Communiqué de presse
Evry, le 18 juillet 2023

Télécom SudParis lance une *Task Force** internationale pour la standardisation d'un format de détection d'incidents cybers et physiques

Dans le cadre du projet SECEF (SECurity Exchange Format), soutenu par la BPI et la région Île-de-France, Télécom SudParis, grande école publique d'ingénieurs reconnue au meilleur niveau des sciences et technologies du numérique, lance une Task Force internationale pour soutenir la standardisation d'un format universel pour la détection d'incidents sur les systèmes cybers et physiques (CPS).

Ce format, intitulé IDMEFv2 (Incident Detection Message Exchange Format) étend la détection d'intrusions cyber de la version précédente à tous les incidents. Après deux ans d'expérimentation, il évolue depuis 6 mois sous forme de version préliminaire : « IDMEFv2 IETF Draft » déposé auprès de l'organisme de standardisation international IETF (Internet Engineering Task Force).

Une extension des détections d'intrusions cyber à tous les incidents

Dans la continuité du format IDMEFv1 (RFC 4765 - 2007) utilisé depuis 15 ans dans la communauté Open Source, les travaux de recherche de Télécom SudParis ont permis de créer une nouvelle version du format IDMEF pour la protection des menaces combinées et complexes sur les infrastructures cybernétiques et physiques. Grâce à son universalité, IDMEFv2 s'avère également pertinent dans le domaine des systèmes intelligents en particulier des véhicules autonomes, la sécurisation des objets connectés mais également pour l'industrie 4.0.

La deuxième version des spécifications préliminaires du format IDMEFv2 a été publiée le 17 avril dernier auprès de l'IETF où sont définis les principaux standards d'internet (HTTP, SMTP, FTP, etc.). A partir de cette version stabilisée, et afin de recueillir des contributions externes pour les versions suivantes, Télécom SudParis a ouvert un site dédié www.idmefv2.org.

"*Nos systèmes de supervision de sécurité sont encore extrêmement cloisonnés. Il est très difficile voire impossible de détecter des attaques ou des incidents complexes et combinés alors que la proportion de ce type d'incidents ne va pas cesser de croître dans les années à venir. Faute de standard ; l'interopérabilité, pourtant indispensable, est également très complexe à mettre en place. Le format IDMEFv2 par son universalité vient combler un vide dans la détection d'incidents. A terme, il doit permettre d'améliorer la prévention/détection/réaction d'incidents en particulier sur les sites sensibles et les infrastructures critiques mais également les architectures « intelligentes ». Cela tout en diminuant les coûts de supervision de sécurité grâce aux possibilités évidentes de convergence et de mutualisation*" commente **Gilles Lehmann, Ingénieur de recherche à Télécom SudParis, initiateur du projet SECEF et rédacteur des « drafts » du format IDMEFv2.**

"Les menaces cybers ont grandement évolué depuis 20 ans et plus particulièrement depuis la convergence progressive des mondes cybers et physiques. En parallèle, le besoin de collaboration et de partage d'information est devenu crucial pour contrer la menace cybercriminelle. IDMEFv2 reprend les concepts de base de IDMEFv1 en les actualisant et répond ainsi à ces enjeux" **Herve Debar, Directeur-adjoint en charge de la recherche de Télécom SudParis**, co-auteur de la RFC 4765 du format IDMEFv1 en 2007.

* *Groupe de travail*

Une collaboration internationale

Télécom SudParis est cofondateur avec CentraleSupelec et CS Group du consortium SECEF en 2015 pour promouvoir la normalisation des formats en cybersécurité. Après une première phase d'analyse et de valorisation du format IDMEFv1, le consortium est aujourd'hui en charge de la standardisation d'un format de détection d'incidents agnostique qui puisse décrire toutes les catégories d'incidents, qu'ils soient cybers ou physiques, d'origine humaine ou naturelle, passés ou potentiellement futurs.

Au sein du consortium SECEF, Télécom SudParis s'appuie pour ses travaux de recherche sur la collaboration de Teclib Group, expert en logiciel libre, qui développe et maintien sur le site dédié des librairies et des outils open-source pour tester et améliorer ce nouveau format.

La Task Force IDMEFv2 s'est élargie en intégrant les expérimentations du projet de recherche européen Horizon 2020 7Shield (22 partenaires dans 12 pays), pour la protection des infrastructures critiques des segments sols européens. Grâce à cette collaboration internationale, plus de vingt-deux partenaires à travers l'Europe, ont contribué à la définition de la première version du format IDMEFv2 et ont pu la déployer sur 5 pilotes réels en Europe (Belgique, Finlande, Grèce, Italie, Espagne). Elle regroupe également des éditeurs comme Beware CyberLabs (plateforme de simulation) et Stamus Networks (détection/réponse aux menaces réseaux) mais également des utilisateurs finaux à l'image de l'AP- HM (Assistance Publique – Hôpitaux de Marseille) avec M. Philippe Tourron, RSSI et coordonnateur du projet de recherche européen H2020 SafeCare (21 partenaires dans 10 pays) similaire à 7Shield mais dans le domaine hospitalier.

"Cette expérimentation à grande échelle en parallèle de nos travaux de recherche théoriques a permis de valider très tôt et in situ de nombreux concepts du format ce qui n'est pas toujours aisé." indique **Gilles Lehmann ingénieur de recherche à Télécom SudParis, initiateur du projet SECEF.**

"L'utilisation du format IDMEFv2 était essentielle pour nos expérimentations. Une trentaine de modules techniques de notre architecture système sont capables de communiquer entre eux grâce à ce format de manière très efficace et transparente. Nous nous réjouissons d'accompagner une future standardisation." confirme **Gabriele Giunta, expert en sécurité des infrastructures critiques, chef de l'unité "Transports et infrastructures intelligents" au sein du laboratoire de R&D IS3 à** ENGINEERING et coordonnateur du projet H2020 7Shield.

Contacts presse Télécom SudParis – Agence Amalthea :
Clara Tonti : 01 76 21 67 54 – ctonti@amalthea.fr & **Sophie Rousset** : 01 76 21 67 53 – srousset@amalthea.fr

À propos de Télécom SudParis

Télécom SudParis est une grande école publique d'ingénieurs reconnue au meilleur niveau des sciences et technologies du numérique. La qualité de ses formations est basée sur l'excellence scientifique de son corps professoral et une pédagogie mettant l'accent sur les projets d'équipes, l'innovation de rupture et l'entreprenariat. Télécom SudParis compte 1 000 étudiants dont 700 élèves ingénieurs et environ une centaine de doctorants. Télécom SudParis fait partie de l'Institut Mines-Télécom (IMT), premier groupe d'école d'ingénieurs en France. L'École est localisée sur deux campus : à Evry-Courcouronnes, avec IMT-BS et à Palaiseau avec Télécom Paris. Télécom SudParis est une école-membre de l'Institut Polytechnique de Paris (IP Paris), Institut de Sciences et Technologies à vocation mondiale avec l'École polytechnique, l'ENSTA Paris, l'ENSAE Paris et Télécom Paris.