October 2017, No 12

Cryptacus Newsletter

October 2017 Cryptacus Newsletter

Welcome to the October 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,

The program of our Cryptacus' workshop in Nijmegen (Nov. 16th-18th, 2017) is currently under preparation. You still have time to submit a short abstract to give a presentation, until October 15th, 2017.

If you are interested in giving a talk, please submit a short abstract, according to the instructions provided on the web page `https://cryptacus.cs.ru.nl/submission.shtml`

Speakers will be reimbursed even if they are not MC Members. Note also that a demo session about hardware and software tools will be organized. If you are interested in presenting such a tool, please contact Lejla Batina.

Another important point I would like to speak about in this newsletter is a specific budget to allow members of Inclusiveness Target Countries (ITC) to attend conferences if they give a talk or present a poster.

This is a new tool provided by COST, and a significant budget for it has been allocated by the COST Office.
The requirements to get the grant are: (i) the application must be submitted at least 45 days before the conference start date, (ii) the applicant must be engaged in an official research programme as a PhD Student or postdoctoral fellow (iii) the applicant must give a talk or present a poster during the conference.
As for STSMs, the application procedure is lightweight and processed through the e-cost online application. Do not hesitate to apply! The guide for applicants is available at `http://www.cost.eu/ITC_conferencegrants_userguide`.
Best regards,

Gildas Avoine

Opportunities

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://goo.gl/uS1o4S` and/or join it by filling the form at `https://goo.gl/tzEJkC`.

It will be great to have a more significant presence of Cryptacus members in a group that will likely influence European Security policies regarding IoT for years to come.

The first meeting is taking place

in the Europol Headquarters in the Hague later this month.

Recommended reading

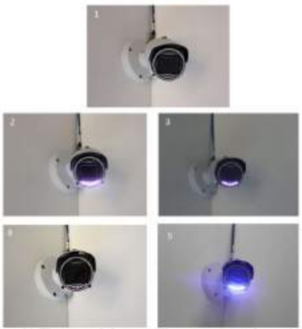


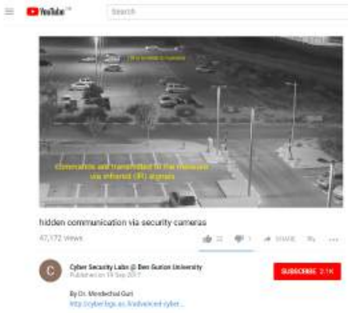
Figure 14. The transmitting surveillance camera, as it seen by a human observer (1) and different camera receivers (2-5).

This month we will cover a great paper titled 'aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR)' that you can find at `https://arxiv.org/abs/1709.05742`.

Its authors are Mordechai Guri, Dima Bykhovsky, Yuval Elovici, from the Ben-Gurion University of the Negev and the Shamoon College of Engineering in Israel.

It deals with two of my favourite topics: data exfiltration and IoT security. In this case, they propose to bypass air gapped systems by infecting infrared cameras and prove it is possible to both send and receive information to/from them without any human noticing because, of course, infrared light is invisible to humans.

They added a couple of videos showing their ideas and associated tools. This one `https://goo.gl/nPP1pq` is particularly impressive, with a car in a car park far away from the targeted building, and in the upper limit of the infected camera vision, transmitting data (commands) in an operation which not even security personnel surrounding the building would be able to notice.



hidden communication via security cameras

47,172 views

Cyber Security Labs @ Ben Gurion University

By Dr. Mordechai Guri

There is a second video, in which an otherwise unremarkable camera is leaking a password and an access pin that could be aimed at facilitating anybody to break and enter the building without triggering any alarms.

YouTube
Search
the malware is leaking sensitive data via infrared (IR) signals (invisible to humans)
SHARE
SUBSCRIBE 2.1K

leaking data via security cameras

Cyber Security Labs @ Ben Gurion University

By Dr. Mordechai Guri

The researchers in addition discuss interesting technical details, such as the maximum distance at which reliable communication is possible and the maximum bit rate.

Of course, this depends of the particular camera used, but rates of around 15bits/s for exfiltrating data and 120bits/s for infiltrating seems achievable, together with effective distances that, in the case of direct line of sight between the devices can be from ten to hundreds of meters for exfiltration to up to kilometers for infiltration.

The method can also work when no direct line of sight exists, and the signals are reflected, which makes the attack even more threatening.

Finally, the authors propose a series of countermeasures, which are not popular nowadays, not trivial to implement nor cheap, so probably this threat will be with us for some time.

All in all, an awesome and very informative piece of work.

Funding News

The European Commission has pre-published the draft 2018-2020 work programme part for the Marie Sklodowska-Curie Actions (MSCA). You can find it here `https://goo.gl/ngkbES`. It contains many changes, mostly improvements in my opinion, over the past rules for Marie Curie Actions.

The European Commission has pre-published the draft 2018-2020 work programme part for Societal Challenge 6 - "Europe in a changing world - Inclusive, innovative and reflective societies". You can access it at `https://goo.gl/jk91TS`.

The European Commission recently published its tenth progress report 'Towards an effective and genuine Security Union', which discusses progress over the last years and planned actions to improve security, including systematic checks and a revamping of the EU entry/exit system, the establishment of an 'European Travel Information and Authorisation System (ETIAS)', reinforce Europol, approving a new directive on combating terrorism and firearms trafficking, as well as explosives-precursors to combat home-made explosives, etc. It's a good read, that you can access at `https://goo.gl/Heb5de`.

The European Commission, and in particular the DG for Research & Innovation has launched a prize on online security as part of H2020 Industrial Leadership pillar. This Horizon prize aims to significantly improve citizen's overall experience on online authentication, looking for a solution enabling citizens to seamless authenticate across a wide range of applications and devices. The ultimate objective is to foster the widespread adoption of services and products provided within the Digital Single Market of the European Union. The call is a single stage and has an estimated budget of 4 Million EUR. The deadline for the submission of proposals is 27 September 2018. You can get more info at `https://goo.gl/JWr1h9`.

Open Positions

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

- 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.

- Lecturer or Senior Lecturer at the University of Cambridge - Department of Computer Science and Technology. This is a full time and permanent positions located at Aston. The deadline is the 10th January 2018. The Lecturer position `https://goo.gl/zDhzhk` has a salary range of £53,691 to £56,950. Interviews will be held on 19-20th March 2018.

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.

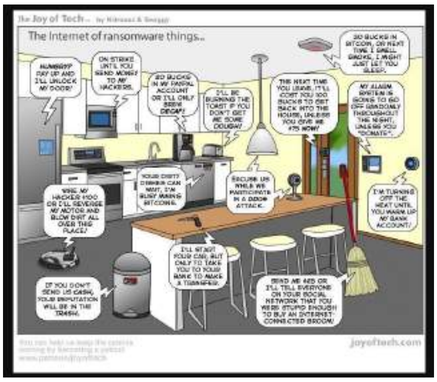
University of Kent

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

Blogs, posts and other good reads

NSA botched attempt at stardardisation in the news

It is not frequent that cryptography gets in the news. This piece by news agency Reuters `https://goo.gl/nwhsiV` was later reproduced in many other media, much to the chagrin of the NSA team that is attempting to make Simon and Speck into ISO standards. Our own Orr Dunkelman had a memorable contribution to the piece, and was quoted saying ”I don't trust the designers. There are quite a lot of people in NSA who think their job is to subvert standards. My job is to secure standards.” This is not a won battle yet, and if you want to know how you can contribute to stop this from happening, please contact your country representatives on the ISO Committee and let them know.


The Joy of Tech... by Nitrozac & Snaggy
The Internet of ransomware things..
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
20 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MAKING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
joyoftech.com

Pray for every minute this is just a comic situation and not a reality, for it will be.

Or, as a more rational alternative to prayer, which by the way doesn't work as Sir Francis Galton showed 145 years ago in his ’Statistical Inquiries into the Efficacy of Prayer’ https://goo.gl/wwLpXr, let's focus on this threat and work to fight against it, right now.

The creepiest webcam: Hola Senorita!

Not a great deal of technical novelty, but loads of nightmarish possibilities in this piece of news: A lady in the Netherlands bought a camera to check on her dog while away, and after two months it started to behave strangely (the camera).

At the beginning it followed her movements across the apartment (the camera, this is normal for a dog) which should have been more than enough to throw it (the camera, not the dog) over the window, but it was not until it (the camera) started producing strange noises that she worried.

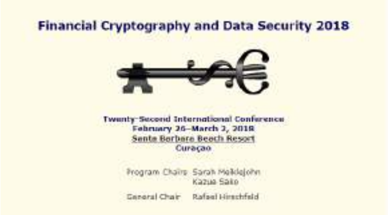
Things went even worse when it (the camera) started speaking to her in a variety of languages (but mostly French) and asked her to engage in sexual activities of the type described in Chapter IX of the Kama Sutra. Probably has happened hundreds of times, but this time she captured the whole scene on video https://goo.gl/VBVfrw.

It is curious how she shouts at the hacker multiples times to 'Get the f*** out' as if that were a technique with any possibility of working. I hope she has taken more drastic measures against it (the camera) by now.

Event calendar

Eurocrypt 2018 will take place in Tel Aviv, Israel, from April 29 to May 3. The 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 notification will arrive on the 17 November.



Financial Cryptography and Data Security 2018

Twenty-Second International Conference
February 26–March 2, 2018
Santa Barbara Beach Resort
Curaçao

Program Chairs Sarah Meiklejohn
Kazue Sako

General Chair Rafael Hirschfeld

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 was 5 October, with a quick notification on December the 4th.

The 10th International Conference on Cryptology, AFRICACRYPT 2018 will take place in Marrakesh, Morocco from the 7-9 May. The submission deadline is on January 7 and the notification on February 20th.

10th International Conference on Cryptology, AFRICACRYPT
May 7-9, 2018, Marrakesh, Morocco

The 23rd Australasian Conference on Information Security and Privacy (ACISP 2018) will be held in Wollongong, Australia on July 11-13, 2018. It will be organized by the University of Wollongong. The submission deadline is the 25 February 2018 at 11:59pm AEST and the notification will be on the 8th April.

23rd Australasian Conference on Information Security and Privacy
July 11-13, 2018, Wollongong, Australia

Welcome to ACISP 2018

[illegible]

The 3rd International Workshop on Boolean Functions and their Applications (BFA) is organized by the Selmer Center of the University of Bergen.

It will take place at the Alexandra Hotel, Loen, in Norway during June 17-22, 2018. The deadline for submission is April 1st, 2018 (no kidding) and the notification will be one week later, on April 7th.

The 3rd International Workshop on
Boolean Functions and their Applications (BFA)

See you all back in November!

Best,
Julio Hernandez-Castro