Cryptacus Newsletter

November'16 Cryptacus Newsletter

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

News from the Chair

by GILDAS AVOINE

November is quite an exciting month for security in ubiquitous computing systems, because several events will be organized this month. First of all, Cryptacus' meetings are in less than a week. The meetings will take place at EURECOM in Sophia-Antipolis (France) on November 6^{th} and 7^{th}. I would like to use this opportunity to thank Aurélien Francillon who is the local organizer. The event is scheduled as follows:

- Sunday November 6^{th}:
  8:30 – 9:45: MC meeting
  10:15 – 12:15: WG1 meeting
  01:45 – 03:45: WG2 meeting
  04:15 – 06:15: WG3 meeting
- Monday November 7^{th}:
  9 – 11: WG4 meeting

Attending Cryptacus' meetings is an opportunity to also attend the closely located conference Cardis (Nov. 7-9, 2016) and the Ecrypt LightCrypto Workshop (Nov 9-10, 2016). Both are organized in Cannes. Another important event related to ubiquitous computing systems is RFIDsec, whose 2016's edition will be organized in Hong Kong on Nov. 30^{th} - Dec 2^{nd}, 2016. The very promising program is now available online at: http://rfidsec2016.org/program.html

Cryptacus expects to organize a workshop early in 2017 and the Management Committee is currently looking for candidates to organize it. The event will be a 2-day or 3-day workshop with invited and submitted talks. The Management Meeting will be colocated with the workshop to reduce travel expenses.

So, if you are interested in organizing this workshop, please contact Gildas Avoine or Bart Preneel. The selection of the candidate will highly likely be done in November.

Finally, I would like to thank those who sent information to cryptacus.newsletter@irisa.fr to feed November's newsletter. Do not hesitate to use this information channel to announce news about your own work and spread important information for the community.

Recommended reading

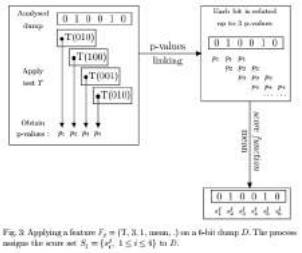


Fig. 3: Applying a feature $F_j = \{T, 3, 1, \text{mean}, \}$ on a 6-bit dump D. The process assigns the score set $S_j = \{s_i^j, 1 \leq i \leq 6\}$ to D.

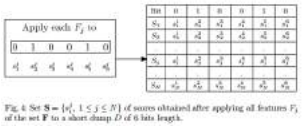
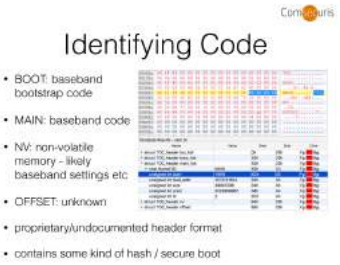


Fig. 4: Set $\mathbf{S} = \{s_i^j, 1 \leq j \leq N\}$ of scores obtained after applying all features F_j of the set $\mathbf{F}$ to a short dump D of 6 bits length.

This month there are just two items on our list of recommended readings. An academic paper and an invited presentation. The paper is by Thomas Gougeon, Morgan Barbier, Patrick Lacharme, Gildas Avoine, and Christophe Rosenberger. It is called "Memory Carving in Embedded Devices: Separate the Wheat from the

Chaff" and was published in the International Conference on Applied Cryptography and Network Security, 2016.
I find particularly fascinating how they try and finally manage to distinguish random data from other meaningful information. You can find it here https://goo.gl/Yx8T5F



The invited presentation goes by the quite funny title "Breaking Band: Reverse engineering and exploiting Samsung's baseband" and is by Daniel Komaromy, who works at Comsecuris. It continues in the good old tradition of breaking Qualcomm basebands, following some preliminary works on the topic presented at the 28C3 and other events earlier this year. It will be presented at Nordsec, which this year is organised by our friends at Oulu, in Finland. You can find more info at https://goo.gl/BqN8JM.

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.
As you may have noticed, the schedule for the Sophia-Antipolis meeting is very tight, but we will try to arrange for a H2020 informal meeting to exchange ideas and encourage members to participate in these competitive but highly rewarding bids.

Open Positions

Please send us any employment opportunity you want to publicize.
There are 2 open positions at Eurecom in the security domain, at assistant professor level, and a number of other positions at lesser institutions at the wrong side of the Channel:

- System and software security: More info at https://goo.gl/WpW8cG
- Security and privacy for cloud computing: More info at https://goo.gl/KqNmuq
- Professor of Telecommunication Networks. Birmingham City University. Deadline is 20^{th} November 2016. Salary in the range £51,559 to £56,042 per year. Full time, permanent position. More info at https://goo.gl/LcxVnd. There are other positions at the same institution at associate and assistant professor level (https://goo.gl/iTMKOI).
- Professor/Associate Professor in Computer and Information Sciences at Northumbria University - Department of Computer and Information Sciences/Faculty of Engineering and Environment. More info at https://goo.gl/bL8Q3m.

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 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, no pun intended, 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 or for further info.

Blogs and posts to read

This month, I will recommend you to check the blog of the IoT Security Foundation, that is a unknown organisation for me, but seems legit having between his members heavyweights such as Ross Anderson and Kenny Patterson, between others. It is at `https://iotsecurityfoundation.org/blog/`. They have just celebrated their first year.

```
#! /bin/sh
cd /home/volatile
cp /mnt/busybox .
chmod +x busybox
ln -s busybox telnetd
cp /mnt/S50telnetd /etc/init.d/
cp /mnt/inittab /etc/
chmod +x /etc/init.d/S50telnetd
/etc/init.d/S50telnetd
```

In addition, I will recommend to read again the blog of Pen-Test Partners, and in particular this `https://goo.gl/ZisRhi` which is the entry in which they report on their demo at Def Con 24 where they demonstrated how easy it was to create ransomware for IoT devices.
They chose a smart thermostat, partly because of the scary/amusing consequences of IoT vendor security complacency. They describe in detail how they created a fully functioning ransomware to take control of a smart thermostat and lock the user out until they paid up.
The sad but very familiar conclusion is that, as they put it, "Simple security controls would have stopped this hack working, yet they were not present."

Event calendar

I hope to meet many of you, either in Sophia-Antipolis, Cannes or Hong Kong later this month, as we have a number of very important events with very appealing programmes already available.

RFIDSec2016 (Hong Kong) has just published its list of accepted papers `http://rfidsec2016.org/program.html` and many talks look really interesting.

The Cardis programme is also available `https://2016.cardis.org/program.html`. It will be co-located with the Lightsec Crypto Workshop in Cannes that also has an outstanding list of speakers `https://www.cosic.esat.kuleuven.be/events/lightcrypto/timeline/`, so no excuses not to attend.

See you all very soon!