Couverture

Resume

Abstract

Sommaire

Contexte du stage :

Présentation de l’entreprise

Histoire

La SAS (Société par Actions Simplifiées) Kereval est une PME fondée en juillet 2002 et dirigée à ce jour par M. Abdelmoula TAMOUDI. Kereval est la combinaison de « KER » et « EVAL », respectivement « maison » en langue bretonne et le début du mot « évaluation » pour l’activité du test. Ce nom traduit les spécialisations et services de l’entreprise que sont l’ingénierie de tests et la qualité logicielle. Kereval est également un centre de validation et de certification dans les domaines représentés dans l’entreprise. L’entreprise effectue à présent un chiffre d’affaires de 5 millions d’euros annuel et a su répondre aux attentes de plus de 190 clients parmi lesquels se retrouvent des domaines très variés : la Société Générale ou le Crédit Agricole dans le domaine de la banque et des assurances, la DGA ou NavalGroup dans le domaine de la défense, Orange ou Bouygues dans le domaine du multimédia, le CNED ou le Ministère de l’Education Nationale dans le domaine public ainsi que de nombreux autres groupes industriels ou tertiaires.

Organigramme & chiffres clés

(IMAGE ORGANIGRAMME.)

(IMAGE CAMEMBERT SECTEUR.)

Secteurs d’activité & Missions

L’activité de Kereval s’oriente principalement autour de 4 axes distincts encadrés par les laboratoires présents en son sein. Chaque axe propose des services tels que l’audit, la certification, le conseil ou la formation. Chaque laboratoire possède une base de clients et de partenaires.

* Santé-IHE :

L’objectif du laboratoire Santé-IHE est la mise en place de tests et d’une plateforme de certification des mutuelles et professionnels de santé. En proposant du conseil et un dispositif d’industrialisation, le but du laboratoire est d’encadrer une mise en place de services de santé. Cet encadrement passe aussi par des formations sur les outils de tests ou le test logiciel. Enfin, les campagnes de tests proposées permettent de tester la gestion du patient, le dossier médical, le dossier de soins, etc. Cette campagne est épaulée par le laboratoire de certification HEALTHLAB IHE, accrédité par le COFRAC (REF COFRAC) et qui permet l’évaluation de la conformité et de l’interopérabilité des logiciels de santé par rapport au standard IHE (REF IHE).

* Cybersécurité : Objectifs, Services et Accréditations. Ex. Clients et Certifications

Les objectifs principaux du laboratoire de Cybersécurité sont les activités de conseil, d’audit et de formation. Les activités d’audit se retrouvent dans des audits de configuration (vérification de mise en place de bonnes pratiques), d’architecture (configuration d’équipements réseaux) et d’organisation (état des lieux de la maturité de la sécurité du système étudié). La phase d’audit donne lieu à une phase de mise en place de tests d’intrusions sur les systèmes d’information, WEB, mobile ou embarqués. Ces tests utilisent un panel d’outils et d’attaques référencés. Des tests d’intrusions résultent une classification et des anomalies et un ensemble de conseils ou pratiques permettant leur correction. Les activités de tests d’intrusion, d’audit de configuration et d’audit d’architecture sont certifiées par l’ANSSI (REF ANSSI) comme PASSI (Prestataires d’Audit et de Sécurité des Systèmes d’Information).

* ISOBUS : Objectifs, Services et Accréditations. Ex. Clients et Certifications

Le laboratoire ISOBUS fait partie des laboratoires de tests de systèmes embarqués de Kereval. En plus de la formation et du conseil sur les normes de certifications ISOBUS définies par l’AEF (REF ANSSI), le laboratoire fait partie des quatre laboratoires mondiaux permettant de décerner cette certification. Il permet en amont d’effectuer les différents tests de conformité à la norme, tests de charge ou tests d’interopérabilité. Un outil de certification a été développé au sein de l’entreprise et permet maintenant de certifier le matériel agricole et le rendre ainsi reconnaissable sur le marché.

* CAN/LIN/SENT : Objectifs, Services et Accréditations. Ex. Clients et Certifications

Les bus CAN et LIN sont des bus systèmes utilisés notamment dans les domaines de l’automobile. Kereval propose un ensemble de formation, conseil et méthodes d’industrialisation lors de la mise en place de tels bus. C’est aussi un centre de validation de tels bus qui permet, à l’aide d’une équipe de tests certifiées CFTL ISTQB (REF ANSSI) de produire un rapport des défauts et axes d’amélioration possibles du produit.

C’est donc autour de ces quatre axes principaux qu’évolue Kereval dans la prestation de services. Cependant, afin de garantir la satisfaction des clients ainsi qu’une conformité à l’état de l’art des technologies actuelles, l’entreprise se doit de maintenir son excellence technique, tant pour sa crédibilité que pour la conservation de ses accréditations.

Cette recherche d’excellence technique amène un intérêt naturel pour le milieu de la recherche et la création de thèses CIFRE en partenariat avec différents laboratoires de recherche (Rennes 1 ou INRIA) mais aussi de sujet de stage résultant sur l’état de l’art d’un projet ou d’un type d’attaque afin de résulter sur un rapport de l’existant, l’élaboration de *proofs of concept*, ou le développement d’un outil complet.

Mon activité

Intitulé du stage et définitions

Le stage tel que donné par Kereval s’intitule « Attaque par Injection de Fausses Données sur des Estimateurs d’Etat : Cas du filtre de Kalman ». Cet intitulé implique plusieurs prérequis ; tout d’abord la mise en place d’un système utilisant un estimateur d’état (tel que Kalman ou un dérivé) et la possibilité dans ce même système d’effectuer une *FDIA* (*False Data Injection Attack* ou Attaque par Injection de Fausses Données). Une *FDIA* correspond à une prise de contrôle d’un des capteurs ou entrées du système par un attaquant et d’une modification de la part de ce dernier de la mesure produite par le capteur compromis dans le but d’influencer le système entier via l’estimateur.

Intégration à l’entreprise

Le sujet du stage s’intègre dans la partie recherche et développement du bureau de cyber sécurité et c’est donc à ce bureau, et donc à l’équipe sécurité, que j’ai pu être intégré. Le projet du stage ne possède pas de bases présentes ni de limitations au moment de mon attribution. La tâche m’est confiée moyennant un retour hebdomadaire auprès de mon tuteur de stage. Le reste du bureau continue son activité principale d’audit

Problématisation

*Quels sont les utilisations des estimateurs d’état ?*

Les principales utilisations d’estimateurs d’état se retrouvent dans les domaines des capteurs ou utilisateurs de capteurs tels que la robotique mobile, les véhicules autonomes, le contrôle aérien ou la gestion de réseaux électriques. Les estimateurs d’états permettent, à l’aide d’un algorithme donné propre à chaque estimateur de prévoir l’état suivant du système connaissant son état précédent, le résultat de la mesure des capteurs ainsi que la prise en compte d’éventuelles entrées du système. L’état d’un système, ou plus précisément la variable d’état qui définit un système, correspond à l’ensemble des variables qui modélisent ce système. Cette variable d’état est choisie par le créateur de l’estimateur et/ou du système. La sélection des variables présentes ou non dans la variable d’état influence l’estimation et la précision de l’estimateur du système et dépend avant tout du choix du modèle de précision que l’ingénieur effectue.

*Pourquoi et comment attaquer des systèmes qui utilisent ces estimateurs ?*

L’attaque d’estimateurs d’état permet à l’attaquant différents niveaux d’impact allant d’une perte de précision de l’estimateur jusqu’au contrôle de celui-ci. Attaquer de tels systèmes permettrait même un gain économique à l’attaquant dans le cas des réseaux électriques (REF MO POWERGRID). L’attaque d‘estimateurs d’état passe dans notre cas par la supposition que l’attaquant contrôle un des capteurs du système et donc a une influence sur la mesure que l’estimateur va percevoir. Un estimateur d’état fonctionne avec un cycle de :

Prédiction suivant un modèle donné

Acceptation de la mesure

Correction et détermination du nouvel état entre état prédit et mesure

Une *FDIA* consiste donc à attaquer au niveau de l’introduction de la mesure dans le système et ressemble à des attaques de type *spoofing* ayant déjà eu lieu en conditions réelles grâce à l’imitation de signaux Wifi (prise de contrôle de drones (REF SPOOF)) ou GPS (dérive de bateaux ou robots mobiles (REF GPS SPOOF)). Dans le cas d’estimateurs d’état, la présence d’une comparaison entre un modèle et la mesure rajoute une complexité supplémentaire. Une mesure trop « grossière » ne sera pas prise en compte par l’estimateur. Il s’agit donc pour l’attaquant de doser son attaque entre efficacité et détectabilité : l’attaque la plus efficace sera aussi celle amenant les mesures les plus facilement détectables comme erronées par l’estimateur.

*Quels sont les objectifs du stage ?*

Les objectifs tels que donnés par Kereval sont de :

Effectuer un état de l’art des estimateurs existants.

Effectuer un état de l’art des types d’attaques sur ces estimateurs.

Etudier particulièrement le cas du filtre de Kalman.

Etudier particulièrement le cas des *FDIA.*

Proposer un ou plusieurs petits systèmes de *proof of concept.*

Proposer ces systèmes dans un langage tel que Python ou Java.

Les objectifs du stage traduisent donc deux composantes importantes : un aspect recherche très important et un besoin d’autonomie à travers la mise en place de *proof of concept* et la conception du projet, partant de zéro.

Etat de l’art et Objectifs (scénario de base)

* Présentation du filtre de Kalman et de ses applications (2/3p.)

Histoire

Etapes/Cycle

Equations

EKF

IMM

* Présentation du système d’ATC (2/3p.)

Fusion de données en provenance de différentes sources (plusieurs radars + ADSB) (REF ARTAS ICAO)

Scénario

* Modélisation Radar/Avion (2/3p.)

Simulateur de manœuvres, système commandé, transformation des coordonnées, bruitage

* Modélisation (IMM et modèles considérés) (2/3p.)

CA CV CT TA (REF MODELISATION ½ AVION ½ RADAR)

* Attaques par injection de fausses données (2/3p.)

Attaques dans la recherche

Détecteurs d’anomalies implémentés

Attaques implémentées

Projet : Structure (1p.)

Présentation des différents modules et de leurs liens (1/2p. / module)

Implémentation & Résultats

Banc d’essai (1p.)

GUI (1p.)

Conclusion (1p.)

Réalisation

Enjeux

Projet professionnel