Commenté [1]: <!--StartFragment-->

Sujet de thèse

Chaire cyber défense navale

Résumé du projet (4 000 car. Maximum)

L'ingénierie de la sécurité s'intéresse à définir des méthodes de conception de solutions de sécurisation d'un système face à des risques, et à permettre de démontrer que le niveau de sécurité (protection, détection, réaction) est satisfaisant. Ceci nécessite l'introduction d'un point de vue et amène les questions suivantes à prendre en compte dans l'ingénierie des modèles :

Question ouverte de la définition des ressources et des processus critiques dans les méthodes d'analyses des risques. Sur l'intégration de ces ressources et processus permettant l'accomplissement d'une ou plusieurs fonctions contributive(s) à une mission, en tenant compte de la survivabilité (au sens continuation totale ou partielle de la fonction) et de la résilience. Faut-il intégrer directement dans le modèle la démarche analytique de définition des biens à protéger, et des conséquences d'attaque selon l'échelle classique DICT (Disponibilité, Intégrité, Confidentialité et Traçabilité) ?

Les biens et les processus à sécuriser étant identifiés, leur criticité est alors structurante pour la modélisation. Ceci amène des contraintes techniques, réglementaires et légales très significatives. En France, les données peuvent être publiques, privées, sensibles ou classifiées. Elles peuvent se voir affectées d'une mention de manipulation en restreignant l'accès à des communautés limitées : c.-à-d. « Spécial — France ». Il existe des classifications similaires dans l'OTAN, et dans la plupart des pays. Des règles de sécurisation telles que le cloisonnement des systèmes en découlent, ainsi que les risques associés comme les risques de « contamination » des canaux d'échanges d'informations sensibles. Ce point de vue est donc structurant pour la conception d'un système. Il peut aussi amener à rejeter d'emblée des évolutions techniques non éprouvées qui amèneraient à contourner ce cloisonnement.

Des capacités de sécurité doivent être intégrées dans le système modélisé pour la gestion opérationnelle de la sécurité : détection, réaction, surveillance. La spécificité du système naval intervient à travers son environnement opérationnel et la chaîne de décision.

Enfin, l'ingénierie de sécurité amène à envisager des scénarios d'attaques, et à démontrer que les mesures de sécurité techniques et organisationnelles retenues permettent d'assurer la sécurité et la protection du système en rendant ces attaques inopérantes ou d'en limiter les effets. Dans le cadre d'un système complexe de défense, la durée de vie du système le confronte à supporter de nouvelles attaques, et les améliorations technologiques permettent de mettre en œuvre des attaques auparavant

complexes ou demandant des moyens financiers importants (cassage de mots de passe par cloud, banalisation d'outil comme le clonage de badge d'accès, etc.). L'ingénierie doit donc pouvoir intégrer de futures attaques, celles auxquelles le système devra faire face en temps opérationnel et non en temps de conception. Une démarche heuristique s'appuyant sur une expertise métier pourrait être utilisée sur un système simple. Intégrer les scénarios d'agression dans le modèle permettrait de mieux identifier les effets, et l'enchaînement possible des attaques sur un système complexe :

L'agresseur menant une action volontaire, la réduction probabiliste liée au faible risque de pannes multiples n'est pas pertinente. Au contraire, une combinaison de vulnérabilités (techniques et non techniques) indépendantes et successives favorise des scénarios d'attaques ;

L'analyse des défaillances évolue dans le temps, en fonction des évolutions des menaces et de la révision des risques, les scénarios d'attaque évoluent alors également, au fur et à mesure de la découverte de vulnérabilités ou de techniques nouvelles d'attaque ;

Qu'est-ce qu'un attaquant dans le cas d'un système complexe de défense de type naval, et comment intégrer ces profils d'attaques' dans la modélisation d'un système ?

Hypothèses, questions posées, identification des points de blocage

La modélisation de propriétés de sécurité dans des systèmes complexes navals n'a pas été explorée pour l'instant. Notre hypothèse est que ce genre de propriétés permettrait de faire émerger des capacités de cyber résilience des systèmes par conception. Les verrous scientifiques concernent l'expression de ces propriétés de cyber résilience ainsi que la modélisation de systèmes industriels à plusieurs niveaux de granularité afin de prendre compte à la fois des aspects techniques et des aspects opérationnels. Le comportement de ces propriétés en fonction des cas d'utilisation et de l'évolution des systèmes sera un point important du projet.

La phase expérimentale et le recueil des données seront un point sensible de cette recherche.

Approches méthodologique et technique envisagées

L'objectif de la thèse est :

– analyser comment intégrer le point de vue d'analyse de risques dans un modèle de conception système et complexe de type naval ;

– exprimer et de modéliser les contraintes (tel que le confinement ou la ségrégation), les propriétés en lien avec la sécurité (communication avec un pair de même niveau, accès à un réseau non protégé, ou un service non fiable, etc.) et les moyens de validation associés (pour vérifier que le système réalisé les respecte) ;

– modéliser formellement des processus d'attaques au sein du modèle, mettant en évidence la capacité de surveillance, de détection, de résilience et de protection du système ;

– définir le bon niveau d'ajustement du niveau de sécurité des modèles ;

– proposer un exemple représentatif sur un cas concret non sensible de fonctions ou de sous-fonctions critiques d'un équipement embarqué.

– développer un prototype illustrant les différentes contributions en lien avec cette thèse.

Contexte scientifique et partenarial : éléments généraux

Ce travail de recherche se fera au sein de la chaire de cyberdéfense des systèmes navals, située à l'école navale à Lanveoc (proximité de Brest). L'encadrement sera fait par des enseignants chercheurs de IMT Atlantique et de l'école navale avec le soutien d'une équipe de THALES.

Contacts :

Yvon Kermarrec (Yvon.kermarrec@telecom-bretagne.eu) et David Brosset (david.brosset@ecole-navale.fr)

Commenté [2]: <!--EndFragment-->