Développement d'un simulateur cyber-physique d'une plateforme de localisation en intérieur sécurisée pour analyse de vulnérabilités et évaluation de contremesures

Position: Stage (niveau Master)
Laboratoire: Univ. Grenoble-Alpes, Grenoble INP LCIS *(Valence, France)*
Équipe: CTSYS *(*sûreté et sécurité des systèmes embarqués et pervasifs*)*

Mots-clefs: Systèmes cyber-physiques, localisation en intérieur, IoT, cybersécurité, contremesures niveau système

La localisation en intérieur est un domaine de l'IoT en pleine expansion, que l'on retrouve dans de nombreuses applications telles que la navigation de robots, la supervision en milieu industriel ou le contrôle d'accès basé sur la position. En dépit d'être employée dans des environnements critiques tels que des hôpitaux ou des usines, la majorité des systèmes de localisation en intérieur sur étagère ne disposent d'aucun mécanisme de sécurité, et négligent souvent les primitives de cryptographie basiques. Plusieurs technologies de communication peuvent être utilisées à des fins de localisation, cependant l'UWB (Ultra-large bande) est actuellement la plus performante, affichant une précision de 10 cm et une fréquence de localisation allant jusque 1000 Hz.
En conséquent, une plateforme de localisation en intérieur sécurisée UWB a été développée au sein du laboratoire. Cette plateforme est ouverte à toutes les couches, permettant d'expérimenter des attaques et d'évaluer des contremesures. Les positions des tags sont calculées et affichées en temps réel par un moteur 3D, et toutes les positions ainsi que les jeux de données sont logués de sortes à pouvoir être rejoués avec des paramètres différents.
Cependant, certains scénarii doivent être évalués à plus grande échelles, ou sont parfois compliqués à mettre en place sur notre plateforme. Un simulateur cyber-physique permettrait de s'affranchir de ces limitations et d'ouvrir la plateforme à un plus large spectre de scenarii. Ceux-ci utiliseront donc à la fois des données réelles et simulées, en simulant par exemple un nœud malicieux au sein d'un scénario enregistré dans des conditions réelles. Le stagiaire implémentera donc des mécanismes de simulation cyber-physique au sein du moteur 3D actuel (codé en Python), en intégrant les fonctionnalités suivantes :

- Ajout de tags fictifs au sein d'un scénario enregistré en conditions réelles
- Émulation de comportement malicieux
- Génération de comportement aléatoire sur large échelle
- Détection des violations de sécurité
- Implémentation de contremesures niveau système dans l'environnement simulé.

Le candidat doit suivre une formation de niveau master en informatique, développement, systèmes embarqués ou équivalents.

Compétences requises : Python, C++, génie logiciel. Des connaissances en systèmes embarqués et en cybersécurité seront appréciées.
Gratification/Avantages : 530€/mois, tarif réduit sur les repas de midi
Contact: baptiste.pestourie@lcis.grenoble-inp.fr