TLS-SEC : une nouvelle formation en sécurité à Toulouse

TLS-SEC est une nouvelle formation en sécurité des systèmes d'information sous la forme d'une dernière année d'école d'ingénieur et validant un parcours dans le cadre du master Réseaux et Télécommunications de l'Université Fédérale de Toulouse Midi-Pyrénées. Cette formation est commune à l'INP-ENSEEIHT, l'INSA, l'ENAC, les Mines d'Albi et le Centre Universitaire Jean-François Champollion et concerne 24 étudiants depuis septembre 2015. Elle évoluera vers 36 ou 48 étudiants. L'INP-ENSEEIHT, l'INSA, et l'ENAC sont co-porteurs de cette formation.

Contexte :

La sécurité des systèmes d'information (SSI) est un domaine porteur dans le secteur de l'emploi depuis de nombreuses années et, au vu de l'évolution de notre société vers l'informatique ubiquitaire, il est peu probable que cela change. Les menaces visant les systèmes informatiques sont aujourd'hui bien réelles et il est fondamental qu'un jeune ingénieur informaticien ait une culture minimum dans ce domaine. Les industriels ont de plus en plus besoin de personnel au fait des problèmes de sécurité, en particulier dans le contexte des industries de pointe, développant des systèmes critiques, comme c'est le cas de la région Midi-Pyrénées. Nous pouvons en particulier remarquer les initiatives dans la région comme Albatros1 (avec Airbus, Steria, etc.), l'expansion de Thalès, et la migration de l'ensemble des services sécurité de Steria sur Toulouse. De même, les services gouvernementaux se soucient de plus en plus des problèmes de sécurité informatique, qui aujourd'hui, peuvent réellement mettre un état en danger. On parle de plus en plus de cyber-sécurité, de cyber-guerre et l'Agence Nationale de la Sécurité des Systèmes d'Information (l'ANSSI) ne cesse de recruter massivement des experts en sécurité informatique.

Dans les différentes formations de écoles membres de Toulouse Ingénierie (TI), les étudiants ont souvent quelques notions de SSI, abordées dans quelques cours, de façon à donner aux étudiants cette "culture de la sécurité" qui est considérée comme indispensable pour un jeune ingénieur. Cependant, il n'existe actuellement pas de formation dédiée, qui permette à des ingénieurs de développer une forte expertise en sécurité informatique dans la région. L'ANSSI, dont une des missions est le suivi et la mise en place de formations en sécurité en France, maintient une carte de ces formations et Toulouse est la seule grande ville ne disposant pas d'une telle formation au niveau Master. La formation TLS-SEC a pour vocation de combler ce manque. Pour cela, les différentes écoles d'ingénieurs proposant déjà une formation en SSI (comme à l'INSA sous la forme d'une mineure) ou étant en cours de mise en place de formation en SSI (comme à l'INP-ENSEEIHT ou à l'ENAC), ont décidé de fusionner leurs efforts et de créer une formation commune et co-portée au sein de TI en SSI. Les entreprises de la région Toulousaine mais aussi extérieures à la région Midi-Pyrénees, à qui nous avons présenté le projet sont unanimement intéressées et beaucoup d'entre elles ont proposé de participer à cette formation. Parmi celles-ci nous pouvons remarquer en particulier : Airbus, Thalès, Steria, QuarksLab et Apsys (expert sécurité du groupe EADS). Enfin, suite à la validation de notre programme, l'Agence Nationale de la Sécurité des Systèmes d'Information a également décidé de participer à la formation. Le but de TLS-SEC est donc de proposer une formation de niveau Master donnant une réelle expertise en sécurité informatique dans la région. Elle est composée d'un premier semestre avec environ 400h d'enseignements et d'un stage de 6 mois effectué lors du second semestre.

Contenu de la formation :

Le premier semestre est composé d'environ 350h de formation, organisées sous forme de 4 modules (dont 100h de TP) ainsi que 60h de compétences professionnalisantes (anglais et sciences humaines).

Ces modules s'intitulent :

Module 1 : Bases de la sécurité informatique : environ 90h

Module 2 : Sécurité logiciel/système/matériel : environ 100h
Module 3 : Sécurité des réseaux : environ 90h
Module 4 : Aspects transverses : intrusion, gouvernance, vie privée, sécurité et aérospatial : environ 90h

Le second semestre est composé au choix d'un projet long (d'une durée d'un mois environ), ou de passages de certifications (notamment Cisco CCNA Security) ou de réalisation de challenges, ainsi que d'un stage obligaoire de 6 mois.

Le module 1 ne nécessite pas compétence en sécurité informatique mais il nécessite un minimum de connaissance en informatique et en programmation. Une partie de ce module est consacré à une mise à niveau des étudiants sur la programmation en langage C et assembleur, ainsi que sur les architectures des ordinateurs et les réseaux informatiques mais cette mise à niveau suppose que les candidats aient déjà des bonnes connaissances en informatique et en programmation. Les compétences acquises à la fin de ce module concernent 1) la maîtrise de la terminlogie et des définitions associées au monde de la sécurité informatique et 2) une bonne compréhension des principes de la cryptographie. Ce module propose ainsi un tour d'horizon assez large de toute la terminologie qu'il est nécessaire d'appréhender dans ce domaine et propose également un cours assez etoffé sur la cryptographie.

Le module 2 nécessite d'avoir suivi le module 1 ou de posséder des bonnes compétences dans la programmation bas-niveau (C, assembleur), dans les protocoles réseaux et d'avoir un minim de culture et de connaissances du monde de la sécurité informatique. En particulier, toute la terminologie doit être connue et les principes fondamentaux de la cryptographie doivent être acquis par le candidat. A l'issue de ce module, l'étudiant aura acquis de solides compétences sur la sécurité du logiciel (comprendre les attaques qui ciblent le logiciel mais aussi les moyens de défense associés), sur la sécurité des systémes d'exploitation (avec une focus sur les systèmes Unix et Windows), ainsi que sur la sécurité du matériel (les attaques ciblant le matériel ainsi que les contre-mesures seront abordées).

Le module 3 nécessite d'avoir suivi le module 1, ou de posséder de bonnes compétences dans l'informatique en général et dans la compréhension des protocoles réseaux qui régissent l'Internet (TCP/IP, protocoles de routage a minima) . En particulier, toute la terminologie doit être connue et les principes fondamentaux de la cryptographie doivent être acquis par le candidat. A l'issue de ce module, l'étudiant sera capable de comprendre l'ensemble des menaces qui pèsent sur les réseaux TCP/IP aujourd'hui ainsi que les attaques associées. Il sera également capable de concevoir et mettre en place des architectures réseaux sécurisés et les techologies associées (firewalls, outils de détection ou de prévention d'intrusions, tunnels et protocoles sécurisés).

Le module 4 nécessite d'avoir suivi les modules 1, 2 et 3 ou de posséder de solides compétences en sécurité des systèmes et des réseaux. A l'issue de ce module, le candidat sera capable de comprendre les principes fondamentaux de la sécurité organisationnelle, des principales normes associées, de l'utilité d'une politique de sécurité et des modèles associés. Il aura également compris les spécificités des problématiques de sécurité du domaine aérospatial, des principales menaces et contre-mesures existantes, spécifiques à ce domaine. Il aura enfin été sensibilité au problème de la protection de la vie privée.

Quelques points forts de cette formation :

Les intervenants

Dans cette formation, notre volonté est de faire intervenir à la fois des acteurs majeurs du monde académique, du monde industriel et du monde gouvernemental. Nous avons ainsi réussi à réunir des personnes issues de sociétés incontournables dans le domaine de la sécurité mais aussi issues des sociétés incontournables de la région Midi-Pyrénées, pour participer à une formation structurée, complète et cohérente vis-à-vis du métier d'expert en

sécurité informatique.

Les projets

Dès le démarrage de l'année scolaire les étudiants sont regroupés en quatre équipes de six personnes avec des profils variés au niveau des compétences d'entrée (électronique, réseau, système, programmation, mathématiques). L'évaluation est en grande partie par projets, où les équipes sont en concurrence. Pour éviter une surspécialisation des étudiants, des rotations sont réalisées sur les postes.

Les challenges

Il est habituel dans les formations en sécurité de participer aux challenges en ligne nationaux ou internationaux. Un des principaux objectifs que nous nous sommes donnés est la participation à ces challenges. De nombreuses ressources en ligne sont disponibles pour préparer ces challenges et nous avons déjà donné des pointeurs vers ces ressources aux étudiants qui ont déjà déposé leur dossier de candidature. Nous avons également des challenges que nous avons développé nous mêmes. Ces challenges seront structurés sous la forme d'une suite de défis qui permettent aux étudiants de pénétrer au fur et à mesure au cœur d'un système d'informations ou d'un réseau vulnérable. Cette méthode d'apprentissage active permet aux étudiants de mieux cerner les stratégies d'attaque que des personnes malveillantes peuvent adopter lors d'une attaque informatique. Elle présente alors l'avantage de leur faire réaliser les enjeux, défis et difficultés de leur futur métier.

Les conférences

Un ensemble de conférences est mis en place pour permettre à des intervenants industriels et gouvernementaux d'illustrer les concepts théoriques vus lors des différents enseignements. Cette forme d'apprentissage permet aux étudiants 1) d'être sensibilisé aux implications de la mise en place de la sécurité informatique au sein d'une entreprise et au sein d'un état, et 2) de mettre en perspective leurs acquis vis-à-vis des problématiques concrètes rencontrées dans le monde industriel ou gouvernemental.

Un lieu privilégié d'enseignement

Pour la mise en place de ces techniques pédagogiques, une salle en libre accès est un atout important de la formation et contribue tout particulièrement à l'auto-formation et l'entraide. Quasiment tous les cours et les TPS ont lieu dans cete salle et chaque étudiant a donc une machine personnelle à sa disposition pendant toute l'année. En ce qui concerne les pédagogies innovantes, il est important de souligner qu'elles sont déjà utilisées par les co-porteurs de TLS-SEC depuis plusieurs années. A titre d'exemple, les challenges proposés dans la formation TLS-SEC sont actuellement mis en place à l'INSA (dans le cadre de la mineure Sécurité), et à l'ENAC et l'ENSEEIHT, au sein de leurs enseignements de sécurité. Par ailleurs, le programme actuel de la mineure sécurité de l'INSA comprend une journée complète de conférences sur la sécurité informatique, donné par des experts issus du monde académique et industriel. Cet existant est un atout précieux pour TLS-SEC.

Objectifs dans le cadre de RESSI

Nous proposons dans le cadre de RESSI de donner un aperçu, non seulement de la formation elle-même, mais aussi du travail qu'il a fallu mener pour monter cette formation inter écoles d'ingénieur. Par ailleurs, comme cette formation est toute jeune, nous proposons de dresser un premier bilan de cette première année et de faire profiter la communauté de notre retour d'expérience.