Conception d'un langage de coordination de processus visant à maitriser la sécurité des systèmes navals par la maîtrise de leurs processus de production

Chaire de cyberdéfense des systèmes navals*
École Navale – IMT Atlantique – Naval Group – Thales

Encadrement
Direction : Antoine Beugnard ou Fabien Dagnat
Encadrement : Jean-Christophe Bach

Cadre
Cette thèse se fera en coopération avec le Centre Support Cyberdéfense de la Marine nationale à Brest, Thalès, l'École Navale et l'IMT Atlantique (ex Télécom Bretagne). Elle sera réalisée à Brest à la fois dans les locaux de la chaire à l'École Navale et au département informatique de l'IMTA, au sein de l'équipe PASS.
Contraintes de sécurité : Le(la) doctorant(e) sera amené(e) à manipuler des données potentiellement sensibles, **il(elle) devra pouvoir être habilité(e).**

Résumé

Les logiciels sont présents partout et s'ils contribuent à l'amélioration et au bon fonctionnement des systèmes technologiques, ils sont aussi sources d'erreurs et de vulnérabilités. Les coûts engendrés par la découverte de failles de sécurité dans un système logiciel en production sont tels qu'il est préférable d'agir le plus en amont possible afin d'éliminer un maximum de risques dès la conception et le développement (*security by design*), tout en conservant des moyens d'agir dans la phase de maintenance. Dans le cas des systèmes logiciels critiques ou sensibles tels que les systèmes navals, le processus de développement est soumis à des contraintes fortes de sécurité et de qualité. La maîtrise de la sécurité d'un logiciel passe donc par la maîtrise de son processus de production ainsi que par la maîtrise de la sécurité de son processus de production. L'objectif de la thèse est de poser les bases méthodologiques et techniques d'une telle coordination entre les processus de sécurité et de développement dans un contexte de systèmes logiciels critiques afin de garantir une meilleure sécurité du produit final par une meilleure maîtrise de la chaîne de production.

Problématique

Les systèmes navals sont sensibles et comportent de nombreux composants logiciels qu'il faut concevoir, implémenter et maintenir durant tout le cycle de vie du navire (de 40 à 50 ans !). Le processus de sécurité a une importance primordiale dans le développement de systèmes logiciels critiques et sensibles tels que ceux embarqués sur les navires de la marine. Il est exécuté en parallèle du processus de développement, tout au long du cycle de vie du logiciel. Les décisions prises dans le cadre du processus de sécurité affectent la structure du processus de développement, tandis que les pratiques et choix opérés durant le développement peuvent aussi avoir des conséquences sur le processus de sécurité.

Les techniques actuelles de modélisation de processus ne se concentrent pas sur la coordination des différents processus, tandis que les techniques manuelles pour la synchronisation de l'exécution de processus en parallèle conduisent à des failles de sécurité. Nous proposons d'utiliser la fédération de modèles pour coordonner les processus de sécurité et ceux de développement dans le contexte

*http://www.chaire-cyber-navale.fr/

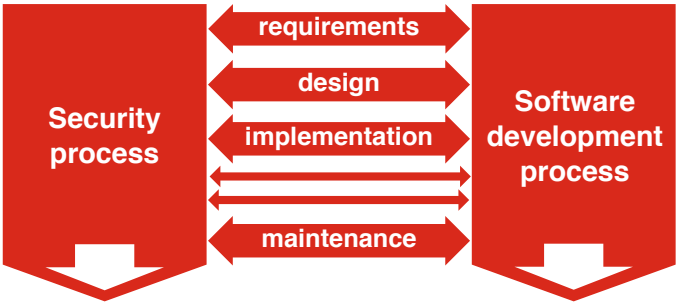

FIGURE 1 – Interdépendance entre les processus de sécurité et de développement

des systèmes critiques. L'objectif est de garantir la sécurité du produit final, en garantissant qu'il n'est pas compromis au cours de la production du logiciel à cause de failles dans le processus de développement.

Ces dernières années, les études de failles de sécurité ont montré qu'une attention plus poussée des processus de développement aurait permis de détecter les vulnérabilités ou de les éviter. Cela suggère que que la sécurisation du processus de développement d'un produit est un élément-clé de la sécurité d'un produit ; et que l'on devrait donc donner autant d'attention au processus de développement qu'au produit lui-même.

Ce type d'événement arrive souvent lorsque les processus de sécurité et de développement de systèmes ne sont pas alignés. Ces processus impliquent du personnel différent, avec des métiers différents, des objectifs différents et parfois même opposés. Cependant, ils partagent l'objectif global commun de développer un système sécurisé donné. Aujourd'hui, à notre connaissance, il n'y a pas de méthode ni d'outil pour synchroniser ces deux types de processus. Nous proposons donc de travailler sur la cohérence entre ces deux processus ainsi que sur leur évaluation dans un cadre formel.

Lors de développement de systèmes critiques complexes, la sécurité est une préoccupation majeure. Par conséquent, un processus dédié à la sécurité est mis en place en parallèle du processus de développement du système. Le personnel intervenant dans le processus de développement de systèmes critiques sont généralement habitués à gérer les aspects liés à la sûreté. En revanche il est plus difficile d'intégrer les contraintes de sécurité provenant d'un processus externe. Pour résoudre ce problème, il est nécessaire de mettre en place des méthodes pour aligner les processus et permettre aux différents intervenants de travailler ensemble. Toute modification de la politique de sécurité a un impact sur le processus de développement qui lui-même influence le processus de sécurité. Cette dépendance entre les processus commence dès la phase d'ingénierie des exigences et continue tout au long du cycle de développement du système, comme illustré par la Figure 1. Dans le contexte particulier des systèmes navals, le cycle de vie du produit est particulièrement long alors que sa criticité est très élevée.

Des travaux ont été menés d'une part sur la sécurité des produits, d'autre part sur la sécurité des processus Cependant, les travaux existant reliant les processus de développement et de sécurité reposent sur des ontologies ou des *patterns*. Nous proposons de travailler sur une solution basée sur l'ingénierie dirigée par les modèles grâce aux compétences de notre équipe autour de la fédération de modèles, du développement de langages dédiés et de la modélisation de processus.

Dans le cadre de cette thèse, nous visons les objectifs suivants :

— étude empirique des processus de conception de systèmes logiciels dans le cadre des systèmes navals
— définition des bases d'un langage pour la synchronisation des processus de sécurité et de développement, ainsi que leur vérification ;
— conception et fédération des modèles de sécurité et de développement pour la synchronisation des activités et des informations.

L'intérêt scientifique serait de fournir une méthode qui renforce la sécurité du produit en même temps que son processus de développement. À terme, nous pourrons valoriser d'autres projets de

recherche en sécurité en intégrant leurs approches dans notre processus générique.

Axes envisagés
Les travaux pourront s'articuler autour de 3 axes :

- **analyse des processus de conception :** une étude empirique des processus de conception de systèmes navals, du point de vue fonctionnel et sécurité, devra être réalisée afin de fournir la matière à l'axe suivant.
- **conception d'un langage de synchronisation de processus :** Il s'agira de concevoir un langage permettant de décrire formellement les processus. Il faudra munir ce langage d'une sémantique afin de pouvoir effectuer des vérifications formelles.
- **implémentation d'un prototype :** Afin de valider le langage et l'approche, il faudra implémenter un prototype. Une piste consisterait à utiliser le *framework* de fédération de modèles Openflexo pour réaliser ce prototype.

Ces axes ne seront probablement pas traités de manière strictement séquentielle, une approche incrémentale devra probablement être adoptée pour aborder les différents axes. De plus, il faudra aussi prendre en compte les contraintes industrielles liées au domaine et aux partenaires. Cela se traduira probablement par des compromis lors des choix de réalisation en fonction des coûts, des performances attendues et des risques.

Compétences attendues
Le candidat devra avoir des compétences (ou être capable de les acquérir rapidement) dans les domaines suivants :

- développement logiciel
- modélisation
- conception de langages

Des compétences dans un ou plusieurs des domaines suivants seront appréciées :

- modélisation de processus
- modélisation de programmes
- vérification formelle
- sécurité des systèmes informatiques

Comme pour toute thèse, le candidat devra être attiré par la recherche, et faire preuve de curiosité et d'autonomie.

Contact informations et candidature : pass-recrutement@imt-atlantique.fr.