful!

For those who need an urgent excuse to escape to New York, the Real World Crypto Conference can't be bested. They have just published a very interesting program at http://www.realworldcrypto.com/rwc2017/program that contains, for example, some very promising presentations on embedded security.

If you want to learn a lot and fast on privacy, you can't get it much better than attending the 7^{th} BIU Winter School on Cryptography, which is devoted this year to "Differential Privacy: From Theory to Practice". Over five days, and with an excellent team of lecturers, you will have the opportunity to learn everything there is about privacy in Tel-Aviv at Bar-Ilan University. More info at http://cyber.biu.ac.il/event/the-7th-biu-winter-school/.

Euro S&P is this year in Paris, 26-28 April. A must! More at http://www.ieee-security.org/TC/EuroSP2017/index.php

Last but not least, the summer school on real-world crypto and privacy organised by Lejla will take place in Sibenik (Croatia), June 5 to 9. Highly recommended, for all ages! Registration will open early February 2017. More relevant info at http://summerschool-croatia.cs.ru.nl/2017/.

See you all soon!