Cryptacus Newsletter

February'17 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 more of your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by GILDAS AVOINE

Dear Cryptacus Members,

I would like to start this newsletter by thanking Milena Djukanovic, the organizer of the Cryptacus workshop that will take place next month in Montenegro, on March 14th-15th.

Milena already did a great job so far to set up the workshop in a very short time. I am sure we will have a great and enjoyable event in Sutomore next month.

A call for presentations was recently distributed around. It can be downloaded from the Cryptacus website, at `https://goo.gl/n8iyLB`. May I ask you to distribute this call to relevant mailing lists?

PhD Students and Postdocs are especially (but not exclusively) invited to submit a presentation proposal.

Note that, for each selected presentation, the travel and accommodation expenses of the speaker will be fully reimbursed. This is an opportunity for young researchers to present their work and share ideas with researchers from the scientific community.

Last but not least, the submission process is very lightweight, given that only a 1-page abstract is required by the program committee for the selection of the presentations.

Whether or not you plan to submit a presentation, you can register to the workshop using this link: `https://goo.gl/P5eCgN`.

Note that booking in the hotel of the workshop is particularly convenient, because Milena Djukanovic negociated that the room rate will include the transportation from/to the airport and the lunches.

If you have other questions, do not hesitate to directly contact Milena.

Gildas

Recommended reading

We will briefly cover in this issue two papers co-authored by the legendary Adi Shamir, investigating Smart Lights in quite some depth.

The first is *"Extended Functionality Attacks on IoT Devices: The Case of Smart Lights"*, and is authored by Eyal Ronen and Adi Shamir, both from the Weizmann Institute of Science.

They showed how the intended functionality of smart lights can be abused to build a covert LIFI communication system to exfiltrate data, even from highly secure environments. They implemented the attack

and were able to read the leaked data from a distance of over 100 meters using only cheap and readily available equipment. Particularly funny was the fact that, as a receiver, they used a 12in Meade LX200 telescope. This was an Invited paper to IEEE S&P Europe 2016.
You can read it at `https://goo.gl/LJCMOA`

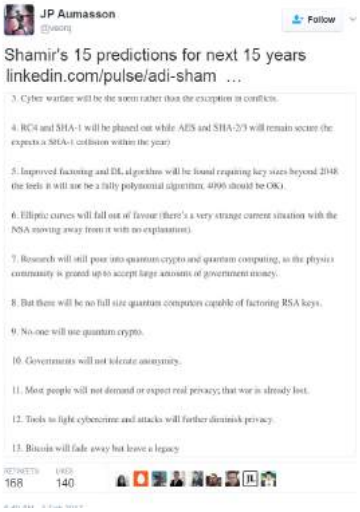
The second extremely interesting paper, on a closely related topic, is *"IoT Goes Nuclear: Creating a ZigBee Chain Reaction"*, also authored by Eyal Ronen and Adi Shamir, this time with the help of Colin O'Flynn and Achi-Or Weingarten.

I was fortunate enough to attend Shamir's fantastic presentation of this work at ESC'17 in Canach, Luxembourg. You can read more about it at `https://eprint.iacr.org/2016/1047` but I would highly recommend you to in addition visit the awesome site devoted to this line of research by Eyal at `http://iotworm.eyalro.net/` where you can find videos of them War-driving and attacking lights installed in the Weizmann, or flying a drone over a high-security building in Beer Sheva (hosting the Israeli CERT) and immediately compromising all installed lights.

This is extremely fun to watch, true, but also extremely concerning, particularly taking into account the very real possibility of creating a worm that will automatically spread unnoticed and could possibly infect all buildings in a large city if only the density of smart lights is over a threshold.

This research has been covered in a number of major generalist newspapers and news sites such as the New York Times, Forbes, Motherboard, PC Magazine, The Register, ComputerWorld, etc.

These brilliant papers will definitely contribute to validate Shamir's 15 predictions for the next 15 years, as presented in his anniversary keynote "Financial Cryptography: Past, Present, and Future" at Financial Cryptography 2016 (check `https://goo.gl/ifBptN`) particularly prediction #1 (Cybersecurity is terrible, and will get worse) and #2 (The Internet of Things will be a security disaster).



Funding News

During the recent ESC 2017, there was much talk about EU funding. There seems to be a number of good consortia building up to target (good news, Switzerland is back in!) the April call on Cryptography `https://goo.gl/6SRvF3` but most of them apparently are going for the straightforward topics of homomorphic encryption, ultra-lightweight crypto, physical cryptanalysis, quantum and automated proof techniques.

It is possible, however, that there will be room for a proposal targeting the challenge defined by 'Authenticated encrypted token research for mobile payment solutions and related applications'. If you have experience in H2020, are willing to coordinate a proposal and have ideas for seriously contributing to this challenge, please do not hesitate to contact me at jch27@kent.ac.uk to further discuss a joint bid.

Alex Biryukov's team (Cryptolux, at University of Luxembourg) is also looking for partners in Crypto, CyberSecurity and FinTech areas for this April call, but also for some of the later August ones. We will be targeting DS-07-2017 on 'Addressing Advanced Cyber Security Threats and Threat Actors' `https://goo.gl/VOQqmd`, so please drop me a line if you think you can significantly contribute to a proposal on that topic.

Of course, we will arrange in the next Cryptacus meeting in Montenegro for a slot to discuss some of these calls in detail and will plan ahead for them, focusing particularly on the August calls as by them the April one will be too close. Our aim is to facilitate the build up of consortia to successfully apply to several of these opportunities.

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.

In addition, we will discuss Marie Curie mobility grants as well.

Open Positions

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

There are still 2 open positions at Kent in the security domain, at assistant professor level, full time and permanent. Salary range is £32,958 to £46,924. Deadline is 6^{th} February, so hurry up! Please come to join an expanding team with many funding successes in Cybersecurity! More info at `https://goo.gl/tHulul`. Also, there is now an open position for a fully funded 3-years long PhD studentship with me, so if you want to apply, please check `https://goo.gl/YxDzTt`.

Other interesting positions are:

- Chair in Cyber-Secure Engineering Systems and Processes at Cranfield University - School of Aerospace, Transport and Manufacturing (SATM). This professorship is full-time, permanent. One of the topics they're interested in is 'Security of Internet of Things (IoT) devices and systems within industrial settings'. The closing date is 9^{th} February 2017. Initial salary is £66,366. More info at `https://goo.gl/aZczjS`
- Lecturer/SL/Reader in Cyber Security at the School of Computing Science, University of Glasgow. Another full time, permanent position with a salary range between £33,943 and £55,998 per annum. Deadline is the 3^{rd} of February. More info at `https://goo.gl/ioChFq`.
- Lecturer or Senior Lecturer in Internet of Things (IoT) and Cyber security at Liverpool John Moores University - Computer Science and Electronics and Electrical Engineering. Starting salary is in the range £39,324 to £48,327. Full time, permanent position. Deadline is 23^{rd} February 2017. More info at `https://goo.gl/aiqfxq`.
- Associate/Assistant Professor in Formal Methods Technical University of Denmark - DTU Compute. Deadline is 5^{th} February 2017. Full time, permanent position. For further info or to apply, check `https://goo.gl/3CHl2z`.
- Lecturer or Senior Lecturer or Reader in Systems for the Internet of Things at the University of Edinburgh - School of Informatics. Closes on the 15^{th} February 2017. Another full time, permanent position. Salary range is £39,324 to £55,998. Edinburgh is one of the nicest places to leave in the UK, its university is extremely prestigious and the cost of living and accommodation is reasonably low. Also, they're very welcoming of foreigners, much more than their neighbors to the South, and there's the off-chance possibility that they might not Brexit as they voted against and they current leaders are strongly opposed to it. Or maybe they will do, later claim independence and try to re-enter the EU. For more info, visit `https://goo.gl/KNB9QD`.
- Lecturer- Internet of Things, at University of Essex - School of Computer Science and Electronic Engineering. Full time, permanent position, with a deadline on the 7^{th} February 2017. The position is based in Colchester, one of the most beautiful and greenest campuses in the UK, and its salary range is £39,324 to £46,924. More details at `https://goo.gl/cSXjXP`.
- Professor in Department of Computer Science (with subsequent Department Headship) at Durham University - Department of Computer Science. This is in my opinion one of the most attractive position in this February list, as Durham is a small and beautiful city and the university is one of the best in the UK. The initial salary will be circa £85,000 and may rise significantly higher, typically around £120,000 depending on experience and achieved targets.

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.

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.

Blogs and posts to read

On his blog 'Schneier on Security', Bruce covers the IoT Ransomware attack against a Luxury Austrian Hotel, with links to a New York times article and one on the local Austrian press. He disputes some of the most alarming elements of the story, but offers a very worrying and probably prophetic personal opinion: 'I expect IoT ransomware to become a major area of crime in the next few years. How long before we see this tactic used against cars? Against home thermostats? Within the year is my guess. And as long as the ransom price isn't too onerous, people will pay.' You can read more, and many interesting comments from readers, at `https://goo.gl/sc92MA`.

Another interesting reading can be found in the article 'How the Internet of Things will affect security & privacy' by Andrew Meola for Business Insider at `https://goo.gl/He3tCE`.

Event calendar

Of course, the main dish in our event calendar is the next Cryptacus Management Committee & Workshop in March, 14-15th, in Sutomore, Montenegro. It will be organised by Milena Djukanovic.

Euro S&P is this year in Paris, 26-28 April. A must! More at `https://goo.gl/fvjBVN`

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`.

Esorics is this year in beautiful Oslo, from 11-15 September. Submission deadline is April 19^{th}. Hope to see many of you there!

Last but not least, Agusti Solanas is editing an Special Issue in the International Journal of RF Technologies Research and Applications (ISSN: 1754-5730) on 'Advances in RFID for Smart Cities' with a deadline of 17^{th} March and a publication date in September. More info at `https://goo.gl/YbjggH`

See you all very soon!

Best,
Julio Hernandez-Castro