Cryptacus Newsletter

February 2018 Cryptacus Newsletter

Welcome to the February 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,

With the approaching end of the current grant period of your COST Action, we received an impressive high number of STSM applications.

STSMs have never been as successful as during this current grant period (May 2017 - April 2018), and this is the first time that Cryptacus fully spends the budget assigned to STSMs.

Next month, I will be able to provide an accurate statement of the accepted STSM applications.

I am also glad to announce that we received about 15 proposals after the publication of the call for chapters for the book.

It is worth noting that many proposals are co-authored by researchers from different COST countries, which points that a scientific network such as Cryptacus is definitely efficient to launch collaborations.

The selection committee is currently reviewing the received chapter proposals. The acceptation deadline will be slightly delayed, given that several authors requested to postpone the submission deadline.

The selection committee will select proposals, then it may invite additional researchers to submit chapter proposals, if the topics covered by the received proposals suffer from gaps that should be filled in order to make the book self-content and fully consistent.

Following several questions that I received about our event in Sao Miguel, I would like to remind you that there is the workshop on distance-bounding protocols on April 14th and 15th, the book working session on April 16th, the MC Meeting on April 17th, and the Training School from April 16th to April 20th.

MC Members should attend the MC Meeting, and they can attend the workshop and the book session if relevant.

For the training school, registration fees apply for all participants, but 37 grants are available for PhD students.

For your information, there is no vacancy anymore in the hotel of the event (Lince Azores Hotel). However, many hotels are available around the venue. For example, several people already booked in Hotel do Colegio. Please check the accommodation page of the training school web site for more details.

The training School web site is `https://www.cryptacus.eu/en/events/training-school-2018/` and the workshop web site is `https://www.surrey.ac.uk/futuredb`

Best regards,

Gildas Avoine

Recommended reading: Alarming state of mobile health applications

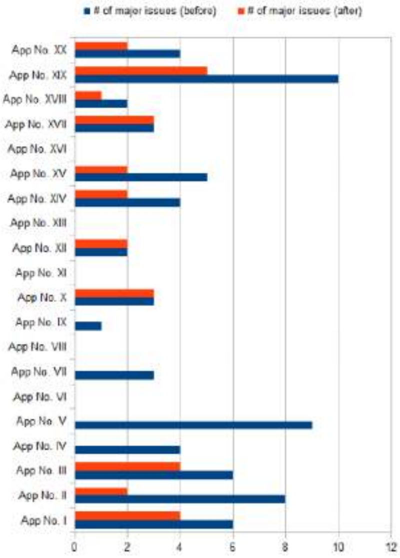


Fig. 6. Number of major issues per app before and after our reportings

This month we will be reporting on a piece by our Cryptacus colleagues Agusti Solanas and Constantinos Patsakis, together with University of Piraeus' Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou and Efthimios Alepis.

This work analyses the security of health applications for smartphones, particularly the most relevant ones in terms of popularity (number of downloads) and user acceptance (high feedback).

These collect users health-related information to help them better follow their health status and promote a healthy lifestyle.

But this information is extremely sensitive, and it should be a top priority of these apps to offer adequate protection, if only to comply with the new regulatory frameworks in Europe.

Unfortunately, and after an in-depth security and privacy analysis of some of the most popular freeware mobile health applications, the authors found that the majority of the analyzed applications do not follow best practices and disregard even legal obligations as imposed by contemporary data protection regulations (GDPR), thus jeopardizing the privacy of tens of millions of users across the World.

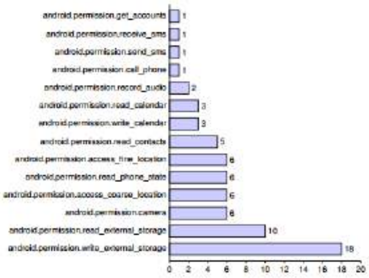
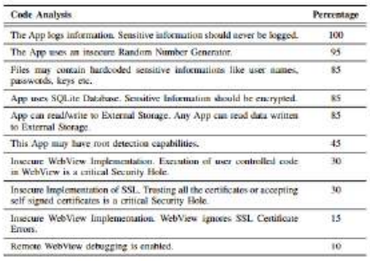


Fig. 2. Summary of dangerous permission requests



Code Analysis	Percentage
The App logs information. Sensitive information should never be logged.	100
The App uses an insecure Random Number Generator.	95
Files may contain hardcoded sensitive informations like user names, passwords, keys etc.	85
App uses SQLite Database. Sensitive Information should be encrypted.	85
App can read/write to External Storage. Any App can read data written to External Storage.	85
This App may have root detection capabilities.	45
Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	30
Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole.	30
Insecure WebView Implementation. WebView ignores SSL Certificate Errors.	15
Remote WebView debugging is enabled.	10

TABLE III
Results of the Static Code Analysis

As revealed by the European Commission's 2014 m-Health Green Paper, European citizens do not trust m-Health apps since 67% of the surveyed said they would never use them.

This work totally justifies this lack of trust, and highlights that there is a major gap in the security and privacy of these popular applications, and that not even the proximity of an extremely important regulation hasn't motivated their authors to improve their security and privacy features. Enforcing the new European laws will probably be difficult in global markets such as Google Play or the Apple Store.

The paper has been accepted for publication in IEEE Access, and can be read (Open Access) at `http://ieeexplore.ieee.org/document/8272037/`.

This work got a lot of media attention, with coverage in radio and online and traditional news media, such as `https://goo.gl/SNxUXU`, `https://goo.gl/dc3HRQ`, and even lead to the COST office to publish a media piece at `https://goo.gl/p9HpLW`.

Funding News

SMI2G Event

The Security Mission Information & Innovation Group (SMI2G) has organised a two-day event in Brussels to exchange information on the 2018 Secure Societies calls and to stimulate networking for the creation of potential ideas and consortia.

I could only attend the second day, on the 2nd of February, at the Central Auditorium (Pierre Lacroix) of the Universite Catholique de Louvain (UCL) in Brussels.

It was a well-attended event, with 459 participants from 31 countries. A good opportunity to make contacts, meet colleagues, and start discussing ideas and building consortia for the security calls of this summer.

All the presentations given during the SMI2G 2018 event have been published on the SEREN3 project official website. All the files are now available through this link `https://cloud.rosa-rc.ro/index.php/s/S1MP48yiFHOSQMD/authenticate` (password: smi2g2018).

A similar event is taking place, again in Brussels, on 12 and 13 March. It is the Horizon 2020 Secure Societies European Info Day and Brokerage Event, organised by the Network of H2020 Secure Societies National Contact Points - SEREN3, in collaboration with the European Commission and Research Executive Agency.

Horizon 2020 Secure Societies

European Info Day and Brokerage Event

The event will take place at Hotel Le Plaza, and will give details of the calls for proposals H2020-CIP 2018, H2020-SEC 2018 and H2020-DS-2018. The event will help participants to prepare their proposal by offering:

- Detailed information about the calls
- Networking possibilities, through project idea presentation & bilateral meetings sessions
- Answers to any questions raised linked to call areas
- Details on the legal and procedural conditions

The programme and all information are available on the event web site `https://seren3brussels2018.b2match.io`.

Registration for the event is free but obligatory, and available at `https://seren3brussels2018.b2match.io/signup`

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.

- Professor in Secure Systems at the University of Surrey, Department of Computer Science. Salary from £67,970 to £91,001 per annum. Deadline for applications is the 5th March.

  Suitable areas of expertise that complement current strengths of the group include (but are not limited to): anti-malware security, adversarial machine learning, risk management and threat modelling, trusted systems, verification, and distributed systems.

  This is a full time, permanent job offer. For more info, visit the ad at `https://goo.gl/SGDf64`.

  The same employer is currently recruiting for a Senior Lecturer or Reader in Secure Systems, this time with a deadline of 23rd April. More info at `https://goo.gl/unyTQp`.

- Lecturer in Computer Science (with a specialization in Security) at King's College London - Department of Informatics.

  This posts is based in London, with a salary of £41,212 to £49,149 plus an annual London allowance of £2,923.

  The deadline for application is 17th March. This is a full-time, permanent position. The successful candidate will be appointed to the Cybersecurity (CYS) Group. More info at `https://goo.gl/dXPP7X`

  In addition to this post, King's College has just published an opening for a Chair in Cybersecurity (Security and Systems). They are currently recruiting heavily in the Computer Science/Informatics department and seem keen to create a strong Cyber security group. More info at `https://goo.gl/M83hc7`. Deadline on the 28th February. Salary starts at £66,084 plus £2,923 of London allowance, but can easily reach two times this amount depending on experience.

- Lecturer, Senior Lecturer, or Reader in Cyber Security at the University of Birmingham School of Computer Science. Full-time, permanent positions, with a closing deadline of 25th

February and a salary ranging from £39,993 to £74,259. They are particularly interested in those specialising in systems security or the intersection of security with artificial intelligence or human-computer interaction. This is a very interesting opportunity to join an expanding group which is rapidly becoming one of the best groups in the UK. More info at `https://goo.gl/9VWs4h`.

UNIVERSITY OF BIRMINGHAM

- Professor of Computer Science at University College Cork - School of Computer Science and Information Technology.

This is an interesting position in Ireland, at a prestigious institution that wants to expand its cyber security expertise.

They state in the ad that "The School strategy is to expand its research and teaching in the area of cyber-security, and candidates with such expertise are especially encouraged to apply. Applications from candidates with expertise in other areas of computer science will also be considered."

This is a full-time and permanent position, with a relatively high salary ranging from €109,129 to €140,962 depending on experience.

Note that, as it is becoming increasingly common with cybersecurity positions, Garda vetting or an international police clearance check may form part of the selection process.

The deadline for applications is Tuesday 6th March 2018 at noon. More info at `https://goo.gl/jq9Vrd`

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

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 50 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.

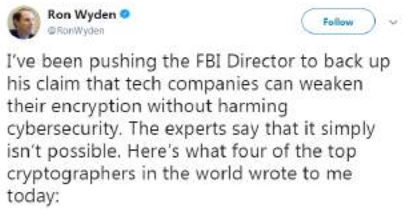
Until I do not have any more, I'll just publish mine:

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

Wyden's letter



Ron Wyden
@RonWyden

I've been pushing the FBI Director to back up his claim that tech companies can weaken their encryption without harming cybersecurity. The experts say that it simply isn't possible. Here's what four of the top cryptographers in the world wrote to me today:

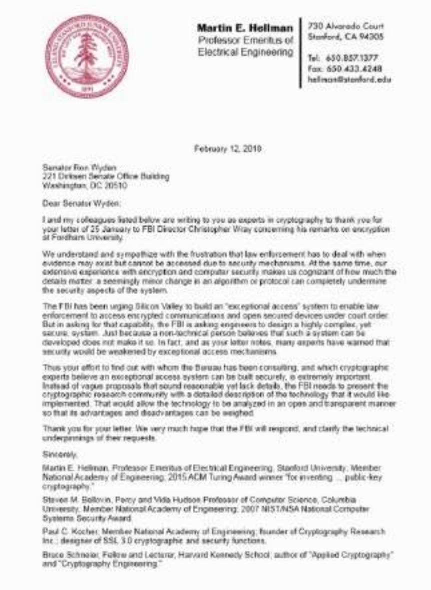
Ron Wyden is the Democratic Senator from Oregon.
He's an interesting and controversial figure in the United States Senate, and although after checking his voting history one may disagree with the timing or wisdom of some of his past actions, it is difficult to argue against the fact that he is a strong advocate of civil liberties and (with the exception of assisted suicide) his views are very liberal (in the best sense of the word, if any still exists) and closer to these of NGOs such as the EFF.

He has recently been again in the spotlight because of his doubts about a recent statement by the FBI Director, who claimed tech companies can weaken their encryption without harming cybersecurity.

He, in a move that is nowadays sadly uncommon for politicians, seek real expert's advice.

As a result, he received a letter from Prof. Martin Hellman (signed also by Bellovin, Kocher and Schneier) saying this is simply not possible right now, at least not as stated by the FBI Director.

It is interesting to note that the FBI Director had claimed that "experts" had concluded these "exceptional access" mechanisms were possible without compromising security. Senator's Wyden call FBI's bluff requesting them to name the experts who made such claim, and he has not received an adequate answer to date.



Martin E. Hellman
Professor Emeritus of
Electrical Engineering

730 Alvarado Court
Stanford, CA 94305

Tel: 650.857.1377
Fax: 650.433.4248
hellman@stanford.edu

February 12, 2018

Senator Ron Wyden
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

I and my colleagues listed below are writing to you as experts in cryptography to thank you for your letter of 25 January to FBI Director Christopher Wray concerning his remarks on encryption at Fordham University.

We understand and sympathize with the frustration that law enforcement has to deal with when evidence may exist but cannot be accessed due to security mechanisms. At the same time, our extensive experience with encryption and computer security makes us cognizant of how much the details matter: a seemingly minor change in an algorithm or protocol can completely undermine the security aspects of the system.

The FBI has been urging Silicon Valley to build an "exceptional access" system to enable law enforcement to access encrypted communications and open secured devices under court order. But in asking for that capability, the FBI is asking engineers to design a highly complex, yet secure, system. Just because a non-technical person believes that such a system can be developed does not make it so. In fact, and as your letter notes, many experts have warned that security would be weakened by exceptional access mechanisms.

Thus your effort to find out with whom the Bureau has been consulting, and which cryptographic experts believe an exceptional access system can be built securely, is extremely important. Instead of vague proposals that sound reasonable yet lack details, the FBI needs to present the cryptographic research community with a detailed description of the technology that it would like implemented. That would allow the technology to be analyzed in an open and transparent manner so that its advantages and disadvantages can be weighed.

Thank you for your letter. We very much hope that the FBI will respond, and clarify the technical underpinnings of their requests.

Sincerely,

Martin E. Hellman, Professor Emeritus of Electrical Engineering, Stanford University; Member National Academy of Engineering; 2015 ACM Turing Award winner "for inventing ... public-key cryptography."

Steven M. Bellovin, Percy and Vida Hudson Professor of Computer Science, Columbia University; Member National Academy of Engineering; 2007 NIST/NSA National Computer Systems Security Award

Paul C. Kocher, Member National Academy of Engineering; founder of Cryptography Research Inc.; designer of SSL 3.0 cryptographic and security functions.

Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School; author of "Applied Cryptography" and "Cryptography Engineering."

This is another twist on the ongoing war on crypto.

Looks particularly worrying if we see it as part of the same effort that is desperately trying to push NSA's SPECK and SIMON for standardisation by ISO/IEC despite the strong opposition of the German, Japanese and Israeli representatives.

Please don't forget to contact your national representative and ask him or her to vote against these abusive behaviour, from the authors of the beloved and heavily backdoored Dual-EC-DRBG.

ALL YOUR MONERO ARE BELONG TO US

The latest pseudo-criminal trend is to turn your browser into a cryptocurrency mining machine.
There is even a legitimate (although admittedly immoral) business model behind it, as for example proposed by `https://coinhive.com`, that tries to sell it as an alternative to online ads.
They basically provide you with javascript that you can embed in your webpages which will abuse your visitor's CPU to mine Monero, a cryptocurrency that can be mined for reasonable profit on normal CPUs and that, conveniently, offers much more privacy than bitcoin.
Coinhive will take 30% of the profits, and 70% will go to the website owner.
This is of course an awful practice that, in the hands of criminals, can be turned into something even worse when they include said javascript on hacked webpages, whose owners remain unaware of the events.
How to prevent attackers to compromise your web and plant code that will abuse your visitors? In addition to the usual security measures, there are some very specific ones that are beautifully covered on a blog `https://goo.gl/iR5p6f` by Scott Helme.

Protect your site from Cryptojacking with CSP + SRI

What happened

The Author

Follow

This was in response to the discovery that more than 4,000 sites were hosting mining scripts, many of these Government websites. This happened because a third party provider (Text Help) was compromised and their javascript library was altered, introducing a crypto mining script that was then subsequently included on thousands of websites.

Fortunately, this is easy to stop with a tiny change to how the script is loaded in the code, adding the SRI Integrity Attribute that allows the browser to determine if the file has been modified, and reject it if needed.

Scott claims that to take this one step further and ensure absolute protection, you can use Content Security Policy and the require-sri-for directive to make sure that no script is allowed to load on the page without an SRI integrity attribute. On top of that, you could be alerted to events like this happening on your site via CSP Reporting.

Event calendar

The 33rd IFIP TC-11 SEC 2018 International Conference on Information Security and Privacy Protection (SEC 2018) will take place in Poznan, Poland, from the 18 to the 20 September. Cryptacus' Miroslaw Kutylowski is in the organisation. Deadline has passed, but this is a very nice event to register and attend, with some very high quality presentations. More info at `http://ifipsec2018.pwr.edu.pl/comittee.php`

33rd IFIP TC-11 SEC 2018 International Conference IFIPSEC 2018
on Information Security and Privacy Protection
Poznan, Poland, 18-20 September, 2018

Welcome to IFIP SEC 2018

Welcome to the IFIP International Information Security and Privacy Conference Web Site. This conference is the flagship event of the International Federation for Information Processing (IFIP) Technical Committee 11 on Security and Privacy Protection in Information Processing Systems (about TC-11 see www.ifiptc11.org).

Previous SEC conferences were held at: 2017: Rome, Italy; 2016: Gent, Belgium; 2015: Hamburg, Germany; 2014: Marrakech, Morocco; 2013: Auckland, New Zealand

WCC 2018 POZNAN

The 24th IFIP World Computer Congress September 17-21, 2018 Poznan, Poland

The SEC 2018 conference will run in in cooperation of the 24th World Computer Congress. We seek submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of security and privacy protection in ICT Systems.

All submissions will be reviewed by at least four reviewers. Papers accepted for presentations at the conference will be published in a book form by Springer.

The 17th Annual Workshop on the Economics of Information Security (WEIS) will take place next year in Innsbruck, Austria.

The notification of acceptance is on March 31. Rainer Böhme is the conference chair.

WEIS 2018

17th Annual Workshop on the Economics of Information Security

The 23rd Australasian Conference on Information Security and Privacy (ACISP 2018) will be held in Wollongong, Australia on July 11-13, 2018.

It will, unsurprisingly, 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

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

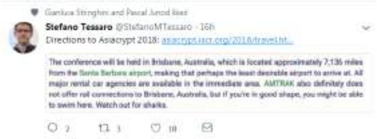
The 13th International Conference on Availability, Reliability and Security (ARES 2018), will be held from August 27 to August 30, 2018 at the University of Hamburg, Germany.

The submission deadline is March 16, 2018. This conference is quickly becoming one of the largest security gatherings in Europe, with more than 12 associated workshops covering from 5G Networks to Information Hiding.

Of special interest to our audience is, possibly, the 2nd International Workshop on Security and Forensics of IoT.

ARES Conference
International Conference on Availability, Reliability and Security
Hamburg, Germany
August 27 – August 30, 2018

Last but not least, the (temporary) travel information for AsiaCrypt2018 have attracted some unexpected attention due to their good sense of humor. As of this writing, they (partly) read "*The conference will be held in Brisbane, Australia, which is located approximately 7,136 miles from the Santa Barbara airport, making that perhaps the least desirable airport to arrive at. All major rental car agencies are available in the immediate area. AMTRAK also definitely does not offer rail connections to Brisbane, Australia, but if you're in good shape, you might be able to swim here. Watch out for sharks.*"



Gianluca Stringhini and Pascal Junod liked
Stefano Tessaro @StefanoMTessaro · 16h
Directions to Asiacrypt 2018: asiacrypt.iacr.org/2018/travel.ht...

The conference will be held in Brisbane, Australia, which is located approximately 7,136 miles from the Santa Barbara airport, making that perhaps the least desirable airport to arrive at. All major rental car agencies are available in the immediate area. AMTRAK also definitely does not offer rail connections to Brisbane, Australia, but if you're in good shape, you might be able to swim here. Watch out for sharks.

See you all back in March!

Best,
Julio Hernandez-Castro