Cryptacus Newsletter

September 2017 Cryptacus Newsletter

Welcome to the September edition of the monthly Cryptacus.eu newsletter, offering a glimpse into recent developments in the cryptanalysis of IoT & related areas. Send more of your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by GILDAS AVOINE

Dear Cryptacus Members,

I hope your all enjoyed your summer break. The Cryptacus' newsletter is back, and I am pleased to announce many good news.

First of all, the COST Association announced this summer that it has been granted extra budget (EUR 6.67 million) from the European Commission. This has mainly been used to increase the budget of running COST Actions, including Cryptacus.

Another news from the COST Association is that Karina Marcus is the new science officer in charge of our action, replacing Luule Mizera. It was a great pleasure to work with Luule since February 2015. I would now like to welcome Karina, and I am looking forward to work with her.

Following the last Cryptacus event, Milena Djukanovik concatenated the abstracts received from the speakers in order to issue a booklet. It will be available on the Cryptacus website very soon.

About the website: I already told you that Pascal Junod (Switzerland) left Cryptacus, given he got a new position in a private company. Pascal was our website manager, and he has been replaced by Ludovic Perret from France. I would like to kindly thank Ludovic for accepting to take care of this new role.

As you know, the next Cryptacus event will be in Nijmegen (The Netherlands) on November 16th-18th. A website has been created by Lejla Batina and Veelasha Moonsamy and it is now publicly available : at `https://cryptacus.cs.ru.nl/index.shtml`

The official invitations will be sent to the MC Members in the coming days, and I will send to this mailing list, next week, more details about the scientific agenda of the workshop.

Please, note that a call for presentations will also be published next week. You can already write - or invite your PhD students, Postdocs, colleagues, etc. to write - a short proposal for a presentation, as done in Montenegro.

Finally, as already announced before the summer, the MC decided that the Action should issue a book about the cryptanalysis in ubiquitous computing systems. The book should be published before the end of the Action, namely December 2018. A draft of call for chapters has been drafted and it will soon discussed by the working group leaders and vice-leaders. We expect to release the final call for chapters to the Cryptacus community by the end of September.

As promised, many good news in this letter, and many forthcoming scientific activities. Have a great September!

Gildas

Opportunities

ISO SC 27 WG2 call for contributions

We thank Orr Dunkelman for pointing us towards a call for contributions by ISO SC 27 WG2. This is the ISO work group that deals with Crypto (it is aptly named 'Cryptography and security mechanisms'), and the discussion seems to be of relevance to the CRYPTACUS action. The deadline for the contributions is the 15th of September.

This request has to do with a first move to study the possibility of standardising tweakable block ciphers and permutations. In this vein, they want your views on the following questions:

1. What advantages or disadvantages do tweakable block ciphers have over conventional block ciphers and cryptographic permutations?
2. What advantages or disadvantages do cryptographic permutations have over conventional block ciphers and tweakable block ciphers?
3. Are there any tweakable block ciphers or cryptographic permutations that are worth considering for standardization?
4. Are there any modes of operation for tweakable block ciphers or cryptographic permutations that should be considered as well?
5. Similar to cryptographic permutations and tweakable block ciphers, are there other mature symmetric-key primitives that should be considered for standardization?

You can get more info at the webpage of the committee `http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg2`.

Please send your contributions to Atul Luykx or Tomer Ashur, both at KU Leuven, Who are the rapporteur and co-rapporteur, respectively.

ENISA Call for IoT Experts

The European Union Agency for Network and Information Security (ENISA) has launched a Call for Participation to invite experts in security of Internet of Things into its expert group. The creation of the ENISA IoT SECurity (IoTSEC) Experts Group aims at gathering experts in the domains of the entire spectrum of Internet of Things to exchange viewpoints and ideas on cyber security threats, challenges and solutions. I highly recommend you to read more about the IoTSEC group at `https://resilience.enisa.europa.eu/iot-security-experts-group-1` and join it by filling the form at `https://goo.gl/tzEJkC`. It will be great to have a more significant presence from Cryptacus members in a group that will likely influence European Security policies regarding IoT for years to come.

Recommended reading

This month we will cover a paper called 'Hacking Robots Before Skynet' by Cesar Cerrudo (@cesarcer) who is the CTO of IOActive Labs and Lucas Apa (@lucasapa) that is a Senior Security Consultant. Their work was presented at the HITB GSEC Conference in Singapore. The organisers have uploaded all contributions to `https://gsec.hitb.org/materials/sg2017/`.

The authors presented an extensive piece of work investigating a variety of robots, from home robots to industrial ones, and found a worrying number of security issues. A non-exhaustive list of the problems included insecure communications, memory corruption issues, remote code execution vulnerabilities, file integrity and authentication issues, lack of authorisation, the use of weak crypto, serious firmware update problems, and lots of privacy issues steaming from a variety of undocumented features.

Hacking robots could have a number of undesirable impacts, dependent on the environment they are used on. For example, the authors mention that at home they mostly lead to privacy issues, with a minor possibility of human and property damage. The compromise of robots in use on business and industry environments lead naturally to espionage, human and property damage and to the compromise of corporate and business networks. It is in a healthcare or military context where successful attacks can be more dangerous, according to the authors, as these will lead to direct threats to human lives.

They highlighted that finding robots in large networks is easer than expected, thanks to mDNS (multicast DNS) and the fact they tend to use only a small range of hostnames such as nao.local or ur.local and serial numbers such as 011303P0017.local.

I was particularly interested in their analysis of robots as dangerous insider threats, mentioning that they come frequently equipped with multiple microphones, HD and sometimes even 3D cameras that can be turned into spy cams, and

loaded with privacy-relevant algorithms such as in-built face recognition software. This landscape make the ideal targets to gain extremely valuable intelligence from inside a company and of course the bunch of robots they examined offered little to none security protections against these attacks.

They have produced an hilarious video, in which a hacked UBTech Alpha 2 goes 'Chucky' `https://youtu.be/9A4ZQgzfl0Y` that I highly recommend you.

A somewhat less impressive but highly educational video showing SoftBank's NAO and Pepper robot being used as an espionage tool can be seen at `https://youtu.be/DSSTUvqMB3M`.

Even worse than all their findings (they are many more than the referenced here, I strongly recommend you to read their paper) was the vendor's response after they responsibly disclosed they vulnerabilities found. Most of them reacted quite positively to the findings, and in some cases they even promised a quick patch or firmware update but unfortunately 3 months later many haven't produced or deployed any solutions.

The researchers found manufacturers were way more focused and more ready to invest in marketing than in security. The authors found that too many research projects moved into production without adding security, and that the very basic human safety protections they come with can be easily and remotely disabled so that robots can kill and hurt people, and also damage property. Something needs to be done to address these threats, and very urgently.

A very nice piece of practical research that brings to our attention multiple security issues in a relatively lesser known area that shares many characteristics with IoT.

Funding News

The European Commission will organise a number of information days in Brussels on the upcoming 2018-2020 calls for proposals in the last Work Programme of Horizon 2020 (to be published in October).

These events will provide information on the content of the calls and will often be combined with dedicated brokerage events to support prospective applicants with finding partners for projects.

The following events are planned in the coming months.

- 3-4 October 2017 - Industrial Innovation Information Days 2017 -Registration is already open.
- 23-25 October 2017 - Energy Challenge Information Days - Registration opens in September.
- 26-27 October 2017 - 'Cities of the Future 2017' International Brokerage Event - Save the date.
- 8-9 November 2017 - Climate Societal Challenge Information Day and Brokerage Event - Registration opens in September.
- 9-10 November 2017 - ICT Proposers' Day 2017 in Budapest - Registration is already open.
- 14-17 November 2017 - Food Security Societal Challenge 2 Infoweek - Registration opens in late September.
- 8 December 2017 (TBC) - Health Societal Challenge Information Day - Save the date. Registration opens in October.

Furthermore, there are a series of national events planned, check with your National Contact Point for further info at this stage.

Open Positions

Please send us any employment opportunity you want to publicize in the newsletter.
Asking for a friend when oh when there will be a more serious and concerted effort from Europe to attract talent willing to leave the UK after the disastrous Brexit. Fine countries such as New Zealand, Australia, Canada, China and Ireland are unashamedly moving in this direction. When will France, the Netherlands and Germany follow?

- Optus Cyber Chair at La Trobe University in Melbourne - Australia. Full time, permanent position. The Optus Cyber Chair is anticipated to be a prominent appointment of academic leadership at the level of professor (Level E) and is a continuing role at La Trobe. Candidates must have academic experience and performance together with an international profile consistent with the expectations of appointment as a full professor at La Trobe. The incumbent is expected to conduct and lead innovative and high impact research at an internationally distinguished level and produce high quality publications resulting from that research. More info at `https://goo.gl/Teo81S`. Deadline is the 18th September.

- Professor/Chair in Cyber Security at the Victoria University of Wellington in Wellington, New Zealand. Another interesting position from down under. A perfect fit for lovers of The Lord of the Rings, The Hobbit, The Chronicles of Narnia and/or earthquakes and sheep. Another full time, permanent position. Bad jokes aside, the University is ranked in the top 2% world-wide and Wellington has been rated in 2017 as the World's best city for quality of life. They state in the ad that they have a very strong link with Carnegie-Mellon, and look to, in collaboration with an industry partner, host a CSIRT. Deadline for applications is the 19th of September. Additional info at `https://goo.gl/JebwLx`

- Professor in the Department of Computer Science at Durham University - Department of Computer Science. This position in one of Britain's finest universities is not particularly earmarked for cybersecurity, but they seem to be open to any outstanding candidate and to the best of my knowledge there is no-one working on cyber at Durham and there's appetite for these skills. The deadline is on the 22nd of September, salary starts at £61K, and there is more info at `https://goo.gl/a31Tmx`.

- 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`.

- Lecturer and Senior Lecturer in Cyber Security at Lancaster University, Department of Computing and Communications. These are two full time and permanent positions at one of the few prestigious GCHQ accredited Centers of Excellence in Cybersecurity Research. The people at Lancaster are building one of the largest and most visible cybersecurity groups in the UK and this investment is starting to bore fruit. The common deadline for these positions is the 3rd of November. The Lecturer position `https://goo.gl/G2NtmG` has a salary range of £34,520 to £47,722 and the Senior Lecturer position `https://goo.gl/bRQdpu` goes from £50,618 to £56,950.

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.

- I will be very happy to receive anyone interested in investigating randomness generation and testing, particularly on IoT devices.

Blogs, posts and other good reads

Mirai-based malware vaccine could protect insecure IoT devices

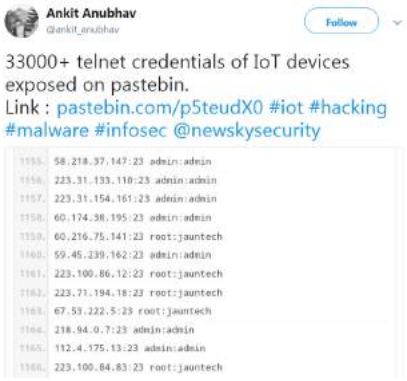
A white worm derived from the Mirai botnet aims to protect the most insecure IoT devices. The idea is not totally original, we discussed a similar concept in a past newsletter, and not free of legal or ethical implications either: to abuse the vulnerability of these devices to inject a worm that patches them. Its creators argue that it is 'similar to the epidemiological approach that creates immunity with a vaccine by exposing the immune system to a weakened form of the disease.'

There still remain many issues: for example, some devices cannot be fixed because they have hard-coded passwords or back doors. Others have software or firmware vulnerabilities that are very hard to patch because of a lack of a software update mechanism.

The idea was presented and developed in a paper called 'AntibIoTic: Protecting IoT Devices Against DDoS Attacks'. This worm also tries to notify the owner or remedy the problem on the owner's behalf by changing credentials, patching software or updating firmware if at all possible. You can read a preprint in `https://goo.gl/x1rMpF`.

AntibIoTic crosses many legal and ethical lines, and I am for one surprised academics have proposed this approach without including a deeper legal analysis.

More than 33,000 telnet credentials from IoT devices exposed



Not much to say about this: More than 33,000 telnet passwords of different IoT devices were exposed publicly on pastebin for all to see and download before the admins deleted them. Right now they will form part of the arsenal of all your future attackers, so please get them and test none of your devices is open to these credentials, and that none of your IPs is listed.

Death in the Car Wash

At Black Hat 2017, one of the most interesting hacks was that of a car wash, surprisingly with life-threatening consequences for passengers. ”We’ve written an exploit to cause a car wash system to physically attack; it will strike anyone in the car wash” one of the authors said. ”We think this is the first exploit that causes a connected device to attack someone."

They showed how a LaserWash car wash system, from manufacturer PDQ, could be breached. An attacker could close one or both doors, trapping passengers inside. To keep passengers in the vehicle, a hacker could command the car wash to blast water constantly at the vehicle, making it a challenge to open its doors. If a driver attempts to escape the hacked device while the car wash’s door is open, the hacker could command a door to open and close repeatedly to strike when passengers exit the vehicle. Or the attacker could hit the car or passengers with a mechanical arm within the car wash. The hack was relatively simple, bypassing the authentication mechanism and enabling them to manipulate a variety of functions.

At the core of the hack is the fact that the entire platform for the washing machine operates Windows CE, which Microsoft killed off in 2013. Sadly, manufacturers are still building futuristic devices like an Internet-connected car washing machine on top of a dead platform.

While not all of the car wash models are connected to the Internet, at least 150 are according to the Shodan search engine which catalogs IoT devices connected to the public-facing Internet. Who would have thought five years ago that car washes could be Internet connected, or that the simple act of going to a car wash could possibly be life-threatening?

You can read the rest of the article at `https://goo.gl/S35y1o`.

Event calendar

Eurocrypt 2018 will take place in Tel Aviv, Israel, from April 29 to May 3. The submission deadline is the 19 September, with notification on the 15 January. Orr Dunkelman is the General Chair.

Financial Cryptography and Data Security 2018 (FC18) is taking place, as usual, in an exotic location. This time in Nieuwpoort in Curacao, from February 26 to March 2. The submission deadline is the 15 September, and the good news will arrive on the 17 November.

The 2018 edition of the new kid on the block, a.k.a. Real World Crypto will take place in Zurich, Switzerland, from January 10-12, 2018. The submission deadline is 5 October, with a quick notification on the 4 December.

See you all back in October!

Best,
Julio Hernandez-Castro