Chaire en cybersécurité des systèmes communicants

1. Positionnement

La cybersécurité a pour objectif d'analyser et de concevoir des systèmes informatiques et de communications qui garantissent la confidentialité, l'intégrité, la disponibilité des communications ainsi que le respect de la vie privée. Ces systèmes se retrouvent dans diverses applications et un grand nombre de domaines tels que les télécommunications, l'électronique embarquée, les réseaux informatiques, l'internet des objets ainsi que dans les domaines stratégiques tels que l'énergie, les transports, le monde médical, le monde bancaire, …

La recherche et la formation dans ce domaine doivent répondre aux défis de l'apparition permanente de nouvelles techniques d'attaques, l'émergence de systèmes toujours plus connectés et la complexité des protocoles qui ouvrent la voie à des attaques de plus en plus complexes et aux conséquences dévastatrices.

Dans un futur proche, tout système qui sera développé devra explicitement intégrer dès sa conception des mécanismes cryptographiques et de sécurité. La recherche dans le domaine des télécommunications ainsi que la formation de nos ingénieurs doit passer par la mise en oeuvre d'une maîtrise approfondie de la cybersécurité pour pouvoir développer les technologies IT du futur.

La cybersécurité est un domaine spécifique de recherche et d'enseignement qui en pleine expansion au niveau mondial. L'ULB possède une expérience établie et reconnue dans le domaine ; depuis 2015, l'institution s'inscrit dans une stratégie de consolidation à travers (1) la création d'un master inter-universitaire (ULB, UCL, UNamur, ERM, ESI, HELB) qui rencontre un franc succès (92 étudiants inscrits en 2018-2019) et (2) la mise sur pied d'un centre inter-facultaire (Faculté des Sciences - Ecole Polytechnique) de recherche en cybersécurité.

2. Pourquoi cette chaire est une priorité pour l'Ecole Polytechnique et la filière "éléctronique / télécom" (Elec)

Le domaine de la cybersécurité des systèmes communicants se trouve intrinsèquement à l'intersection de plusieurs domaines de recherche fondamentale et appliquée. Actuellement, le Master ELEC est essentiellement tourné vers l'électronique et les couches basses des télécommunications (transmission radio, codage, traitement du signal). D'autre part, le Master cybersécurité (conjoint entre l'EPB et la faculté des Sciences à l'ULB) repose essentiellement

sur l'enseignement de la cryptographie, de la sécurité et des protocoles réseaux. L'objectif de la chaire est de faire le lien entre les deux aspects et de suivre dès lors une approche plus globale de la cybersécurité. Il s'agira d'étudier comment la sécurité d'un système communicant peut être conçue à travers l'ensemble des couches du système (électronique, couche physique, modulation et couche réseau).

Caractère stratégique

Au niveau industriel, la cybersécurité est devenue une priorité tant pour les aspects opérationnels (gestion et renforcement des technologies existantes) que lors du développement de nouveaux systèmes. C'est pourquoi en 2018 l'ULB a signé une convention cadre avec THALES (entreprise leader dans le domaine de la cybersécurité) pour renforcer l'accueil de stagiaires, de mémorants et de chercheurs au sein de l'entreprise.

La formation d'ingénieur doit donc intégrer ces aspects et renforcer cet enseignement dans l'ensemble des cours à vocation digitale (réseaux, électronique, informatique). La cybersécurité moderne requiert une approche transdisciplinaire, ce qui est parfaitement aligné avec l'approche prônée par l'École Polytechnique. En effet, tout système se conçoit en partant de l'électronique jusqu'au protocole réseau, en passant par les implémentations en couche physique et la conception du modem. C'est pourquoi il nous semble indispensable de proposer cet axe de formation en sécurisation des systèmes communicants pour l'ensemble des futurs ingénieurs en télécommunications au travers d'un renforcement des fondements théoriques ainsi que par une connaissance concrète acquise lors de projets intégrés (multi-disciplinaires) qui mettront en oeuvre des mécanismes et des architectures de sécurité.

L'engagement d'un professeur dans le domaine de la conception sécurisée de systèmes communicants est indispensable afin de renforcer les synergies en cours au niveau recherche et enseignement. Il s'agit de proposer une recherche à la fois de pointe et interdisciplinaire dans le domaine et de renforcer les axes de recherches dans les domaines des communications sécurisées.

Au niveau Facultaire, la thématique de la cybersécurité s'intègre dans le thème de recherche cross-disciplinaire *sécurité* du projet pôles de recherche qui est soutenu par l'École. Cette thématique permet également de créer une dynamique de recherche autour de la plateforme ICT et qui peut fédérer de nombreux laboratoires de recherche.

Possibilités d'intégration dans l'équipe existante

Depuis une dizaine d'années le groupe OPERA WCG (Wireless Communications Group) rassemble les activités de recherche et d'enseignement liées aux communications sans-fil et les réseaux de télécommunications. De nombreux fonds de recherche ont été levés (FER, INNOVIRIS, EOS, Feder, etc.) pour soutenir l'activité "couche physique" et "cybersécurité". Une convention Erasmus a été signée dans le domaine de la cybersécurité avec l'Université de Bretagne Sud (UBS - Vannes, France) ainsi qu'avec le leader mondial du secteur: THALES.

L'équipe OPERA-WCG collabore également au niveau de l'ULB avec la Faculté des Sciences (cryptographie et protocoles cryptographiques : Olivier Markowitch, et systèmes et réseaux

temps-réels critiques: Joël Goossens) et au sein de l'Ecole Polytechnique avec le service BEAMS-EE (projet ARC: SOFIST de sécurisation des protocoles sur chips électroniques). L'objectif est de renforcer et fédérer l'acquis pour permettre un rayonnement de l'ULB dans ce domaine.

Enrichissement et création de nouveau axes de recherche au sein de OPERA - Wireless

L'approche prise aujourd'hui par les experts de la sécurité des systèmes communicants consiste principalement à développer des protocoles réseau robustes aux attaques malveillantes et des algorithmes de chiffrement pour assurer la confidentialité et l'intégrité des informations. Depuis plusieurs années, le groupe OPERA-WCG (Jean-Michel Dricot) collabore avec la Faculté des Sciences (Olivier Markowitch) en ce sens. Plusieurs projets de recherche ont été lancés dans le domaine de la sécurité de l'internet des objets, des systèmes critiques ou l'optimisation des réseaux pour la blockchain.

Plus récemment, de nouvelles approches ont aussi été proposées dans les couches plus basses des protocoles de communication. Prises individuellement, elles ne suffisent pas à assurer la sécurité et l'intégrité du système mais elles peuvent être combinées avec les approches classiques (cryptographiques) afin renforcer de manière significative la cybersécurité. Il a par exemple été montré que la réponse impulsionnelle du canal de propagation caractérisant la propagation des ondes à un endroit particulier était une donnée intéressante sur base de laquelle des clés de chiffrement uniques peuvent être dérivées. Il est aussi possible de s'intéresser au traitement du signal, grâce aux nouvelles formes d'ondes et au déploiement massif de la technologie multi-antennes envisagés pour les systèmes 5G. Ces derniers permettent de focaliser la puissance des signaux aux endroits (espace/temps/fréquence) où se trouvent les terminaux communicants afin d'empêcher l'interception des signaux par des tiers. Enfin, tous ces systèmes sont développés sur des plateformes électroniques qui, elles-mêmes, doivent être sécurisées avec soin.

L'objectif est donc de concevoir la cybersécurité des systèmes à travers toutes les couches de communications. Seule cette approche globale permettra de relever les défis posés dans le futur et nous pensons que, comme cette compétence n'existe pas aujourd'hui à l'ULB, une nouvelle activité de recherche doit être lancée dans ce domaine transverse de manière à renforcer l'expertise existante et à développer de nouvelles compétences.

Moyens de recherche disponibles

Au cours des années, le service OPERA WCG mis sur pied un laboratoire complet permettant le prototypage d'un système de télécommunications sans-fil. En 2017, un crédit FER a été utilisé pour la mise sur pied d'un labo de cybersécurité des réseaux. Le laboratoire dispose par ailleurs d'un ensemble de radios programmables (software defined radios) acquises à l'aide de différentes fonds et permettant de simuler la couche physique d'un réseau complexe de système de communication et de localisation.

La prochaine étape consiste à fusionner les deux composantes dans une plateforme de recherche commune (au sein de la future plateforme ICT au bâtiment E) afin de posséder une

chaîne complète de communication sécurisée permettant de simuler tout système télécom moderne.

Les moyens actuels sont donc importants et pertinents. Ils peuvent être immédiatement utilisés par le futur professeur qui sera engagé et il aura l'occasion de l'étendre au moyen de fonds adéquats (FER, Innoviris, FNRS,etc.).

Opportunités de recherche contractuelle

Les domaines de recherche liés à la cybersécurité et à la sécurité des systèmes communicants sont considérés comme stratégiques par les bailleurs de fonds. Les nombreux appels aux projets dans ce domaines indiquent que la personne engagée aura les outils et les moyens nécessaires au développement de ses activités :

- H2020, SU-ICT-01-2018 : Dynamic countering of cyber attacks
- H2020, SU-ICT-03-2018 : Cybersecurity Competence Network
- H2020, ICT-01-2019 : Computing technologies and engineering methods for cyber-physical systems of systems. *«supporting the creation of reliable, robust and energy-aware solutions for autonomous and safety-critical systems. The issues of energy efficiency, testability, trust and* ***cyber-security*** *should be considered, as well as the support of different levels of criticality on the same computing platform where needed».*
- H2020, SU-DS03-2019-2020 Digital Security and privacy for citizens and SME
- H2020, SU-DS04-2018-2020 Cybersecurity for Electrical power and energy system and armour against privacy attacks and data breaches
- H2020, SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems
- H2020, SU-ICT-03-2020: Advanced cybersecurity and digital privacy technologies

Et, au niveau régional

- Nombreux appels INNOVIRIS depuis 2015 tournant autour de la sécurité: BruFence, SCAUT, ORACLE, LEGO_BLOCKS, etc.. (> 3M€)
- Lancement en 2018 du centre BICI - *Brussels Initiative on Cybersecurity Innovation*

Articulation avec la recherche de la VUB

Le Prof. Jean-Michel Dricot collabore depuis de nombreuses années avec le groupe de recherche du Prof. Kris Steenhaut à la VUB sur les sujets liés à l'Internet de Objets (IoT) et les protocoles de réseaux informatiques. Ce groupe de la VUB a également des liens avec le Prof. An Braeken (Erasmushogeschool Brussel) qui a effectué sa thèse dans le domaine de la sécurité des protocoles et de l'électronique.

Il apparaît donc assez naturellement une excellente complémentarité et la possibilité d'un renforcement mutuel entre les équipes ULB, VUB et Erasmushogeschool. Ceci permettra d'atteindre une taille suffisante que pour placer l'ULB et la VUB comme leader de la recherche en cybersécurité en Belgique, en s'appuyant sur la nouvelle plateforme BICI (Brussels Initiative on Cybersecurity Innovation de INNOVIRIS).

Enrichissement des programmes d'enseignement et collaboration avec le Master en Cybersécurité

En 2015, l'Ecole Polytechnique (Jean-Michel Dricot) et la Faculté des Sciences (Olivier Markowitch) ont été à l'origine de la création d'un master inter-universitaire (ULB, UCL, UNamur, ERM, HE2B, HELB) qui rencontre un franc succès. Il compte à ce jour 90 étudiants et est en lien avec les entreprises et d'autres institutions académiques. Ce Master en accessible aux ingénieurs informaticiens et télécom soit en Master 120 ECTS, soit en Master complémentaire (60 ECTS). Le groupe OPERA-WCG y dispense les cours *Network Security* et *Mobile and Wireless Networks*.

Une chaire à vocation transverse de conception sécurisée de systèmes communicants viendrait renforcer la filière ELEC et le Master Cybersécurité en développant des thématiques transdisciplinaires et nécessaires pour les ingénieurs IT du futur. En pratique, il pourrait s'agir de proposer 2 cours spécifique de 4-5 ECTS à créer :

- Un premier cours introductif en MA1. Le départ à la retraite de Martin Timmerman, responsable du cours ELEC-Y-404 (Operating systems and security) donné aux étudiants MA1 ELEC sera l'occasion de réévaluer la pertinence de l'attribution des crédits aux différents cours.

- Un cours plus avancé en MA2, dans le cadre du projet intégré à l'option télécommunication qui compte actuellement 12 crédits. Ce cours serait alors à répartir entre les 4 académiques et couvrira le champ complet de l'expertise des télécoms en allant de la couche physique (propagation, codage) jusqu'aux protocoles réseaux en considérant systématiquement une conception sécurisée ("security by design") de ces différents éléments.

Une chaire à vocation transverse de conception sécurisée de systèmes communicants viendrait donc renforcer la filière ELEC et le Master Cybersécurité en permettant (à long terme) de proposer un expertise bien établie dans la capitale de l'Europe.

3. Profil recherché

Partant du constat de la nécessité de renforcer les recherches et les enseignements dans le domaine de la cybersécurité à l'ULB, la proposition suivante est formulée.

Ouverture d'une position en sécurité des systèmes communicants dont le candidat aura pour objectif d'insérer sa recherche dans les domaines présents au sein de OPERA - Wireless Communications Group, y compris la conception de protocoles de communication sécurisés (de la couche physique au réseau) et l'ingénierie de la sécurité.

Des connaissances dans le domaine de la sécurisation des systèmes de télécommunications, la réalisation d'attaques par canaux auxiliaires, la certification de systèmes sécurisés et l'intégration de techniques de machine learning dans le domaine de la sécurité seront considérés comme un plus et permettront d'offrir une ouverture sur de nouveaux champs de recherche pour le groupe.