OCTOBER 2016, NO 2

Cryptacus Newsletter

October'16 Cryptacus Newsletter

Welcome to the second edition of the monthly Cryptacus.eu Newsletter, bringing you a quick glimpse into the latest developments in the IoT cryptanalysis area. We'd love you to send us your own contributions for incoming issues, comments and feedback to cryptacus.newsletter@irisa.fr

News from the Chair

by GILDAS AVOINE

Cryptacus' management committee approved in September 2016 the yearly work and budget plan. I am glad to inform Cryptacus' members that the third grant period is consequently open. Researchers interested on short-term scientific missions can apply for a grant, following the procedure described on the website of the Action, www.cryptacus.eu. All valid applications have been granted so far, so do not hesitate to apply.

Two major events will be organized during the third grant period. First of all, the Action will organize its scientific meetings on November 6^{th} and 7^{th}, 2016, in Sophia-Antipolis (France).

Members of the management committee will soon receive an official invitation. Any other researcher interested by the cryptanalysis of ubiquitous computing systems is welcome to participate in these meetings. The program will be available on the website soon.

The Action will then organize a workshop, early in 2017. The Action is looking for organizers for this workshop. If you are interested in organizing this event in your country, please contact Gildas Avoine or Bart Preneel.

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

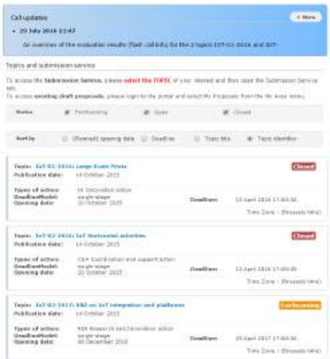
This month we have two items on our list of recommended readings. One of them is an academic paper, for which we have to thank Handan Kilinç, the other a series of news posts describing from different angles the recent massive DDoS attack suffered by Brian Krebs and others which apparently exploited a very large network of compromised IoT devices.

1. **Efficient Public-Key Distance Bounding Protocol**. Considering that products which use Distance Bounding protocols tend to be quite computationally constrained, the authors constructed the most efficient public-key DB protocol (Eff-pkDB) which is secure against distance fraud, mafia fraud and distance hijacking. It can be also converted to a strong private variant efficiently using a IND-CCA secure encryption scheme. The two protocols are the most efficient ones when compared with other protocols offering the same security level. **Handan Kilinç and Serge Vau-**

denay. *Efficient Public-Key Distance Bounding Protocol*. In Asiacrypt, 2016

2. A gargantuan DDoS attack (up to 620Gbps) directed towards journalist Brian Krebs' website was apparently based on a million-device-strong IoT botnet, including security cameras and the like. Akamai had problems defending Krebs' site so he took it down. This seems as a revenge for his recent journalistic efforts unmasking DDoS gangs. More info here `https://goo.gl/joEHDh`. Part of the problem seems to be related to 'the sheer difficulty of patching and updating IoT devices to take advantage of the latest vulnerability plugs'. Food for though and a potentially very interesting research area for some of you. Additional info on this and related security events can be read at `https://goo.gl/iGQ56r` and `https://goo.gl/bfgV4J`.

Funding News



Call updates

- 20 July 2016 12:47

An overview of the evaluation results (flash call info) for the 2 topics IOT-01-2016 and IOT-

Topics and submission service

To access the **Submission Service**, please **select the TOPIC** of your interest and then open the Submission Service tab.

To access **existing draft proposals**, please login to the portal and select My Proposals from the My Area menu.

Status ● Forthcoming ● Open ● Closed

Sort by ○ (Planned) opening date ○ Deadline ○ Topic title ● Topic identifier

Topic: IoT-01-2016: Large Scale Pilots Closed
Publication date: 14 October 2015
Types of action: IA Innovation action
DeadlineModel: single-stage
Opening date: 20 October 2015
Deadline: 12 April 2016 17:00:00
Time Zone : (Brussels time)

Topic: IoT-02-2016: IoT Horizontal activities Closed
Publication date: 14 October 2015
Types of action: CSA Coordination and support action
DeadlineModel: single-stage
Opening date: 20 October 2015
Deadline: 12 April 2016 17:00:00
Time Zone : (Brussels time)

Topic: IoT-03-2017: R&I on IoT integration and platforms Forthcoming
Publication date: 14 October 2015
Types of action: RIA Research and Innovation action
DeadlineModel: single-stage
Opening date: 08 December 2016
Deadline: 25 April 2017 17:00:00
Time Zone : (Brussels time)

There are a number of interesting European calls for H2020 projects, but the one we cover this month is possibly the most obvious one, as its topic is 'R&I on IoT integration and platforms'.

In particular, we focus this month on the call IoT-03-2017 which is a Research and Innovation action with a deadline of 25 April 2017.

The call draft specifically mentions security and privacy within its scope: 'Advanced concepts for end-to-end security in highly distributed, heterogeneous and dynamic IoT environments. Approaches must be holistic and include identification and authentication, data protection and prevention against cyber-attacks at the device and system levels. They should address relevant security and privacy elements such as confidentiality, user data awareness and control, integrity, resilience and authorisation.'

Further good news: 'The Commission considers that proposals requesting a contribution from the EU of between EUR 3 and 5 million would allow this specific challenge to be addressed appropriately.' More info on this particularly tempting call can be found at /urlhttps://goo.gl/66XM3Y.

There are many other interesting calls that we will mention in future issues. If you are interested in participating in one call and want us to highlight it in the newsletter, and to help build a consortium, don't hesitate to contact us.

We will encourage and support consortia build-up from within Cryptacus, involving as many MC members as possible.

Incoming MC and WG meetings will include opportunities to create consortia and exchange know-how to competitively apply to H2020 calls.

Open Positions

We would like to include in future newsletters open positions related to our are of interest, so please send us any employment opportunity you want to publicize. For the time being, we have these:

- Faculty Position in Distributed and Secure Hardware Systems. Ecole Polytechnique Federale de Lausanne - EPFL - School of Engineering. Permanent, Full Time Position. Deadline is 30^{th} October 2016. More info at `https://goo.gl/XhF7hf`.

- Professor in Department of Computing The Hong Kong Polytechnic University. Priority will be given to candidates with expertise in big data analytics, human-centered computing and security. Recruitment will continue until the position is filled. More info at `https://goo.gl/dK9mz6`. There are other positions at the same institution at the associate and assistant professor level (`https://goo.gl/zI8s9w`).

- Lecturer in Computer Security. University of Birmingham. If you want to join the prestigious Birmingham research group in a full time permanent position, hurry up and apply before the 9^{th} October. More info at `https://goo.gl/k78cFz`.

- If you don't have your CV at the ready, you can try Loughborough University, that offers a similar position (`https://goo.gl/paKkxv`) with a deadline on the 14^{th}.

- If the **Brexit** woes are giving you sleepless nights, this full-time permanent position at the National College of Ireland could be a good option. Offering more generous salaries in general than in the UK, this has a deadline of 18^{th} October and a remuneration of up to €78k/year. More info at `https://goo.gl/MUtA0r`.

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.

Aurélien Francillon was nice enough to send us a proposal for STSMs to Eurecom, that we added below: '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 desired 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.'

Thanks a lot Aurélien for this, and please keep these bits encouraging visitors to your institutions coming!

Blogs and posts to read

There is a black hole at the center of this particular galaxy – the GNU C Standard Library, or glibc. And at this center, in this black hole, there is a flaw. More than your average or even extraordinary flaw, it's affecting a shocking amount of code. How shocking?

```
root@staging:~# apt-get update
0% [Connecting to us.archive.ubuntu.com] [Connecting to archive.canonical.com] [
0% [Connecting to us.archive.ubuntu.com] [Connecting to archive.canonical.com] [
*** Error in `/usr/lib/apt/methods/http': double free or corruption (out): 0x0000
*** Error in `/usr/lib/apt/methods/http': double free or corruption (out): 0x0000
E: Method http has died unexpectedly!
E: Sub-process http received a segmentation fault.
root@staging:~#
root@staging:~# exit
ubuntu@staging:~$ sudo bash
*** Error in `sudo': double free or corruption (out): 0x00007fff[illegible] ***
======= Backtrace: =========
/lib/x86_64-linux-gnu/libc.so.6(+0x[illegible])[0x7f17[illegible]]
/lib/x86_64-linux-gnu/libresolv.so.2(__libc_res_nsearch+0x[illegible])[0x7f17[illegible]]
/lib/x86_64-linux-gnu/libnss_dns.so.2(_nss_dns_gethostbyname4_r+0x[illegible])[0x7f17[illegible]
/lib/x86_64-linux-gnu/libc.so.6(+0x[illegible])[0x7f17[illegible]]
/lib/x86_64-linux-gnu/libc.so.6(getaddrinfo+0x[illegible])[0x7f17[illegible]]
/usr/lib/sudo/sudoers.so(+0x[illegible])[0x7f17[illegible]]
/usr/lib/sudo/sudoers.so(+0x[illegible])[0x7f17[illegible]]
sudo(+0x[illegible])[0x7f17[illegible]]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf5)[0x7f17[illegible]]
sudo(+0x58c5)[0x7f17[illegible]]
======= Memory map: ========
[illegible]
```

I've seen a lot of vulnerabilities, but not too many that create remote code execution in sudo. When DNS ain't happy, ain't nobody happy. Just how much trouble are we in?

We're not quite sure.

This month, I will highly recommend you to actively follow the blog of Dan Kaminsky at `https://dankaminsky.com/`.

Dan is a security researcher and his blog features interesting posts with plenty of insightful views on current security issues.

Dan is best known for his work finding critical flaws in the Internet Domain Name System (DNS), and for leading what became the largest synchronized fix to the Internet infrastructure of all time.

Of the seven Recovery Key Shareholders who possess the ability to restore the DNS root keys, Dan is the American representative.

Dan is presently working on developing systems to reduce the cost and complexity of securing critical infrastructure. He also tweets actively at @dakami.

Event calendar

RFIDSec2016 (venue is Hong Kong) is on the middle of the review period and promises to be a very exciting event `http://rfidsec2016.org/`.

Cardis will be co-located with the Lightsec Crypto Workshop in Cannes from 7–10 October (see `https://2016.cardis.org/` and `https://www.cosic.esat.kuleuven.be/events/lightcrypt`.

Last but not least, the Cryptacus MC and WG meetings will also take place on the same place and dates. Registrations are open. See you all very soon!