Cryptacus Newsletter

May'17 Cryptacus Newsletter

Welcome to the latest edition of the monthly Cryptacus.eu newsletter, offering a glimpse into recent developments in the IoT cryptanalysis area. 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,

The last Grant Period ended on April 30th, 2017.

The new one should start soon. Following the official procedure, the work and budget plan has been submitted to the COST Office and Cryptacus' Management Committee will then be requested to approve it.

Two events have been suggested in the work and budget plan, namely a workshop in November, and a training school in April 2018. Locations and organizers will be publicly announced after the official validation of the plan, likely before the end of May.

As you will be able to read in this newsletter, many faculty positions in the field of computer security are currently open.

If you have such open positions in your institution, or Phd/Postdoc opportunities, do not hesitate to contact Julio (cryptacus.newsletter@irisa.fr) who will advertise them in the next newsletter.

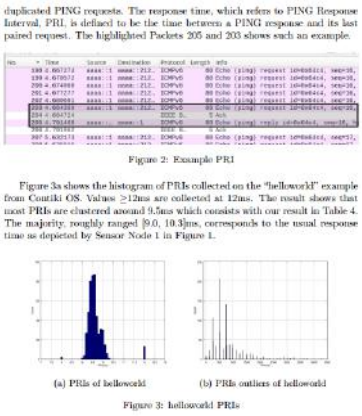
For young researchers (i.e., early career investigators according to COST's terminology) applying for an STSM is an opportunity to visit an institute and promote yourself in case a position would be opened in your field.

Finally, I would like to encourage Cryptacus' members to attend and send their students to the two summer schools mentioned in this newsletter, namely the summer schools on "security and correctness in the IoT" in Austria, and about "real-world crypto and privacy" in Croatia. Both are highly recommended.

All the best.

Gildas

Recommended reading



duplicated PING requests. The response time, which refers to PING Response Interval, PRI, is defined to be the time between a PING response and its last paired request. The highlighted Packets 205 and 203 shows such an example.

Figure 2: Example PRI

Figure 3a shows the histogram of PRIs collected on the "helloworld" example from Contiki OS. Values ≥12ms are collected at 12ms. The result shows that most PRIs are clustered around 9.5ms which consists with our result in Table 4. The majority, roughly ranged [9.0, 10.3]ms, corresponds to the usual response time as depicted by Sensor Node 1 in Figure 1.

(a) PRIs of helloworld (b) PRIs outliers of helloworld

Figure 3: helloworld PRIs

This month we will briefly cover an important paper titled *Exploring Potential 6LoWPAN Traffic Side Channels* by Yan Yan, Elisabeth Oswald and Theo Tryfonas from the Bristol Security Group. You can read a preliminary version of it at `https://eprint.iacr.org/2017/316.pdf`. 6 LoWPAN is the name for IPv6 over Low power Wireless Personal Area Networks, massively used in IoT environments, and the paper raises some serious security and privacy issues. They study side channel information on the protocol level that can ex-

ist despite the correct use of cryptography. Concretely, they investigate the potential for using packet length and timing information extract valuable information from a device. Exploiting this, they can distinguish (fingerprint) between devices, know which different programs are running on the same device, including which sensor is accessed. They also distinguish between different ICMP message types despite the use of encryption.

They finish their work by providing a set of recommendations to efficiently mitigate these side channels in the IoT context, notably padding and using time-constant code.
The paper is very practical, with examples over two extremely popular devices running on an open source OS (Contiki) with a typical stack of protocols.

Funding News

We will continue to arrange another H2020 session on the next Cryptacus meeting. It will be a good opportunity to discuss some of the most relevant future calls in detail, and plan well ahead of them to increase your success chances.

If you are interested in participating in this session, and particularly if you want to briefly present a project idea to get feedback and potentially start building-up a consortium, please contact me for booking a slot.

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 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`.

- Professor in Cryptology at Aalto University. This post has been around for a while. The deadline for applications has been moved forward from the 1st April to the 3rd of May. More info at `https://goo.gl/m35w5A`

- 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`.

  In addition, a good number of positions on the wrong side of the channel have recently opened:

- 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`.

- Last but not least, a couple of new positions at the University of Kent, my current institution, at the Senior Lecturer and the Lecturer level. Deadline is the 5th of June, applications and further info at `https://goo.gl/7AjKg2`.

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

Proposals for STSMs

EURECOM
Sophia Antipolis

By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short)

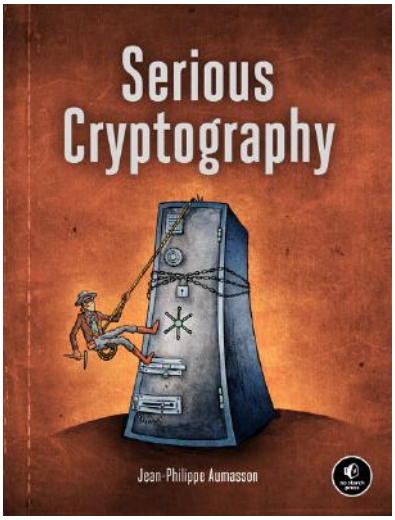
are, but we have a healthy budget for them within the Cryptacus project and not enough demand.

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



This month, we start by seriously recommending a brilliant piece of ongoing work by a well-known colleague. It is a book called Serious Cryptography by Jean-Philippe Aumasson.
Aumasson is now a Principal Research Engineer at Kudelski after being an academic for many years. He has authored many important crypto papers and primitives such as BLAKE2 and SipHash.
He regularly speaks at some of the best-known InfoSec conferences. The book will be published by the prestigious No Starch Press, and you can get a better idea of its contents and download Chapter 4 for free at `https://www.nostarch.com/seriouscrypto`.
I am really looking forward to read his Chapter 2, on Randomness. This looks like a really good book for both teaching and refreshing your crypto knowledge, and I appreciate the useful Python examples that populate its pages.

Another interesting news item is Brickertbot, one of the first Permanent Denial of Service (PDoS) IoT threats `https://goo.gl/O72mpE`. This techniques is also known as âĂIJphlashingâĂİ. PDoS are attacks that damage systems so badly that they require replacement or reinstallation of hardware.

By exploiting security flaws or misconfigurations, in this case matching the devices targeted by Mirai, this type of cyber attack can destroy the firmware and/or basic functions of system. In the figure above (by Radware) you can observe the actual command sequence used by BrickerBot.1 to compromise IoT devices and corrupt their storage, disrupt Internet connectivity, performance, and wipe all files on the device.

The BrickerBot author was later interviewed in `https://goo.gl/NgzUVY` and claimed to have bricked 2 million IoT devices. The hacker also claims that the malware first attempts to secure the units without damaging them and only bricks them as a last resort. He or she goes by the very appropriate handle of Janit0r, who claims his work was just an attempt to make the creation of million-device botnets more difficult, and raise awareness.

Janit0r may have half a point, but I rather deal with the approach use by Hajime `https://goo.gl/vQfe6E` or Wifatch `https://goo.gl/YpLfSS` that seem to try to harden compromised devices.

In any case, interesting times ahead!

Event calendar

The first spring school (thanks Stefan!) on security and correctness in IoT, takes place May 8-12

in Graz, Austria. Topics range from software exploits and hardware side-channels to formal methods for security verification. Standard registration was open until April 16. More info at `http://springschool.iaik.tugraz.at/`.

The program is very interesting, and brings in some of the best in the area (including many Cryptacus people) and lots of practical labs. In addition, they offer a limited number of student stipends to cover registration.

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 `https://goo.gl/cSCcUZ`.

LatinCrypt is this year in La Habana, Cuba, running immediately after the Advanced School on Cryptology and Information Security in Latin America (ASCrypto 2017), in cooperation with IACR. The school will take place from the 17-19 September, and the LatinCrypt conference from the 20-22. Deadline for paper submission is the 8th May at 2pm GMT.

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.

See you all very soon!

Best,
Julio Hernandez-Castro