DE SECNUM : former les futurs experts des 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

Dans un monde de plus en plus digitalisé, le nombre d'objets connectés ne cesse de croitre. Afin d'assurer la sécurité de ce type d'objets, il est nécessaire d'en maitriser la sécurité tant au niveau matériel que logiciel. L'objectif de ce papier est de présenter une formation dispensée par le pôle CNFM de Montpellier. Ce diplôme d'établissement de niveau BAC+6 spécialisé en sécurité des systèmes embarqués allie à la fois cours théorique, mise en pratique à l'Université mais aussi en entreprise.

I. 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-malicieux 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 parues le 21 janvier 2020 (6).

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20241002

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.

II. Pertinence et contexte

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.

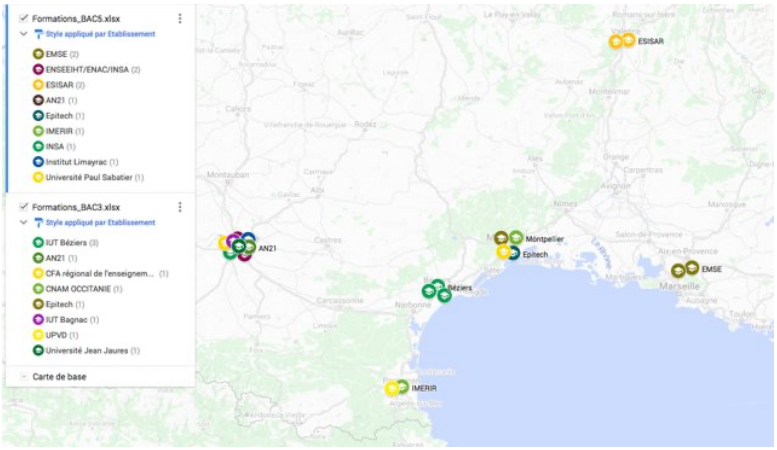

Fig.1. Cartographie des formations en cybersécurité.

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. 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.

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.

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 réalisé 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.

III. Présentation de la formation

1. Équipe 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.

2. Enseignements

La formation se déroule sur une année avec un volume horaire de 290h 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 quinzaine d'étudiants.

Le DE cybersécurité est ouvert en formation continue sous forme de contrat de professionnalisation que ce soit pour des étudiants fraichement diplômés ou des salariés ou demandeurs d'emploi souhaitant renforcer leurs compétences ou changer d'orientation de carrière. Il 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.

a. 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 peuvent être 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 4 Unités d'Enseignement (UE) académiques pour un total de 290h d'enseignement. La premier, 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.

b. 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.

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

Unité d'Enseignement	Module	Volume horaire (h)
UE 1 - Fondamentaux de la cryptologie		63
	Principes, algorithmes de chiffrement (symétrique, asymétrique) et standards	36
	Statistiques pour la cryptographie	27
UE 2 - Sécurisation des applications embarquées		81
	Prototypage de systèmes embarqués sécurisés	21
	Vulnérabilité et preuve formelle	9
	Conception, techniques d'attaques et contremesures associées	30
	Expérimentation sur plateformes d'analyse	6
	Injection de fautes	15

UE 3 - Sécurisation des réseaux, protocoles et infrastructures		54
	Sécurité des réseaux et des communications	16
	Protocoles IoT	12
	Certification CSNA Stormshield	8
	Sécurité des infrastructures	18
UE 4 – Aspects réglementaires, juridiques et experts de la sécurité numérique		74
	Aspects réglementaires et juridiques	17
	Gestion de projet	8
	Forensic	21
	Aspects experts	18
UE 5 – Projet tueuré		100
UE 6 – Entreprise		560

c. 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 évènement de type CTF d'envergure nationale ou internationale (Defcon ou Black Hat), où ils pourront se confronter aux étudiants des autres formations. Ces évènements 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.

IV. Améliorations

1. Diplôme

Lors des trois premières moutures 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 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.

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 plate-formes logicielles et matérielles du pôle CNFM de Montpellier mises à la disposition des apprenants lors des pratiques en situation. Ellefavorisera 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 contextede la sécurité comme le social engineering. Cette stratégie reposera sur des méthodespédagogiques comme l'apprentissage mutuel et par problèmes, le serious game « AMUSE» où le stagiaire est acteur de son apprentissage.

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.

V. 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 290h de formation académique ainsi qu'un projet tuteuré et 1.260h de présence en entreprise. Plusieurs pistes d'amélioration ont été identifiée avec notamment l'évolution vers un nouveau diplôme mais aussi la mise en place de certifications académiques et professionnelles. Le découpage de ce diplôme en deux options (industrie et santé) est également en cours d'étude.

Remerciements

Les auteurs remercient l'Agence Nationale de la Recherche (ANR) pour le support apporté grâce aux financements ANR-16-IDEX-0006 (I-SITE MUSE, projet DE SECNUM) et ANR-23-CMAS-0024 (France 30, INFORISM).

Références

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*, Grenoble, France, pp. 88-91 (2012).
3. F. Bruguier, P. Benoit, L. Torres : "Enseignement de la sécurité numérique : De la sensibilisation à l'expertise", J3eA, 2017.
4. F. Bruguier, 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. F. Bruguier, E. Lecointre, B. Pradarelli, L. Dalmasso, P. Benoit, and L.Torres, . Teaching Hardware Security: Earnings of an Introduction proposed as an Escape Game. In *International Conference onRemote Engineering and Virtual Instrumentation, Springer, Cham.* pp. 729-741 (2020).
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).