Cryptacus Newsletter

January'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 your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by GILDAS AVOINE

Happy new year to everyone, and happy Cryptacus 2017!

This year will be highly important for Cryptacus, especially with the organization of a workshop at Sutomore, in Montenegro, on March 14th and 15th. This workshop is open to everyone - not only Cryptacus members - and a call for presentations will be published very soon. Researchers interested in presenting their work will be invited to submit a one-page abstract describing their presentation. Selected speakers will be fully reimbursed by Cryptacus, including travel, hotel, and meals. More information will be published in the coming days on the mailing list of the Action, including information for the submission and for booking the hotel.

Apart from this event, I also encourage you to submit proposals for Short-term Scientific Missions. STSMs are a great opportunity for researchers to do a 1-week to 3-month stay in a foreign country. If you are interested in benefiting from such an opportunity, please have a look at this page: https://www.cryptacus.eu/en/stsm/

Note that there is still plenty of money for funding STSMs. Given that the current Grant Period will be completed at the end of April 2017, your STSM must finish before the end of April, or start after the beginning of May.

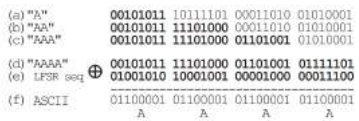
If you are interested to set up a consortium for a H2020 proposal, do not hesitate to send an email to Julio, who can spread this information in the newsletter, or you can send yourself an email to the mailing list of the Management Committee.

Finally, if you are interested in organizing a Cryptacus event in 2017 or 2018, please contact me. The Management Committee will soon discuss about the activities of the next Grant Period that will start in May 2017.

Once again, have a happy new year!

Gildas

Recommended reading

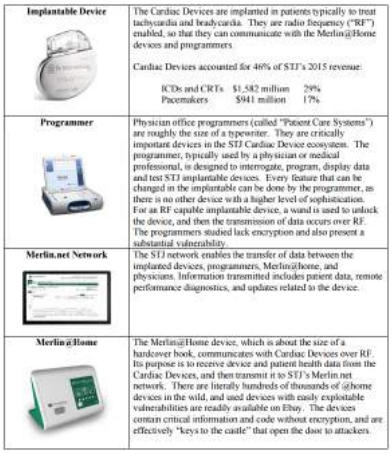


We will start 2017 by highlight a paper that has received a fair share of media attention and is specially dear to our hearts, as it benefited from a STSM within Cryptacus. Its title is *"On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them"*, and is authored by Eduard Marin, Dave Singelée, Flavio D. Garcia, Tom Chothia, Rik Willems, and Bart Preneel. It appeared in the Proceedings of the 32^{nd} Annual Conference on Computer Security Applications, pp. 226–236. ACM, 2016. You can read it at `https://goo.gl/MKPJ69`
The findings presented in the paper were discussed in Security Week, The Register, the Inquirer and The Sun, to mention only some of the many media outlets that reflected on this

interesting research.

2016 was not a good time to be a major manufacturer of Implantable Cardiac Defibrillators, and the future looks even bleaker. Apart from the above paper, which is clearly bad news for business in general, the controversial Muddy Waters Capital published in August a very strong short recommendation on St. Jude Medical, Inc. `https://goo.gl/noGpyQ`.

It claimed their pacemakers, ICDs, and CRTs should be recalled immediately. These devices collectively generated 46% of their 2015 revenue, and they seemed to suffer from serious product safety issues leading to unnecessary health risks. They continued describing two types of attacks against the devices: a *crash* attack that causes Cardiac Devices to malfunction, including by apparently pacing at a potentially dangerous rate; and a battery drain attack that could be particularly harmful to device dependent users.



Implantable Device	The Cardiac Devices are implanted in patients typically to treat tachycardia and bradycardia. They are radio frequency ("RF") enabled, so that they can communicate with the Merlin@Home devices and programmers. Cardiac Devices accounted for 46% of STJ's 2015 revenue: ICDs and CRTs $1,582 million 29% Pacemakers $941 million 17%
Programmer	Physician office programmers (called "Patient Care Systems") are roughly the size of a typewriter. They are critically important devices in the STJ Cardiac Device ecosystem. The programmer, typically used by a physician or medical professional, is designed to interrogate, program, display data and test STJ implantable devices. Every feature that can be changed in the implantable can be done by the programmer, as there is no other device with a higher level of sophistication. For an RF capable implantable device, a wand is used to unlock the device, and then the transmission of data occurs over RF. The programmers studied lack encryption and also present a substantial vulnerability.
Merlin.net Network	The STJ network enables the transfer of data between the implanted devices, programmers, Merlin@home, and physicians. Information transmitted includes patient data, remote performance diagnostics, and updates related to the device.
Merlin@Home	The Merlin@Home device, which is about the size of a hardcover book, communicates with Cardiac Devices over RF. Its purpose is to receive device and patient health data from the Cardiac Devices, and then transmit it to STJ's Merlin.net network. There are literally hundreds of thousands of @home devices in the wild, and used devices with easily exploitable vulnerabilities are readily available on Ebay. The devices contain critical information and code without encryption, and are effectively "keys to the castle" that open the door to attackers.

They concluded: "STJ's apparent lack of device security is egregious, and in our view, likely a product of years of neglect". Predictably, St. Jude Medical sued Muddy Waters over their hacking claims, and this lead to an interesting legal battle in which MW produced even more evidence of hacks and showed additional vulnerabilities.
To top it all, in October the FDA issued an urgent warning after STJ devices 'ran out of battery' three months too early, a defect that had lead at the time to at least 2 deaths. You can read more about this catastrophic development at `https://goo.gl/cn5cSg`. Curiously enough the short-selling following the MW report this time would have not generated massive profits, as the stock price of STJ was $81.88 when the report was published and never fall below $77.82 despite all the evidence against their products. All in all, a good case for research impact and, interestingly, an example that major security weaknesses can be a good predictor of other, even more egregious, technical shortcomings.

Please send your contributions and suggestions for future issues of this newsletter.

Funding News

As we have shown in the last issues of this newsletter, there is no shortage of European calls for H2020 projects in our area of interest or closely related ones.

We will arrange, in the next Cryptacus meeting in Montenegro, a 2 hours H2020 session in which we will discuss some of these calls in detail and will plan ahead for them, focusing particularly on the August calls. 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 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. More info at `https://goo.gl/tHulul`

Other interesting positions are:

- Lecturer/Senior Lecturer in Cyber-Physical Systems, University of Cambridge. Deadline is 10^{th} January 2017. Salary in the range £39,324 to £55,998 per year. Full time, permanent position. More info at `https://goo.gl/oQMRZo`. They explicitly mention Internet-of-Things/IoT, wearable technologies and security & privacy.

- Chair in Computer Science, at the University of Edinburgh. This professorship is full-time, permanent. Some of the topics they're interested in are: algorithmic foundations of data privacy, algorithmic aspects of security and cryptography, and quantum algorithms/complexity. The closing date is 31 January 2017. More info at `https://goo.gl/Z7C8cg`

- 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`.

- Lectureship/Senior Lectureship in Computer Systems and Security at the Department of

Computing of Imperial College London. The position is again full-time, permanent. Deadline is the 24th January. They mention in their areas of interests network security, applied cryptography, crypto-currencies and blockchain technologies.

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:

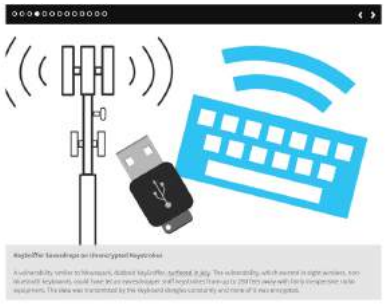
"At Eurecom we are actively working on analyzing embedded devices software and building methodologies and tools for this. An example of that is our open source Avatar Framework (see `http://s3.eurecom.fr/tools/avatar/`) which is aimed to reverse engineer devices and search for vulnerabilities. We are 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.

If you want to see what kind of work I'll be interested in carrying out, check my paper at RFIDSec'16 or the preliminary presentation at the WG4 meeting.

Contact me at jch27@kent.ac.uk if interested and/or for further info.

Blogs and posts to read



Chris Brook has recently published an interesting piece called '2016: The Year in IoT Insecurity' at `https://goo.gl/As1laR` where he makes a recap of some of the biggest stories of the past year in IoT security.

Another interesting read is '17 for 17', a series of Q&A with leading Microsoft researchers across the World and across disciplines, where they share their general prediction for 2017 to 2027 on a number of Computer Science related topics, where computer security and IoT are covered directly or in passing in many of the answers. Truly though provoking and inspiring reading at `https://goo.gl/bSrcQM`

If you want to check with another doctor, TechRepublic has also published a list of predictions, this time more focused on IoT, at `https://goo.gl/7DJIH8`

Event calendar

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

Another quite interesting event is the Early Symmetric Crypto (ESC), that will take place 16-20 January in Canach, Luxembourg. Organised by Alex Biryukov it will cover, as one of their Special Topics, Lightweight Cryptography for the IoT. The aim of the workshop is to bring together leading experts and talented junior researchers, and to let them exchange ideas, and discuss open problems in an informal atmosphere. More info at `https://goo.gl/EeoWw7`.

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`.

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