July 2017, No 10

Cryptacus Newsletter

July'17 Cryptacus Newsletter

Welcome to the July edition of the monthly Cryptacus.eu newsletter, offering a glimpse into recent developments in the IoT cryptanalysis and related areas. We'd love to receive many more of your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by Gildas Avoine

Dear Cryptacus Members,

The summer break is coming soon, and this newsletter is the last one of the current academic year.

The next one will be in September. I hope you will enjoy your summer break and come back well rested in September.

On November 16-18, 2017 in Nijmegen (Netherlands) Lejla Batina will organize Cryptacus' workshop. You can already motivate your PhD students and colleague to submit a presentation.

A call for presentation will be published during the summer. As I told you in the last newsletter, the invitation letters for the MC members will also be sent soon.

Another major action that will be launched soon, is the writing of a book on the topics addressed in Cryptacus.

This idea comes from Montenegro's meeting, and Julio and I currently work on the organization of this collaborative work. Cryptacus' members will receive an email soon about this work.

I am sure many of you will be volunteers to work on this issue, possibly with some of your PhD Students.

Have a great Summer!

Gildas

Recommended reading

This month we will briefly cover an important paper just uploaded to the WEIS 2017 program webpage titled *Standardisation and Certification of the 'Internet of Things'* by Eireann Leverett, Richard Clayton and Ross Anderson.

You can read a preliminary version of it at `https://goo.gl/ih2MTG`.

The authors present their report on a research project commissioned the EU on the future of safety regulations once computers IoT is everywhere. Authors reason that the EU already regulates many aspects of the safety of vehicles, medical devices, electrical equipment, domestic appliances and even toys and that as these devices become 'smart' their vulnerabilities may be remotely exploited, with consequent risks.

These systems are certified under a disparate range of European, national, industry and other schemes so in their work they describe the problems and outline the opportunities for governments, industry and researchers.

The controversially state:'The EU is already the world's main privacy regulator, as Washington doesn't care and nobody else is big enough to matter.'

This will generate huge opportunities and challenges, and change the environment as we see it now. For example, they claim that safety and security are merging: safety engineers are going to have to learn all about security, and vice versa.

Interesting food for though.

Funding News

We have been given early access to the next set of EU Horizon2020 draft work programmes.

These are important documents - describing all the EU research funding calls that will happen between 2018 and 2021.

This is a great opportunity to get ahead of the game, plan early and start talking to collaborators.

Although off-putting in size, these documents outline all the calls, budgets and deadlines for the next three years: 2018-2021 (with the exception of the ERC that publishes annually).

We cannot share these documents publicly, but will be happy to answer your questions on particular calls if you send them to me by email.

Use this opportunity to check calls in your area of interest and buy yourself months of extra time before the calls are published later in the year or in coming years.

As a brief taster, the areas most relevant to the Cryptacus aims are perhaps those covered in the Secure Societies. in particular we want to highlight the following calls: SU-INFRA02-2019 on 'Security for Smart Cities and soft targets in Smart cities'. Interestingly, subtopic 3 on 'Understanding the drivers of cybercriminality and new methods to prevent, investigate and mitigate cybercriminal behaviour' has a description around IoT and how it is an increasingly interested target for cybercriminals.

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, China 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`.
- Hamilton Professorships in Computer Science at Maynooth University. The areas of interest cover, between others, Cybersecurity and Privacy. Plenty of time to decide whether to apply, with a deadline on Friday 20th of October. Salary could be €110,060 to €139,501 p.a. for Professor A and €80,650 to €106,655 p.a. for the Professor B range. More info at `https://goo.gl/LSvKhM`.
- 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`.
- There is also an exceptional opportunity at the increasingly active and prestigious security group at the Vrije Universiteit Amsterdam. The post is for an Assistant or Associate Professor position in Systems Security, with a salary from €3605 to €6438. More info at `https://goo.gl/5bWHl8`.

In addition, there are a good number of positions on the wrong side of the channel:

- 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`.

- Lecturer/Senior Lecturer in Cyber Security at De Montfort University - Faculty of Technology. De Montfort is recruiting heavily in recent times, and clearly is trying to attract talent and build a good cybersecurity team. Deadline for applications is the 2nd of July. More info at `https://goo.gl/0tK1AX`

Last, but not least, our CRYPTACUS colleague Billy Brumley (you can contact him at billy.brumley@tut.fi) sent us this position at his institution:

- Tenure Track at Assistant Professor or Associate Professor level, with a focus on software security, hardware security, critical systems security or network security at Tampere University of Technology. The deadline is 28 Aug. More information at `https://goo.gl/9UCn16`

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.

Please send your willingness to receive STSMs proposal to me for publishing here. Until I do not have any more, I’ll just publish mine.

University of Kent

- 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

New Fund for investing on IoT start-ups

Trend Micro, the well known security company, has recently launched a $100 million fund to invest in promising start-ups in the area of IoT security.

The company current value is around $7.5 billion, and it is present in over 50 countries, with over 5,000 staff, and is best known for IT security products that include threat detection and antivirus. A spokesperson said:’Working with these investments will uncover insights into emerging ecosystem opportunities, disruptive business models, market gaps and skillset shortages.

These learnings will influence Trend Micro’s cybersecurity solution planning across the company’. The form is looking at making 15-20 investments per year. If you’re interested in this initiative, please check `https://goo.gl/6pacxQ`.

Not so smart, robbing smart vending machines

A funny piece of news was the revelation that a number of CIA contractors were fired for stealing from a smart vendor machine. The investigation, unveiled by BuzzFeed after requesting a FoIA, showed that the total amount of snack stolen was of $3,314.

They used some sort of manipulates payment cards after unplugging a cable connecting the machines to their electronic payment system.

They were caught after surveillance cameras at several vending locations recorded their moves.

They admitted to the thefts. All surrendered their CIA badges, were escorted from the building by security, and fired by their respective contract employers.

The Department of Justice declined to press charges. More info here `https://goo.gl/9wY5bw`.

Hypponen’s Bleak Forecast

Mikko Hypponen, the chief research officer at F-Secure, gave a very interesting but arguably pessimistic interview to The Reg (more at `https://goo.gl/cwn1aj`) discussing IoT security.

Hypponen says IoT is unavoidable. "If it uses electricity, it will become a computer. If it uses electricity, it will be online. In future, you will only buy IoT appliances, whether you like it or not, whether you know it or not."
He added: "Home appliance manufacturers will be adding connectivity to every device, no matter how mundane, because the price of adding it will be marginal. Those devices will not be going online to benefit the consumer, they will be going online to benefit the vendor."
If this was not worrying enough, he affirmed "They want analytics. In 10 or 15 years, they will add this 2-cent chip on every toaster. Now they know where their customers are, on which side of the city, how often do they toast, at what time of day, with what kind of bread, how often there are failures. We can't avoid the IoT revolution by refusing to play part."
"Consumer appliance vendors which are serious about [security] are very hard to find," said Hypponen, "because cybersecurity is not a selling point for washing machines. Price is the most important selling point. This means we are setting ourselves up for failure."
Interesting thoughts that, if true, guarantee hard work for us Cryptacus people for many years to come.

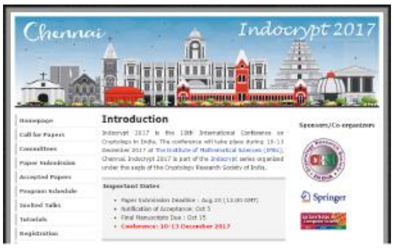
Gone with the wind

A very interesting piece published in WIRED recently (`https://goo.gl/cCAsuT`) showing yet another potential hacking target that no-one though of previously, wind-farms. For two years researchers at the University of Tulsa have been pen-testing wind farms around the United States and found some glaring vulnerabilities. They will present some of the technical details at Black Hat. After bypassing the physical security put in place (which seems to be exceedingly easy, most are just protected by a PIN or a lock) and planting a Raspberry Pi in a single turbine, they managed to compromise all the ones in the windfarm and mount attacks able of stopping then, repeatedly and suddenly triggering their brakes to damage them, and relaying false feedback to operators to prevent the sabotage from being detected. As Prof. Staggs, the leader researcher, said "Once you have access to one of the turbines, it's game over."
Quite interesting stuff and a new critical domain in desperate need for security.

Event calendar

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.



Homepage
Call for Papers
Committees
Paper Submission
Accepted Papers
Program Schedule
Invited Talks
Tutorials
Registration

Introduction

Indocrypt 2017 is the 18th International Conference on Cryptology in India. The conference will take place during 10-13 December 2017 at The Institute of Mathematical Sciences (IMSc), Chennai. Indocrypt 2017 is part of the Indocrypt series organized under the aegis of the Cryptology Research Society of India.

Important Dates

- Paper Submission Deadline : Aug 20 (13:00 GMT)
- Notification of Acceptance: Oct 5
- Final Manuscripts Due : Oct 15
- Conference: 10-13 December 2017

Sponsors/Co-organizers

Springer

The 16th IMA International Conference on Cryptography and Coding will take place in St Catherine's College, University of Oxford from 12-14 December. The deadline for submission is the 14th of July. This is a prestigious and venerable conference with an excellent Program Committee. More info at `https://goo.gl/KejTXB`.

See you all back in September!

Best,
Julio Hernandez-Castro