Formation cybersécurité des systèmes industriels pour les ingénieurs non-informaticiens

Stéphane Mocanu

Formation cybersécurité des systèmes industriels pour les ingénieurs non-informaticiens

Stéphane Mocanu

Résumé : ***Nous présentons une nouvelle formation d'initiation des ingénieurs non-informaticiens à la cybersécurité des systèmes industriels. Le module est basé sur le MOOC « Cybersécurité » de l'ANSSI, les supports CyberEdu et un cycle de mini-projets de découverte pratique des concepts de la cybersécurité (interception du trafic, injection de données, détection des intrusions, filtrage du trafic). Les scénarios des mini-projets peuvent être exécutés à distance sur une plateforme matérielle.***

***Mots clé*— Cybersécurité des systèmes industriels, SCADA, supervision industrielle, automates programmables**

I. Introduction

L'objectif de cette communication est de présenter la démarche de sensibilisation des élèves ingénieurs non-informaticiens à la cybersécurité des systèmes industriels. La démarche est déployée dans l'ENSE3, école d'ingénieurs de Grenoble-INP.

II. Contexte local et analyse des besoins

L'Ecole Nationale Supérieure de l'Energie, Eau et Environnement (ENSE3) est l'une des six écoles d'ingénieurs de Grenoble-INP. De par ses filières de formation en automatique, smartgrids, énergétique, électrotechnique, hydraulique, nucléaire et mécanique, l'ENSE3 se situe à la pointe de la formation dans le domaine des systèmes industriels.

De par la nature des métiers formés par l'école, pratiquement tous les étudiants travailleront dans des *Secteurs d'Activité d'Importance Vitale*. Les employeurs des étudiants de l'école sont les acteurs et les constructeurs majeurs de ces secteurs. On peut donc raisonnablement supposer que la majorité des étudiants seront employés par de *Opérateurs d'Importance Vitale* ou leurs fournisseurs.

L'étude statistique des sujets de projets de fin d'études des deux dernières années, ainsi que les retours des partenaires industriels membres du conseil de l'école montrent un intérêt croissant des industriels pour une compétence cybersécurité de nos étudiants.

A. Difficultés

Le déploiement d'un nouveau programme dans des formations déjà en place est, évidemment, ardu. Au-delà de la difficulté évidente d'introduire un nouvel enseignement dans une maquette déjà complète dans les cas de l'ENSE3, il faut prendre en compte le caractère plutôt généraliste et la multidisciplinarité de l'école. L'ENSE3 est issue de la fusion en 2012 d'une école de génie mécanique et d'une école de génie électrique. Cette caractéristique « double culture » se retrouve encore dans le programme des filières métier de l'école. En particulier, par rapport à la thématique communication dans les systèmes industriels, les acquis des étudiants sont très hétérogènes. Si dans les filières électriques des prérequis sur les automates programmables et les SCADA existent (avec un maximum de compétences pour la filière Automatique) les filières de profil mécanique n'intègrent pas de notions sur les systèmes de contrôle/commande industriels. A une exception près (filière Automatique), aucune notion sur les réseaux de communication n'est enseignée.

B. Une formation à deux vitesses

Etant donnée l'hétérogénéité des parcours des étudiants, une formation transversale, unique, en cybersécurité n'est pas possible. Nous avons décidé de mettre en place deux formations avec deux niveaux de technicité totalement différents.

1) Sensibilisation aux enjeux et risques des technologies numériques.

Une première formation de sensibilisation aux risques cyber, sans prérequis, a été mise en place dans une Unité d'Enseignement (U.E.) optionnelle de 30h ouverte à tous les étudiants de 3ème année de l'école. Sans aucune ambition de transmettre des notions techniques sur la cybersécurité, l'objectif de l'enseignement est de montrer aux étudiants la place des technologies numériques dans leur métiers et les risques associées. Le programme de l'U.E. propose :

1) Une découverte expérimentale des technologies Internet et des SCADA
2) Un cycle de conférences industrielles sur les smart-secteurs industriels (smart-buildings, smart-energy, Industrie 4.0) et les risques cyber associées.
3) Une découverte pratique de l'analyse de données appliquée aux métiers de l'école (modélisation des systèmes physiques) et à l'analyse de trafic réseau.

Soumis le 12 janvier 2018

Stéphane Mocanu est enseignant ENSE3/Grenoble-INP et membre du Laboratoire d'Informatique de Grenoble Univ. Grenoble Alpes, CNRS, Grenoble INP*, Inria, LIG, F-38000 Grenoble France

L'intérêt pédagogique de cette double approche à l'analyse de données est de permettre aux étudiants de s'approprier rapidement de méthodes statistiques à l'aide d'une application qu'ils connaissent (modélisation d'un système physique) pour découvrir ensuite l'utilisation des mêmes méthodes pour la détection des intrusions.

L'U.E. a été lancée en septembre 2017. Nous avons fait intervenir deux constructeurs d'automatisme et SCADA (Schneider et Rockwell), un industriel du numérique (Thales), un opérateur réseau (Renater), un acteur de l'analyse de données et cybersécurité « ESI-group » et l'ANSSI. Après cette première expérience, nous avons observé que le fait de faire parler des industriels de l'automatisme sur les enjeux de la cybersécurité, facilitait le passage du message auprès des étudiants. Placé dans le contexte de l'application industrielle, le discours des acteurs du numérique et des autorités de la sécurité informatique est accepté. Néanmoins il nous reste à travailler le lien entre les différents discours ainsi que la communication auprès des étudiants. On vise un objectif d'environ 10% des étudiants de 3ème année inscrits dans la formation. Pour la première année nous avons à peine atteint 5% des étudiants.

2) Formation de base en cybersécurité industrielle.

Une deuxième formation, beaucoup plus technique, a été mise en place et démarrera au second semestre de l'année 2017/2018. Il s'agit de l'acquisition des bases de la cybersécurité des systèmes industriels par les étudiants de la filière Automatique de l'ENSE3 [1][2]. La formation est intégrée à une U.E. existante (Systèmes de Communication pour l'Automatique).

La partie Cybersécurité de la U.E. est structurée en trois volets :

1) Formation distante utilisant le MOOC SecNum Academie[1] de l'ANSSI. Sur le 5 ECTS de la U.E., 1 ECTS sera validé sur présentation des badges de validation des quatre modules du MOOC libre de l'ANSSI.
2) Cours en amphi. Une formation de 12h basée sur les supports de formation de la mallette CyberEDU validée par un examen écrit permettra aux étudiants de valider un autre ECTS.
3) Des mini-projets pratiques en distanciel sur des sujets de cybersécurité industrielle seront validés à hauteur de 0,25 ECTS

Les autres 2,75 ECTS seront validés par deux projets en présentiel : un projet d'étude et configuration d'un réseau local TCP/IP sous PacketTracer et un projet de développement d'un système de contrôle/commande/supervision d'un procédé réel : programmation des automates programmables, implémentation d'un protocole de communication industriel (Modbus/TCP) et réalisation d'un pont (TCP/IP/RS-232).

Nous présentons ensuite trois exemples de mini-projets cybersécurité des systèmes industriels.

III. ENSEIGNEMENTS PRATIQUES DISTANCIELS CYBERSECURITE DES SCADA

Les mini-projets SCADA peuvent être réalisés à distance sur la plateforme de cybersécurité et communication industrielle G-ICS.

A. La plateforme matérielle

G-ICS (GreEn-ER[2] Industrial Control systems Sandbox) [6] est une plateforme d'enseignement/recherche développée depuis 2014 grâce à plusieurs programmes de financement des plates-formes pédagogiques (financements FAIRE[3] de l'ENSE3 et Grenoble-INP, financement Labex Persyval plateformes de l'Université Joseph Fourier et financement Plateformes Learning-by-doing par l'IdEx Université Grenoble Alpes) ainsi qu'à des programmes de recherche (ANR et CIFRE). La plateforme réunit une centaine d'équipements de contrôle/commande/supervision industriels multi-protocole et multi-constructeur qui peuvent être couplés de manière flexible avec un système de simulation matérielle (hardware-in-the-loop). La simulation logicielle des procédés peut être réalisée avec des simulateurs commerciaux (Matlab/Simulink, Dymola) ou libre (Scilab ou Modelica) ainsi qu'avec des environnements de virtualisation (Factory I/O ou Home I/O). On peut ainsi réaliser des architectures de système couvrant des domaines industriels allant de domotique et distribution électrique de bâtiment jusqu'à l'industrie manufacturière et smartgrids[3]. L'image suivante donné une idée du matériel disponible su r la plateforme.

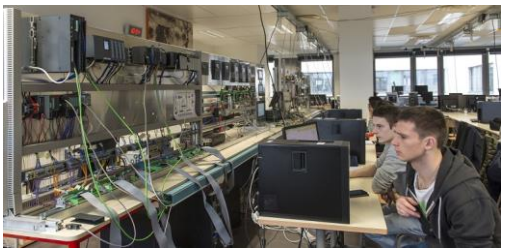

Fig 1. Vue partielle de la plateform G-ICS

La plateforme est accessible à distance par VPN.

B. Les mini-projets cybersécurité SCADA

Nous présentons par la suite trois exemples de mini-projets cybersécurité exploitant le matériel de la plateforme G-ICS. Dans les trois cas les étudiants doivent réaliser l'architecture en présentiel, ensuite exécuter les scenarios d'attaque/détection à distance.

1) Projet recherche de vulnérabilités : interception des mots de passe des communications non-sécurisées.

En utilisant l'architecture simple indiquée en Fig. 2, le mini projet consiste à récupérer le mot de passe root d'un relais de

[1] https://secnumacademie.gouv.fr/

[2] GreEn-ER : Grenoble énergie - enseignement et recherche, pôle d'innovation porté par le PRES Université de Grenoble

[3] FAIRE: Fond d'Aide à l'Investissement en Recherche et Enseignement

protection de réseau de distribution électrique par observation de trafic. Le chargement du programme sur le relais de protection utilise le transfert FTP classique. Une simple observation de trafic permet de récupérer en clair le login root et le mot de passe. Les identifiants sont utilisés ensuite pour récupérer le programme du relais de protection.

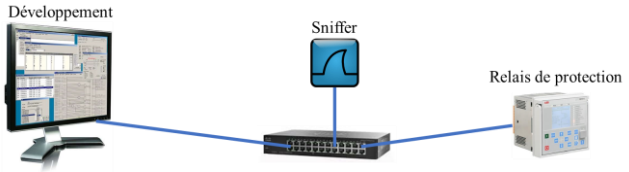

Fig 2. Architecture du mini-projet interception des mots de passe.

2) IDS industriel.

Une architecture incluant un IDS commercial (CyberVision de Sentryo) est utilisée afin d'illustrer l'utilisation des détecteurs d'intrusions [3]. Un agent Metasploit [5] attaque un automate par des écritures des variables de mémoire. Les flux illicites sont détectés et alertés par la sonde Sentryo.

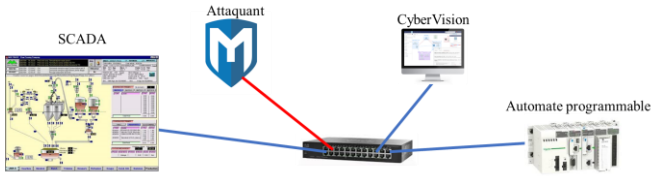

Fig 3. Architecture incluant une sonde IDS CyberVision.

3) IPS industriel.

On illustre le filtrage du trafic industriel en utilisant un IPS orienté systèmes industriels (SNi40 de Stromshield). L'architecture utilisée est celle de la Figure 4. L'attaquant Metasploit lance une requête d'arrêt de l'automate sur les deux automates programmables. L'attaque va aboutir sur l'automate non-protégé mais sera bloquée par l'IPS sur le second automate.

Fig 3. Architecture incluant un IPS SNi40

D'autres thèmes de mini-projets sont en cours de réalisation. Nous souhaitons illustrer les vulnérabilités dues aux sites web embarqués sur les automates (souvent non-sécurisés), les dénis de services (suite à des tempêtes Ethernet par exemple ou au clonage des adresses IP) ou encore les manipulations des donnés de supervision par injection des données.

IV. Conclusions et perspectives

Nous avons présenté une nouvelle formation de cybersécurité des systèmes industriels proposée à un public non-informaticien. Nous souhaitons essaimer l'initiative au niveau d'autres formations d'ingénieurs notamment au niveau des projets pratiques. Une perspective intéressante serait l'interconnexion de plusieurs plateformes SCADA situées sur de sites distants et la réalisation des expériences multisites.

References

[1] ANSSI, La cybersécurité des systèmes industriels, 2014
[2] ANSSI, Guide pour une formation sur la cybersécurité des systèmes industriels, 2015
[3] CEI 62443 Cyber-sécurité des installations industrielles.
[4] CEI 61850 Communication networks and systems in substations
[5] Kennedy, D., Metasploit: The Penetration Tester's Guide, No Starch Press, 2011
[6] Mocanu S.. Une plate-forme de cybersécurité et interopérabilité des systèmes industriels : le projet G-ICS. Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2015), May 2015, Troyes, France. 〈hal-01291757〉