Press release
Evry, 18 July 2023

Telecom SudParis launches an international Task Force for the standardization of a cyber and physical incident detection format

As part of the SECEF (Security Exchange Format) project supported by BPI and the Ile-de-France region, Telecom SudParis, a public engineering graduate school recognized for its high-level training and research in digital science and technology, is launching an international Task Force to support the standardization of a universal format for detecting incidents within cyber and physical systems (CPS).

The format, called IDMEFv2 (Incident Detection Message Exchange Format), extends the detection of cyber intrusions from the previous version to include all incidents. Following two years of experimentation, it has existed in draft form "IDMEFv2 IETF Draft" for six months and is registered with the international standards organization IETF (Internet Engineering Task Force).

Extending the detection of cyber-intrusions to include all incidents

In keeping with the IDMEFv1 format (RFC 4765- 2007) which has been in use for 15 years in the Open Source community, Telecom SudParis' research led to the creation of a new version of the IDMEF format to protect against combined, complex threats to physical and cyber infrastructure. The IDMEFv2 format's universality also makes it suitable for the field of smart systems, particularly autonomous vehicles, securing connected devices and for Industry 4.0.

The second version of the draft specifications for the IDMEFv2 format were published on 17 April with the IETF where the main internet standards are defined (HTTP, SMTP, FTP, etc.). Telecom SudParis has opened a dedicated website www.idmefv2.org based on this stabilized version, and in order to collect external contributions for the subsequent versions.

"*Our security monitoring systems are still extremely compartmentalized. It is very difficult, if not impossible, to detect complex, combined attacks, while the share of these types of incidents will continue to grow in the years ahead. Without a standard, it will also be very difficult to establish interoperability, which is crucial. Through its universality, the IDMEFv2 format fills a void in incident detection. Ultimately, it should allow us to improve incident prevention/detection/response – especially for sensitive sites and critical infrastructure, as well as for "smart" architectures – while reducing security monitoring costs by providing clear possibilities for convergence and pooling,*" said **Gilles Lehmann, a research engineer at Telecom SudParis, SECEF project leader and author of the IDMEFv2 format drafts.**

"Cyber-threats have changed significantly over the past two decades, especially since the gradual convergence of the cyber and physical worlds. At the same time, the need for collaboration and sharing information has become critical in order to combat the threat of cybercrime. IDMEFv2 takes up the basic concepts of IDMEFv1 and updates them to address these issues," said **Herve Debar, Deputy Dean of Telecom SudParis and Director of Research**, co-author of RFC 4765 for the IDMEFv1 format in 2007.

An international collaboration

Telecom SudParis co-founded the SECEF consortium with CentraleSupelec and CS Group in 2015 to promote format standardization in cybersecurity. Following a first stage of assessing and enhancing the IDMEFv1 format, the consortium is now tasked with standardizing an agnostic incident detection format that can describe all categories of incidents – whether cyber or physical, man-made or natural, past or potential in the future.

Within the SECEF consortium, Telecom SudParis's research is supported by its collaboration with the Teclib Group, a free software expert that develops and maintains libraries and open source tools on the dedicated website to test and improve this new format.

The IDMEFv2 Task Force has been expanded to include the experiments of the Horizon 2020 7SHIELD research project (22 partners from 12 countries) for the protection of critical infrastructure in European ground segments. Through this international collaboration, over 22 partners across Europe helped define the first version of the IDMEFv2 format and have been able to implement it on five pilot use cases in Europe (Belgium, Finland, Greece, Italy, Spain). It also includes cybersecurity companies such as Beware CyberLabs (simulation platform) Stamus Networks (detection/response to network threats) and end users like AP- HM (Public Assistance –Marseille Hospitals) with Philippe Tourron, CISO at AP- HM and coordinator of the European research project H2020 SafeCare (21 partners from 10 countries), which is similar to 7Shield, but for the hospital sector.

"This large-scale experiment along with our theoretical research allowed us to quickly validate many format concepts in situ, which is not always a simple task," said **Gilles Lehmann, a research engineer at Telecom SudParis, and SECEF project leader.**

"The use of the IDMEFv2 format was essential for our experiments. It enabled some thirty technical modules in our system architecture to communicate with one another in an efficient, seamless way. We look forward to supporting a future standardization," said **Gabriele Giunta, an expert in critical infrastructure security and head of the "Smart Transport and Infrastructure" unit at the IS3 R&D lab at** ENGINEERING and H2020 7Shield project coordinator.

Telecom SudParis press contacts – Agence Amalthea:
Clara Tonti: 01 76 21 67 54 – ctonti@amalthea.fr & **Sophie Rousset**: 01 76 21 67 53 – srousset@amalthea.fr

About Telecom SudParis

Telecom SudParis is a public engineering graduate school recognized for its high-level training and research in digital science and technology. Its outstanding teaching is based on the scientific excellence of its faculty and a focus on team project-based learning, disruptive innovation and entrepreneurship. There are currently 1,000 students enrolled at Telecom SudParis, including 700 engineering students and around 100 PhD students. Telecom SudParis is part of Institut Mines-Telecom (IMT), the leading group of engineering and management schools in France. The School is located on two campuses: in Evry-Courcouronnes with IMT-BS, and in Palaiseau with Telecom Paris. Telecom SudParis is a member of Institut Polytechnique de Paris (IP Paris), a world-class Institute of Science and Technology, along with École Polytechnique, ENSTA Paris, ENSAE Paris and Telecom Paris.