Special Interest Group on Internet Security (ISEC SIG)

Internet Technical Committee (ITC)
Webpage : http://internet-security-sig.lip6.fr
ITC representative: Stefano Secci (Stefano 'DOT' Secci 'AT' ieee 'DOT' org)

2017 activity report

The Special Interest Group on Internet Security was created in 2017 following discussions within ITC and ComSoc at large, including the technical and educational activities council. As a matter of fact, it was identified that there is a low level of activity and synergies in the area of cybersecurity in networking. The need to further stimulate technical activities in this area for the communications community was expressed, in particular in less conventional topics. The identified need is to go beyond classical cryptography research and related applications to network protocols and physical communications, focusing on new networking environments and cybersecurity contexts.

ITC officers hence decided to create the ISEC SIG to gather and report on on-going initiatives by the ITC community in the area, and stimulate the emergence of further actions. Preliminary activities along the mentioned research and technical directions were henceforth launched in 2017 as described in the following, including hyperlinks to web material for additional details.

At the IEEE ICC 2017 ITC meeting in Paris, two lightening talks on security were given:
"SDN Security – What's done, what's next?", by Sandra Scott-Hayward.
'A Secure Routing Architecture', by Nirmala Shenoy.
To raise awareness on major issues in routing and challenges related to softwarization.

Moreover, a new brigade was created in the framework of the Open Network Operating System (ONOS) open source project on network virtualization and softwarization, under the auspices of the Open Networking Foundation (ONF), to work in the area.
The ONOS Security & Performance Brigade is actually composed of about 20 active members. Besides documenting performance tests result against the latest releases of the ONOS Software Defined Networking (SDN) controller, the brigade supports the development of the DELTA tool and its usage to assess SDN controller robustness against a large set of identified threats.
The brigade produced a 1st report, presented at ONOS Build 2017, where the following tests are reported:

- LISP SouthBound Interface stress tests, leading to improvement of the SBI in latest releases.
- Karaf-level bundle failure performance tests, identifying some important weaknesses being considered for future releases.
- Quality Assurance tests on control-plane latencies related to different features.
- DELTA tests results on ONOS 1.11.
- Configuration and communications vulnerabilities documentation, with wiki guidelines to set countermeasures being prepared.

The report is available as ONF Informational Report.

The brigade is actually working on the second report, as regular yearly brigade report, and on an additional special report on ONOS vs ODL (Open Day Light) performance and security comparison. Both will be presented at ONOS Build 2018.
The brigade is continuously looking for new proposals of security and performance tests activities and is open to integrate new members actively contributing to the brigade charter. Besides meeting at ONOS Build, a yearly workshop is run. The first took place in May 26, 2017, and the next one will take place in Paris in March 2018 (date to be announced on the brigade wiki page).
In this area, it is worth mentioning the ARTEMIS (Automated System against BGP Prefix Hijacking) ONOS framework, developed in the frame of the ERC NetVolution project lead by Xenofontas Dimitropoulos, FORTH, Crete.

Another important rising activity of the ISEC SIG is a new conference that was launched by ITC members and endorsed by ITC, the 1st Cyber Security in Networking Conference (CSNET), which took place in Rio de Janeiro, Brazil, in Oct. 18-20, 2017. ITC members involved in the organization and technical committees include Otto Duarte, Deep Medhi, Stefano Secci, Michele Nogueira. Despite the very short notice in announcing the event, the conference was a good success with about 100 participants, ~50 submissions and 20 papers scheduled in technical sessions. The conference also featured five keynotes and invited talks.
The 2nd CSNET conference is planned to be organized in Paris in November 2018, at Ecole Militaire. Detailed information will be announced in the coming months.

Another event being launched in the area of the ISEC SIG is the Managing and Managed by Blockchain Workshop, co-located with IEEE/IFIP NOMS 2018, taking place in Taipei, Taiwan, in April 27, 2018. Involved ITC members include Jérôme François, Michele Nogueira and Stefano Secci. This area, and in particular topics related to blockchain federation for network control-plane operations, Internet addressing, mapping and management information ,is a second new networking and cybersecurity context the ISEC SIG will focus on, also following the rising interest at the IRTF on decentralized Internet infrastructures exploiting blockchain-based bricks. The workshop is currently calling for paper submissions, with a deadline set to January 5, 2018.

Others activities organized by ITC members in the coming months are:
- the Workshop on research advances in Cooperative ITS cyber security and privacy (C-ITSec), co-located with VTC Spring 2018, on June 3, 2018, Porto, Portugal. The workshop focuses on cybersecurity for intelligent transportation systems. The call for papers deadline is set to Jan. 19, 2018. On the same topic, a Special Issue on Recent advances on security and privacy in Intelligent Transportation Systems is being prepared by the Ad Hoc Networks Journal, with March 1, 2018, as deadline.
- Workshop on 5G Wireless Security (5G-Security), co-located with ICC 2018, and taking place in Kansas-City on May 24, 2018. The call for papers deadline is set to Jan. 3, 2018.
- IEEE Communications Magazine is preparing a Feature Topic on Information-Centric Networking Security, to be published in 2018.

Finally, there are open PhD opportunities on SDNFV Security at Queen's University Belfast.
http://www.csit.qub.ac.uk/PhD-in-Cyber-Security-Centre-for-Doctoral-Training/PhD-Research-Projects-2017/
Interested candidates can contact Dr. Sandra Scott-Hayward (s.scott-hayward@qub.ac.uk).