



HAL
open science

DE SECNUM : un diplôme d'établissement pour former les experts en systèmes embarqués sécurisés

Florent Bruguier, Béatrice Pradarelli, Lionel Torres, Pascal Benoit

► To cite this version:

Florent Bruguier, Béatrice Pradarelli, Lionel Torres, Pascal Benoit. DE SECNUM : un diplôme d'établissement pour former les experts en systèmes embarqués sécurisés. Colloque sur les Objets et Systèmes connectés, May 2022, Dakar, Sénégal. lirmm-03729120

HAL Id: lirmm-03729120

<https://hal-lirmm.ccsd.cnrs.fr/lirmm-03729120>

Submitted on 20 Jul 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

DE SECNUM : un diplôme d'établissement pour former les experts en systèmes embarqués sécurisés

F. Bruguier^{a,c}, B. Pradarelli^{b,c}, L. Torres^{b,c}, P. Benoit^{b,c}

a IUT de Nîmes et Pôle CNFM de Montpellier (PCM), Université de Montpellier, Montpellier, France

b Polytech Montpellier et Pôle CNFM de Montpellier (PCM), Université de Montpellier, Montpellier, France

c LIRMM, Université de Montpellier, CNRS, Montpellier, France

Contact email : polytech-secnum@umontpellier.fr

RESUME : Dans un monde de plus en plus digitalisé, le nombre d'objets connectés ne cesse de croître. Afin d'assurer la sécurité de ce type d'objets, il est nécessaire d'en maîtriser la sécurité tant au niveau matériel que logiciel. C'est pourquoi nous proposons une nouvelle formation : un diplôme d'établissement BAC+6 spécialisé en sécurité des systèmes embarqués alliant à la fois cours théorique, mise en pratique à l'Université mais aussi en entreprise. La formation est dispensée par le pôle CNFM de Montpellier en partenariat avec l'IUT de Nîmes et Polytech Montpellier.

Mots clés : systèmes embarqués, sécurité numérique, diplôme d'établissement.

1 INTRODUCTION

En novembre 2018 lors d'un discours à l'UNESCO, le chef de l'état lançait l'appel de Paris pour la cybersécurité mondiale qui fut co-signé par 50 pays. Huit axes d'intervention étaient mis en avant parmi lesquels la prévention de la prolifération des programmes et techniques cyber-malicieuses mais aussi la sécurité des produits et services numériques. Afin de travailler sur ces axes de développement l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), dans son manifeste « Pour l'ANSSI des 10 prochaines années ; pour l'écosystème de la cybersécurité », a défini la formation comme une priorité de ces nouvelles orientations stratégiques. « Nous devons renforcer notre engagement dans la formation initiale et continue pour intégrer plus avant ces thématiques dans les formations... ». Dans la même veine, la région Occitanie, à travers la Stratégie Régionale de l'Innovation (SRI), a fait de la sécurité numérique une de ses priorités et a décidé de créer un portail de la cybersécurité en Occitanie : Cyber'Occ [1]. Parmi les 4 axes de travail de cette plateforme, on retrouve deux axes qui nous tiennent à cœur : la sécurité des systèmes embarqués et la formation.

Le diplôme présenté ici, le Diplôme d'Établissement (DE) SECNUM, diplôme de niveau BAC+6, s'inscrit dans la volonté de développer une formation d'experts en sécurité numérique des systèmes embarqués pour répondre à la carence d'ingénieurs spécialistes sur le marché. La formation est dispensée au sein du pôle CNFM de Montpellier en partenariat avec Polytech Montpellier et l'IUT de Nîmes.

L'objectif de ce DE est de répondre à un besoin sociétal d'accroître le nombre d'acteurs économiques ayant des compétences en cybersécurité pour protéger les données (médicales, agricoles, industrielles, personnelles) circulant dans une société de plus en plus numérique et connectée. Cette ambition est en phase avec les nouvelles orientations stratégiques de l'ANSSI paru le 21 janvier 2020 [6].

Cet article décrit la formation proposée dans le cadre du DE SECNUM. Après avoir décrit le besoin et présenté le contexte, nous décrierons les objectifs pédagogiques ainsi que les principaux enseignements proposés. Enfin nous proposerons des pistes d'évolution pour cette formation.

2 PERTINENCE ET CONTEXTE

2.1 Besoin en ingénieurs spécialisés en sécurité des systèmes embarqués

Afin de vérifier la pertinence de créer une formation sur cette thématique forte d'un déficit en candidats, nous avons réalisé une étude des formations proposées en région.

Cette étude approfondie des formations disponibles sur la région Occitanie a mis en évidence une offre variée des formations dans le domaine au niveau licence (une dizaine sur l'Occitanie) et un déficit de formations pour le niveau supérieur notamment sur le bassin montpelliérain comme le montre la carte proposée sur la Figure 1. La thématique est seulement abordée dans certains modules, comme par exemple, pour les élèves ingénieurs en 4ème année de la spécialité EII (Electronique Informatique Industrielle) et les apprentis ingénieurs en 5ème année de la spécialité SE (Système Embarqué) mais aussi du département IG (« Informatique et Gestion ») sans pour autant faire des étudiants des experts du domaine. Les autres formations proposent des compétences dans des domaines éloignés de celui des systèmes embarqués comme par exemple la sécurité réseau ou encore la sécurité des systèmes d'information.

Or, il ressort de l'étude initiale du bassin économique montpelliérain, étendue ensuite à l'Occitanie que le profil des salariés actuellement en poste et celui des candidats recherchés par les entreprises est un profil d'ingénieur « spécialiste » de niveau BAC+5 ou BAC+6.

2.2 Contexte local

Le projet proposé ici, le Diplôme d'Établissement (DE) SECNUM, diplôme de niveau BAC+6, s'inscrit dans la volonté de l'établissement porteur Polytech Montpellier de développer une formation d'experts en sécurité numérique des systèmes embarqués pour répondre à la carence d'ingénieurs spécialistes sur le marché.

Ce projet est co-porté par l'IUT de Nîmes auquel est rattaché le responsable de la plateforme « SECNUM » [2]. Cette plateforme, issue des activités de recherche du LIRMM, permet de sensibiliser et former les étudiants du l'Université de Montpellier aux problématiques de la sécurité numérique à travers l'étude des attaques par canaux cachés [3]. Plusieurs initiatives d'excellence pédagogique ont été développées sur cette plateforme au travers notamment d'un projet d'innovation pédagogique : AMUSE [4-5]. Ce projet a fait l'objet de plusieurs publications internationales valorisant l'approche pédagogique innovante (serious game) mise en œuvre pour enseigner la sécurité numérique. Il a aussi reçu le prix « Coup de cœur du Jury » lors des Rencontres Cybersécurité en Occitanie en 2019.

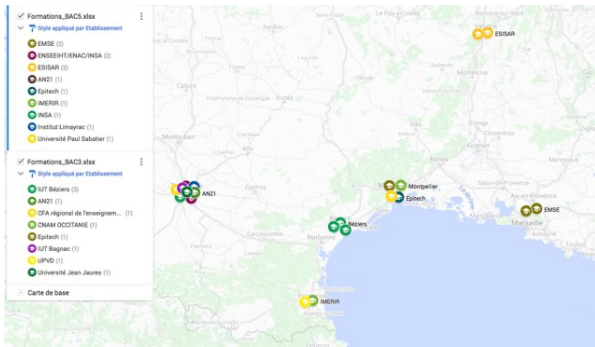


Figure 1 : Cartographie des formations en cybersécurité.

Ce co-portage affiche l'ancrage de Polytech Montpellier et de l'IUT de Nîmes au sein de l'Université de Montpellier. Il est aussi un gage de confiance et de conviction que la transdisciplinarité permet de relever le défi de créer une formation orientée compétences métier en rassemblant les expertises pédagogiques et scientifiques (électronique, système embarqué & informatique) nécessaires.

2.3 Métiers visés

Afin de définir les métiers ciblés, nous nous sommes appuyés sur les besoins retournés par les entreprises local et avons défini les profils à l'aide du panorama des métiers réalisés par l'ANSSI [7].

Les métiers ciblés par le DE sont les suivants :

- Évaluateur de la sécurité des technologies de l'information (Hardware)
- Évaluateur cybersécurité
- Architecte de sécurité
- Experte en test d'intrusions
- Consultant en sécurité
- Cryptologue

- Ingénieur d'études de systèmes spécifiques dans le secteur des services

3 PRESENTATION DE LA FORMATION

3.1 Equipe pédagogique

L'équipe enseignante est composée d'une dizaine d'enseignants-chercheurs, de chercheurs et de doctorants du LIRMM, tous experts en sécurité numérique de par leurs travaux de recherche, leurs participations à des conférences nationales et internationales, ainsi que par leurs collaborations avec des entreprises de ce domaine. Des spécialistes du secteur industriel interviendront également lors des enseignements mais aussi lors de conférences sur des thématiques actuelles pour rapprocher les stagiaires du monde socio-économique.

3.2 Enseignements

La formation se déroule sur une année avec un volume horaire de 200h pour les enseignements académiques auquel il faut ajouter 100 heures de projets tuteurés. Ces enseignements se déroulent sur 3 périodes de 4 semaines. Le reste de l'année, les étudiants sont à la disposition de l'entreprise. La capacité d'accueil est d'une vingtaine d'étudiants.

Le DE cybersécurité est ouvert en formation initiale pour permettre à tout étudiant de se spécialiser dans ce domaine et en formation continue afin de pouvoir accueillir tout salarié ou demandeur d'emploi souhaitant renforcer ses compétences ou changer d'orientation de carrière. Le DU vise son enregistrement au Répertoire Spécifique par France Compétences afin de pouvoir être répertorié dans la liste des formations diplômantes accessibles depuis l'application « Mon compte Formation » et financés par le CPF (Compte personnel de Formation) dont dispose chaque salarié et demandeur d'emploi.

3.2.1 Unités d'enseignement académiques

Les contenus pédagogiques de la maquette ont été élaborés avec le concours des filières impliquées dans la formation en cybersécurité, dont notamment l'IUT de Béziers. La volonté est de mettre en œuvre une approche par compétences, basée sur l'analyse de situations de travail s'appuyant sur les recommandations de l'ANSSI et notamment le panorama des métiers de la cybersécurité [7].

Le DE est constitué de modules spécifiques et transversaux dont la majorité sont dispensés en anglais afin d'immerger les stagiaires dans la terminologie anglo-saxonne. Cette action linguistique s'inscrit dans la volonté de donner une coloration internationale au DE et d'offrir aux stagiaires l'opportunité de se former dans un environnement proche de celui rencontré en entreprise. Le DE contient 5 Unités d'Enseignement (UE) académiques pour un total de 200h d'enseignement. La première, Fondamentaux de la cryptographie, est constitué de deux modules : Théorie, principes, algorithmes de

chiffrement et standards, et Statistiques pour la cryptographie. La seconde UE se focalise sur la sécurisation des applications embarquées à travers 4 modules (Prototypage de systèmes embarqués sécurisés ; Vulnérabilité et preuve formelle ; Conception, techniques d'attaques et contremesures associées ; Injection de fautes). La troisième UE est centrée autour de la Sécurisation des réseaux, protocoles et infrastructures et contient 3 modules : Sécurité des réseaux et des communications, Protocoles IoT, et Sécurité des infrastructures.

La dernière UE permet d'aborder les aspects réglementaires, juridiques et aspects experts. La place des questions juridiques dans le monde de la cybersécurité s'étant considérablement accrue ces dernières années, l'enseignement de sciences juridiques et sociales (droit, éthique, social engineering) fait partie intégrante de la maquette. L'insertion de tels modules au sein de cette formation high-tech donne une coloration interdisciplinaire qui valorise l'employabilité des stagiaires à l'issue du DE.

La répartition des volumes horaires est proposée dans le tableau 1.

3.2.2 Unités d'enseignement professionnelles

La partie professionnelle du DE est composée de deux UE. La première, le projet tuteuré est une mise en situation de l'étudiant sur un sujet qui est spécifique à son projet professionnel. Le projet tuteuré s'effectue à l'Université soit dans les locaux du pôle CNFM de Montpellier soit en laboratoire en fonction des besoins en matériel nécessaire. Pour les étudiants en alternance, le sujet est proposé par l'entreprise en accord avec le tuteur académique en charge de l'étudiant correspondant.

3.3 Participation à des CTF

Par ailleurs, dans le domaine de la sécurité, la participation à des « serious game » appelés CTF (« Capture The Flag ») est un moyen à la fois ludique et utile de développer un réseau de contacts dans le domaine de la sécurité, ainsi que d'approfondir les connaissances académiques à des applications très concrètes. Lors de ces jeux, les participants sont amenés à détecter des failles de sécurité afin de pénétrer au fur et à mesure dans un système ou un réseau. Cette méthode de pédagogie active permet aux étudiants de comprendre les stratégies malveillantes mises en œuvre par les attaquants afin qu'ils appréhendent au mieux les méthodes de sécurisation. Ils percevront ainsi plus aisément les enjeux et défis de leur futur métier. Les étudiants seront amenés tout au long de l'année à travailler sur ce type de problèmes pour améliorer leurs connaissances et compétences. En fin de formation, les étudiants seront incités à participer à un événement de type CTF d'envergure nationale ou internationale (Defcon ou Black Hat), où ils pourront se confronter aux étudiants des autres formations. Ces événements étant accompagnés de conférences d'experts sur les dernières avancées du domaine, cela sera l'occasion de parfaire leur formation. L'ensemble contribuera à l'acquisition des compétences requises pour la

réalisation d'une activité professionnelle à haut niveau d'expertise.

4 AMELIORATIONS

4.1 Diplôme

Lors de cette première mouture du diplôme, nous avons choisi de présenter la formation sous la forme d'un diplôme d'établissement. Cette première version du diplôme permet de mettre en place les premiers enseignements mais aussi de tisser de nouvelles relations avec les entreprises spécialisées du domaine. Il est envisagé dans un futur proche de faire évoluer la formation vers un Mastère spécialisé des grandes écoles. Ce format permettra d'avoir un cadre précis pour le diplôme mais aussi d'augmenter sa visibilité auprès des futurs candidats et des futurs recruteurs.

4.2 Enseignements innovants

L'équipe enseignante s'appuiera sur le Centre de Soutien aux Innovations Pédagogiques (CSIP) pour définir une stratégie pédagogique innovante, pertinente et actuelle (par exemple le design thinking), permettant de répondre aux besoins métiers. Cette démarche éducative aura pour objectif d'optimiser l'apprentissage des savoirs et savoir-faire techniques réalisés sur les différentes plateformes logicielles et matérielles du pôle CNFM de Montpellier mises à la disposition des apprenants lors des pratiques en situation. Elle favorisera aussi l'acquisition de savoir-être génériques (softskills) comme la collaboration, la communication, l'écoute, la prise de décision et de savoir-être spécifiques au contexte de la sécurité comme le social engineering. Cette stratégie reposera sur des méthodes pédagogiques comme l'apprentissage mutuel et par problèmes, le serious game « AMUSE » où le stagiaire est acteur de son apprentissage. Le développement d'une version immersive du serious game est envisagé en utilisant les ressources logicielles et matérielles de la salle MUSE VR. L'objectif sera à la fois la découverte du contexte de la cybersécurité et l'évaluation des acquis d'apprentissage.

4.3 Labélisation

Afin de garantir l'excellence de notre formation ainsi que sa visibilité au niveau national, nous souhaitons demander pour notre diplôme d'établissement la labélisation SecNumedu [8]. Ce label, délivré par l'ANSSI garanti le niveau des formations qui consacrent au moins 70% de leur temps à la cybersécurité et qui allient théorie et pratique. Il est aussi un gage de qualité et récompense la pertinence du programme pédagogique de la formation.

Lors des prochaines éditions de la formation, les étudiants seront amenés à passer des certifications métier telles que la certification Cisco Industrial Networking Specialist pour l'Internet des Objets. Ces certifications peuvent être un atout supplémentaire lors de la recherche d'emploi dans le domaine.

5 CONCLUSION

Ce papier présente le diplôme d'établissement SECNUM. Ce diplôme de niveau BAC+6 permet de former des étudiants à la sécurité des systèmes embarqués. Elle s'appuie sur 200h de formation académique ainsi qu'un projet tuteuré et 580h de stage ou de présence en entreprise. Plusieurs pistes d'amélioration ont été identifiées avec notamment l'évolution vers un nouveau diplôme mais aussi la mise en place de certifications académiques et professionnelles.

REMERCIEMENTS

Les auteurs remercient l'Agence Nationale de la Recherche (ANR) pour le support apporté grâce au financement ANR-16-IDEX-0006 (I-SITE MUSE, projet DE SECNUM).

Bibliographie

- [1] Cyber'OCC portail cybersécurité d'Occitanie: website: <https://www.cyberocc.com/> (Accès octobre 2021).
- [2] M. Bourrée, et al.: "Secnum: an open characterizing platform for integrated circuits", Euro. Work. Microelectronics Education, 2012, Grenoble, France, pp. 88-91.
- [3] F. Bruguier, P. Benoit, L. Torres : "Enseignement de la sécurité numérique : De la sensibilisation à l'expertise", J3eA, 2017.
- [4] Bruguier, F., P. Benoit, L. Dalmasso, B. Pradarelli, E. Lecointre, and L. Torres. "AMUSE: l'escape game pour s'évader en toute sécurité-Enseignement de la sécurité numérique sous forme d'un escape game." J3eA 18 (2019).
- [5] Bruguier, F., Lecointre, E., Pradarelli, B., Dalmasso, L., Benoit, P. and Torres, L., 2020, February. Teaching Hardware Security: Earnings of an Introduction proposed as an Escape Game. In International Conference on Remote Engineering and Virtual Instrumentation (pp. 729-741). Springer, Cham.
- [6] ANSSI : Communiqué de presse : https://www.ssi.gouv.fr/uploads/2020/01/anssi-communique_presse-orientations_strategiques.pdf (Accès octobre 2021)
- [7] ANSSI, Panorama des métiers de la cybersécurité : https://www.ssi.gouv.fr/uploads/2015/07/anssi-panorama_metiers_cybersecurite-2020.pdf (Accès octobre 2021)
- [8] Label SecnumEdu, ANSSI, site internet : <https://www.ssi.gouv.fr/entreprise/formations/secnumedu/> (Accès octobre 2021).

Unité d'Enseignement	Module	Volume horaire (h)
UE 1 - Fondamentaux de la cryptologie		50
	Principes, algorithmes de chiffrement (symétrique, asymétrique) et standards	30
	Statistiques pour la cryptographie	20
UE 2 - Sécurisation des applications embarquées		69
	Prototypage de systèmes embarqués sécurisés	20
	Vulnérabilité et preuve formelle	9
	Conception, techniques d'attaques et contremesures associées	30
UE 3 - Sécurisation des réseaux, protocoles et infrastructures		46
	Injection de fautes	10
	Sécurité des réseaux et des communications	16
UE 4 – Aspects réglementaires, juridiques et experts de la sécurité numérique	Protocoles IoT	12
	Sécurité des infrastructures	18
		35
UE 5 – Projet tuteuré	Aspects réglementaires et juridiques	17
	Aspects experts	18
UE 6 – Entreprise		100
		560

TABLEAU I. UE et modules d'enseignement du DE SECNUM.