March 2018, No 17

Cryptacus Newsletter

March 2018 Cryptacus Newsletter

Welcome to the March 2018 edition of the monthly Cryptacus.eu newsletter, offering a glimpse into recent developments in the cryptanalysis of IoT & related areas. Send your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by Gildas Avoine

Dear Cryptacus Members,

Our next Cyptacus event will be held in less than a month in São Miguel.

I would like to remind you that the training school program is available online and grants to attend the event are still available for students.

Ricardo Chaves and his team did a great job to make this event successful, and I would already like to thank them for the organization.

The Training School web site is `https://www.cryptacus.eu/en/events/training-school-2018/`).

Jointly located with the training school, Cryptacus organizes a workshop on distance-bounding protocols. Many top-level researchers from this field accepted to give a talk.
The key idea is to make theoreticians and practitioners discussing together. The program has been prepared by Ioana Boureanu, Stéphanie Delaune, and Cristina Onete, and the event is co-funded by the ERC POPSTAR headed by Stéphanie.

The Workshop web site is `https://www.surrey.ac.uk/futuredb`.

In this March newsletter, I would also like to recap the short-term scientific missions (STSMs) that were funded by Cryptacus during the current Grant Period (May 2017 to April 2018).

We indeed received many STSM applications during the last months, much more than usual, and Cryptacus has been able to fund all of them after refilling the STSM budget. We so far funded: Sam Thomas (UK to FR), Milena Djukanovic (ME to IT), Veelasha Moonsamy (NL to ES), Elena Pagnin (SE to FR), David GÃľrault (FR to UK), Hannes Gross (AT to BE), Ioana Boureanu (UK to FR), Bogdan Dina (DE to FR), Ana Lucila Sandoval Orozco (ES to UK), Matthias J. Kannwischer (UK to NL), Esteban Armas Vega (ES to UK), Yu Long Chen (BE to NL).

In total, these STSMs represent 318 funded days. It is worth noting that inclusiveness target countries (ITC) are under-represented in spite of our effort to promote this scientific tool.

Finally, I would like to stress that the next Grant Period will start on May 1st, 2018. Cryptacus' members will then be able to apply again to STSM grants (https://www.cryptacus.eu/en/stsm/how-to-apply/) and to ITC conference grants (check `https://goo.gl/qfNrmL`).

The Work & Budget Plan of the next Grant Period has been recently approved, and the last Cryptacus' events will be announced in the April newsletter.

In the meanwhile, have fun with the March newsletter!

Best regards,

Gildas Avoine

Recommended reading: Predicting mergers via aviation traffic

MODERN JETS, RETRO CIPHERS:
HOW MONOALPHABETIC SUBSTITUTION
CIPHERS ARE STILL IN USE

Matthew Smith*, Daniel Moser‡, Martin Strohmeier*, Vincent Lenders‡, Ivan Martinovic*

*University of Oxford first.last@cs.ox.ac.uk ‡ETH Zurich first.last@inf.ethz.ch armasuisse first.last@armasuisse.ch

Real World Crypto 2018, January 10–12, Zurich

Modern jets, retro ciphers: how monoalphabetic substitution ciphers are still in use | Matthew Smith

This month we will be reporting on particularly nice and insightful paper author by a security team at Oxford and Armasuisse, which is a Swiss federal agency specialised on the procurement of armament.
It is titled "The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication".

Authors are Martin Strohmeier, Matthew Smith, Vincent Lenders and Ivan Martinovic. This paper continues the research from the Oxford team on aircraft security communication. For a previous work on a closely related topic, you can watch the video of Matthew Smith on ACARS insecurity titled "Modern jets, retro ciphers: how monoalphabetic substitution ciphers are still in use" at this year's Real World Crypto, accessible at `https://www.youtube.com/watch?v=hEqcITbBNh4`.

As stated in their abstract, this paper exploits publicly available aircraft meta data and unfiltered air traffic communication gathered from a global collaborative sensor network to study the privacy impact of large-scale aircraft tracking on governments and public corporations.

They track travel data from 542 aircraft used by 113 different governments to identify events and relationships in 'the real world'. They develop a spatio-temporal clustering method which returns 47 public and 18 non-public meetings attended by dedicated government aircraft over the course of 18 months.

Additionally, they illustrate the ease with which one could analyze the behavior and relationships of aviation users through the example of foreign governments visiting Europe. In an even more interesting and practical application of their findings, they exploit similar travel date to predict potential merger and acquisition (M&A) activities by 36 corporations listed on the US and European stock markets. His findings could potentially lead to a very profitable investing strategy, as they identify seven M&A cases, in all of which the buyer has used corporate aircraft to visit the target prior to the official announcement, on average 61 days before. This period of time give ample time to take financial positions to benefit from the information leakage.

Finally, they try to find solutions to stop this massive information leakage from occurring, quantifying their popularity and effectiveness, and finding them mostly ineffective.

This work has recently been accepted for the 3rd IEEE European Symposium on Security and Privacy, that is going to take place on April 24-26, 2018 in London, United Kingdom.

Funding News

Warsaw Brockerage Event

H2020 SECURE SOCIETIES
International Information Day & Brokerage Event
11th April 2018, Copernicus Science Centre, Warsaw

11 April 2018
Warszawa, Poland

H2020 Sec Soc Info Day and Brokerage Event

Home How it works? Venue Useful information Contact

Horizon 2020 Secure Societies
European Info Day and Brokerage Event

The event is organized by the Network of Secure Societies National Contact Points – SEREN3, in collaboration with the European Commission. This information day and brokerage event gives details on the calls for proposals H2020-CIP 2018, H2020-SEC 2018 and H2020-DS-2018, published on 27 October 2017 under the societal challenge Secure Societies - Protecting freedom and security of Europe and its citizens.

These calls offer new research funding opportunities to research institutions, universities, industries, SMEs, civil society organizations and other security stakeholders. Participation to the event is free of charge and the number of participants is limited due to the capacity of the rooms.

Main topics

- Critical Infrastructure Protection
- Disaster Resilience: Safeguarding and securing society
- Fight Against Crime and Terrorism
- Border Security and External Security
- General Matters on Security
- Digital Security

REGISTRATION
Open until 1 April 2018

LOCATION
Wybrzeże Kościuszkowskie 20
Warszawa, Poland

ORGANISED BY

There is an interesting Info Day and Brokerage Event on the Horizon 2020 Secure Societies call.

The event is organized by the Network of Secure Societies National Contact Points - SEREN3, in collaboration with the European Commission. This information day and brokerage event gives details on the calls for proposals H2020-CIP 2018, H2020-SEC 2018 and H2020-DS-2018, published on 27 October 2017 under the societal challenge Secure Societies - Protecting freedom and security of Europe and its citizens.

These calls offer new research funding opportunities to research institutions, universities, industries, SMEs, civil society organizations and other security stakeholders.

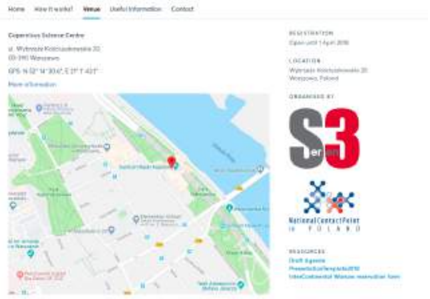
Participation to the event is free of charge and the number of participants is limited due to the capacity of the rooms.

The main topics to be covered are Critical Infrastructure Protection, Disaster Resilience, Safeguarding and securing society, Fight Against Crime and Terrorism, Border Security and External Security, General Matters on Security and Digital Security. There are many reasons to participate, including: receiving information about the calls, networking possibilities, to get answers to your questions linked to call areas and to get details on the legal and procedural conditions.

One of the great benefits of these events is that you can present project ideas briefly (you generally get 2 min for a lightning presentation) to all participants and explicitly seek collaboration from organisations with a given set of skills. There will be also face to face meetings that you can ask for on the web of the event. Ping me if you plan to attend, as I will be there.

The registration is open until 1 April 2018. The event venue is the Copernicus Science Centre in Warsaw.

You can register at `https://goo.gl/vogvYw`



Copernicus Science Centre
ul. Wybrzeże Kościuszkowskie 20
00-390 Warszawa
GPS: N 52° 14' 30.6", E 21° 1' 43.1"
More information

REGISTRATION
Open until 1 April 2018

LOCATION
Wybrzeże Kościuszkowskie 20
Warszawa, Poland

RESOURCES
Draft Agenda
PresentationTemplate2018
InterContinental Warsaw reservation form

EIBURS Call for Proposals

The European Investment Bank Institute has just launched a new EIBURS sponsorship under its knowledge programme.

The EIB University Research Sponsorship Programme (EIBURS) provides research grants of up to €100,000 a year for a period of three years, to interested university departments or research centres with expertise in that year's topic. The EIBURS topic for this year is "The economic effects of a joint European security and defence policy".

The deadline for submission of proposals is 15 April 2018.

Further information on this call can be found at the European Journal, C60 (16.02.18)

Open Positions

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

- Lecturer in Cyber Security at the University of Southampton

This is an interesting position in one of the growing cybersecurity teams in the UK

It is a full time, permanent position with a starting salary of between £37,706 and £47,722 per annum. The deadline for submission of candidatures is the 18th April.

They are looking for scholars in the broad area of cyber security, covering science and engineering of cyber security and information assurance. Specific topics of interest include the security and privacy of emerging applications of the internet-of-things and cloud computing, the protection of cyber-physical systems, system and network security, computer forensics, intrusion detection, authentication systems, cyber risk and economics, usability and human aspects of cyber security.

More info at https://goo.gl/tgKdH6

UNIVERSITY OF Southampton

- Senior Lecturer or Reader in Secure Systems at the University of Surrey, Department of Computer Science. Surrey is a good UK university not far from London, which has international visibility in Cybersecurity and is consistently growing and investing in the area.
This position would be located in Guildford, with a salary of £49,149 to £69,984 per annum. This is, of course, a full time permanent position. Suitable areas of expertise that complement current strengths of the group include (but are not limited to): antimalware security, adversarial machine learning, risk management and threat modelling, trusted systems, verification, and distributed systems.
The deadline for applications is the 23rd April 2018.
More info available at https://goo.gl/fgg22s.

UNIVERSITY OF SURREY

- A position as (full) professor of Computer Science is available as soon as possible at the Department of Computer Science, Aarhus University (www.cs.au.dk). The department has research groups within 'Algorithms and Data Structures', 'Data-Intensive Systems', 'Cryptography and Security', 'Mathematical Computer Science', 'Logic and Semantics', 'Ubiquitous Computing and Interaction', 'Computer-Mediated Activity', 'Use, Design and Innovation', and 'Programming Languages'. Moreover, they wish to build competencies within Machine Learning and Systems Security. The deadline is 03.05.2018. More information at https://goo.gl/rnJYSh.

AARHUS UNIVERSITY

For other interesting positions all across Europe, please check the recently revamped "Researchers in Motion" portal at https://euraxess.ec.europa.eu/. It currently has close to 60 open positions in computer security and related areas, including in Poland, the UK, Finland, Slovenia, Italy, Norway, Switzerland, and even in Spain!

Proposals for STSMs

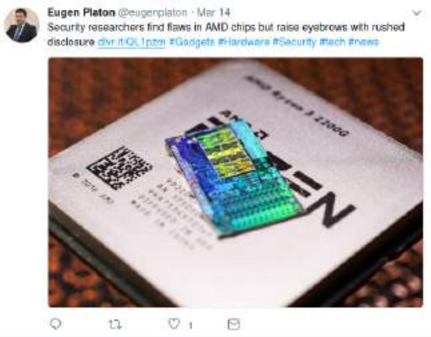
By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short) are. Please make your willingness to receive STSMs proposals known by sending me an email. Until I do not have any more, I'll just publish mine:

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 recommended reads

Irresponsible disclosure



Eugen Platon @eugenplaton · Mar 14

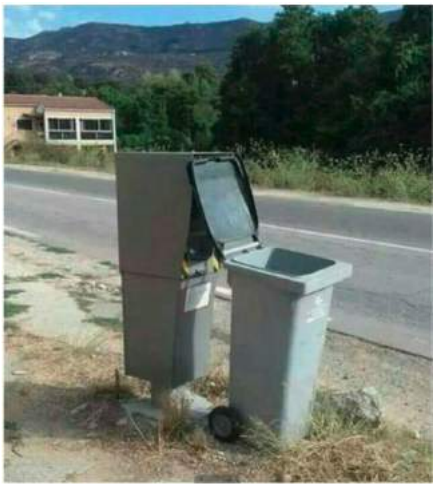
Security researchers find flaws in AMD chips but raise eyebrows with rushed disclosure dlvr.it/QL1pzm #Gadgets #Hardware #Security #tech #news

More info at `https://goo.gl/Dvyy7w`

'R2D2' stops disk-wipe malware before it executes evil commands

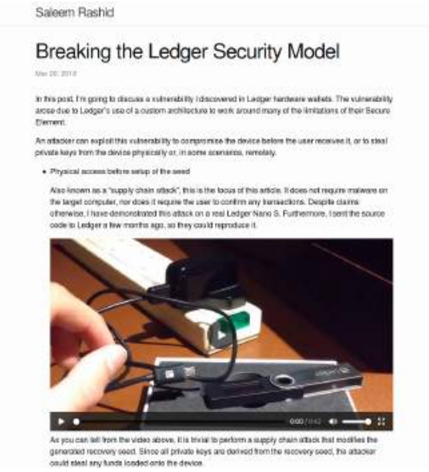
Purdue University researchers have developed a way to protect against wipers. Their idea is to analyse write buffers before they reach storage, and decide whether the intended write is destructive, and stop it if so. Wipers cause substantial damage by overwriting critical digital assets on compromised machines, denying users access to computing resources. They interpose an inspection step in the Virtual Machine Monitor (VMM) through a technique known as Virtual Machine Introspection (VMI). This has the benefit that it does not rely on the entire OS as a root of trust. The prototype seems to be effective (99.8%) against malware such as Shamoon and Stonedrill, and some other secure delete tools. The authors acknowledge that the performance of their tool needs to be investigated further, but the approach seems quite promising. More info at `https://goo.gl/pnJEDC`.

Low-cost hacking of a road speed radar :-)



Ledger security problems

The Ledger Nano is quite possibly, the most popular hardware wallet in the market. It's manufactured in France and has sold more than 1,000,000 copies. Hardware wallets are used by cryptocurrency holders to keep their coins off the markets, securely stored in an off-line device for extra security. So news of the finding of a number of weaknesses in the device have shocked its customer base. All the technical details and a video showing the hack can be accessed at `https://goo.gl/BT6JVa`, but to cut a long story short, it seems all Ledger hardware wallets are vulnerable to a relatively simple man in the middle attack.



Saleem Rashid

Breaking the Ledger Security Model

Mar 20, 2018

In this post, I'm going to discuss a vulnerability I discovered in Ledger hardware wallets. The vulnerability arose due to Ledger's use of a custom architecture to work around many of the limitations of their Secure Element.

An attacker can exploit this vulnerability to compromise the device before the user receives it, or to steal private keys from the device physically or, in some scenarios, remotely.

- Physical access before setup of the seed

  Also known as a "supply chain attack", this is the focus of this article. It does not require malware on the target computer, nor does it require the user to confirm any transactions. Despite claims otherwise, I have demonstrated this attack on a real Ledger Nano S. Furthermore, I sent the source code to Ledger a few months ago, so they could reproduce it.

As you can tell from the video above, it is trivial to perform a supply chain attack that modifies the generated recovery seed. Since all private keys are derived from the recovery seed, the attacker could steal any funds loaded onto the device.

Event calendar

SSR 2018, The 4th Conference on Security Standards Research, will take place in Darmstadt Germany, on 3-4 December 2018. The purpose of this conference is to discuss the many research problems deriving from studies of existing standards, the development of revisions to existing standards, and the exploration of completely new areas of standardisation. The deadline for submissions is 22 June 2018 (3pm UTC). The General Chair is Marc Fischlin. More info at `https://ssr2018.net/`.

SSR 2018: Security Standardisation Research

The 23rd European Symposium on Research in Computer Security (ESORICS) will be held in Barcelona, at the Universitat Politecnica de Catalunya - BarcelonaTech, on September 3-7 2018. Several co-located workshops will be held in conjunction with the Symposium. The submission deadline is April 18, 2018 (11:59 p.m. American Samoa time). General Chair is Miguel Soriano.

ESORICS 2018

Practical Info

Welcome to ESORICS 2018

Sponsors

The 2nd IMA Conference on Theoretical and Computational Discrete Mathematics accepts abstracts of up to 500 words to be submitted for either oral or poster presentation via `https://my.ima.org.uk` by Friday 13 April 2018.

2nd IMA Conference on Theoretical and Computational Discrete Mathematics

EVENT

Important Links

Latest News

2nd IMA Conference on Theoretical and Computational Discrete Mathematics

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)

This workshop occurs immediately after a related one called WAIFI (International Workshop on the Arithmetic of Finite Fields 2018) in Bergen, which is on June 14-16, with a **deadline on April 1st**, and acceptance notification on May 11th, 2018.

More info at `http://waifi.org`.

International Workshop on the Arithmetic of Finite Fields

WAIFI 2018

The 21st Information Security Conference (ISC 2018), will take place in London (Guildford), from September 9 to September 12, 2018. The **submission deadline is 16 April**, with notification on the 18 June. The General Chair will be Steve Schneider.

21st Information Security Conference

9-12 September 2018, London (Guildford), UK

ISC 2018

The 'IoT Autentication 2018' Conference will take place in Melbourne, Australia on November 28-30, 2018. It will feature invited presentations from Auto-ID Labs, IoT Alliance Australia, IoT (Internet of Things) Security, Prof. Michael Sheng, Prof. Margreta Kuijper, Dr. Omid Kavahei, Prof. Seng Loke,and Prof. Lejla Batina. The Keynote speaker is Dr. Veena Pureswaran from IBM. If you want to attend, check `http://www.authiot2018.conferences.academy/`.

IoT Autentication 2018

AUTHENTICATION FOR THE FUTURE INTERNET OF THINGS

Significance

Organizers

Flyer

See you all back in April!

Best,
Julio Hernandez-Castro