

CAIRN-SéCuriser des Architectures logicielles avec des patRoNs de sécurité

Responsable : Isabelle BORNE

Encadrants : Jérémy BUISSON, Vanea CHIPRIANOV

Équipe : ARCHWARE, IRISA

Contexte scientifique

La sécurité des systèmes informatiques est devenue de plus en plus critique pour les entreprises, les banques, mais également pour les systèmes d'infrastructure critiques, tels que les réseaux électriques et de transport (intelligents). La sécurité doit être considérée dans toutes les étapes du cycle de vie d'un système informatique. Nous allons nous concentrer sur l'étape de conception de l'architecture logicielle.

De nombreuses propositions d'aide à la conception d'une architecture logicielle ont été faites. Parmi ces approches, nous nous intéresserons à celles utilisant des patrons de conception, qui ont pour objectif de proposer des solutions à des problèmes récurrents de conception. Plus spécifiquement, pour ce projet, nous nous concentrerons sur des patrons de sécurité qui décrivent des solutions de sécurité et des mécanismes de défense (vs. par exemple des mécanismes d'attaque) d'un système informatique au niveau logiciel.

Pour permettre aux architectes logiciels d'intégrer le plus automatiquement possible des patrons de sécurité dans leurs architectures, ces patrons doivent être décrits dans un format lisible à la fois par l'humain et traitable par l'ordinateur.

Objectifs du projet

Le principal objectif du projet est de sécuriser des architectures déjà définies ou en cours de définition.

Pour cela nous commencerons par étudier les catalogues existants de patrons de sécurité afin d'extraire un ensemble pertinent pour les architectures logicielles. Certains patrons mériteront peut-être d'être adaptés pour la sécurisation des architectures logicielles. Un premier objectif sera donc d'obtenir un ensemble de patrons de sécurité.

Un deuxième objectif est d'obtenir une modélisation de ces patrons, qui est indispensable si on veut les manipuler, dans un langage de modélisation qui aura été choisi au préalable.

Le processus à mettre en œuvre pour appliquer un patron de sécurité à une architecture constitue le troisième objectif. Il s'agit de développer des outils et de la documentation pour outiller le processus et le rendre utilisable.

Enfin, afin d'illustrer et d'expérimenter notre processus nous devons choisir un cas d'étude. Il pourra s'agir, par exemple, de la modélisation et de la sécurisation de l'architecture d'une *Smart City*.

Méthodes et outils

Pour répondre aux différents objectifs le projet sera divisé en étapes.

Il démarrera par la sélection d'un ensemble de patrons de sécurité. Ces patrons seront à choisir parmi des catalogues, par exemple [Fernandez, 2013] et devront répondre à ces problèmes de sécurité dans les architectures logicielles.

Le projet se poursuivra par une étude des langages de modélisation pour les patrons qui seront recensés dans des travaux existants. Ensuite le langage choisi permettra de modéliser des patrons de conception de sécurité. Il s'agit d'une partie délicate et importante du projet. En parallèle il faudra choisir un cas d'étude dont l'architecture devra être modélisée avec des langages comme UML/SysML.

Dans un troisième temps, le développement du processus outillé sera entamé. On commencera par étudier des mécanismes utilisant ces patrons de conception de sécurité. Nous regarderons, en particulier, comment remplacer une portion d'un modèle d'architecture par un (élément de) patron de conception à partir des approches existantes d'intégration automatique des design patterns, telles que [Castellanos, 2013], qui formalise les patrons de conception comme des transformations de modèles avec des pré- et des post-conditions. Une documentation accompagnera les différents mécanismes mis en œuvre.

Ce projet s'appuie sur des connaissances fondamentales sur les architectures logicielles, le concept de patron de conception, et des langages de modélisation tels que UML. Pour les parties d'implémentation, une bonne connaissance d'un langage de programmation à objets, tel que Java, sera nécessaire. Les modèles issus d'UML seront probablement décrits dans un format XMI.

Résultats attendus

Les résultats attendus pour ce projet sont

- Une bibliothèque exploitable de patrons de sécurité pour les architectures.
- Un processus outillé et documenté pour l'intégration des patrons dans les architectures.
- Un rapport d'expérimentation avec le cas d'étude choisi.

Références

[Fernandez, 2013] Fernandez-Buglioni, *Security Patterns in Practice: Designing Secure Architectures using Software Patterns*, 2013.

[Castellanos, 2013] Cuauhtemoc Castellanos, Thomas Vergnaud, Etienne Borde, Thomas Derive, and Laurent Pautet. 2013. Formalization of design patterns for security and dependability. In *Proceedings of the 4th international ACM Sigsoft symposium on Architecting critical systems (ISARCS '13)*. ACM, New York, NY, USA, 17-26.

Bibliographie

Des références supplémentaires seront fournies.