Evolution continue et sécurisée des artefacts logiciels

Chahrazed Boudjemila

Directeur : Fabien Dagnat

Encadrant : Salvador Martinez

École nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire

Processes for Safe and Secure Software and Systems (P4S) Lab-STICC

Thèse janvier 2022

Sommaire

Introduction : Contexte général

- La sécurité
  - Représente un aspect essentiel pour les systèmes
  - Appliquer les pratiques de sécurité permet de : protéger contre les attaques, identifier les vulnérabilités, garantir les accès confidentiels, etc

Introduction : Contexte général

- La sécurité
  - Représente un aspect essentiel pour les systèmes
  - Appliquer les pratiques de sécurité permet de : protéger contre les attaques, identifier les vulnérabilités, garantir les accès confidentiels, etc
- Évolution du système ou de son environnement
  - Possibilité d'évolutions continues au fil du temps pour différentes raisons : ajout de nouvelles fonctionnalités, correction des *bugs*, identification d'une vulnérabilité, changement de déploiement

Ces évolutions doivent satisfaire les exigences de sécurité du système

Problématique

Résultat : ces changements peuvent rendre les systèmes non sécurisés

Problématique

Résultat : ces changements peuvent rendre les systèmes non sécurisés

- Évaluer qu'un changement n'affecte pas la sécurité d'un système nécessite au moins :

Problématique

Résultat : ces changements peuvent rendre les systèmes non sécurisés

- Évaluer qu'un changement n'affecte pas la sécurité d'un système nécessite au moins :
  - Des moyens de représenter l'état de sécurité actuel

Problématique

Résultat : ces changements peuvent rendre les systèmes non sécurisés

- Évaluer qu'un changement n'affecte pas la sécurité d'un système nécessite au moins :
  - Des moyens de représenter l'état de sécurité actuel
  - Les moyens d'évaluer les propriétés de sécurité, lors d'une évolution

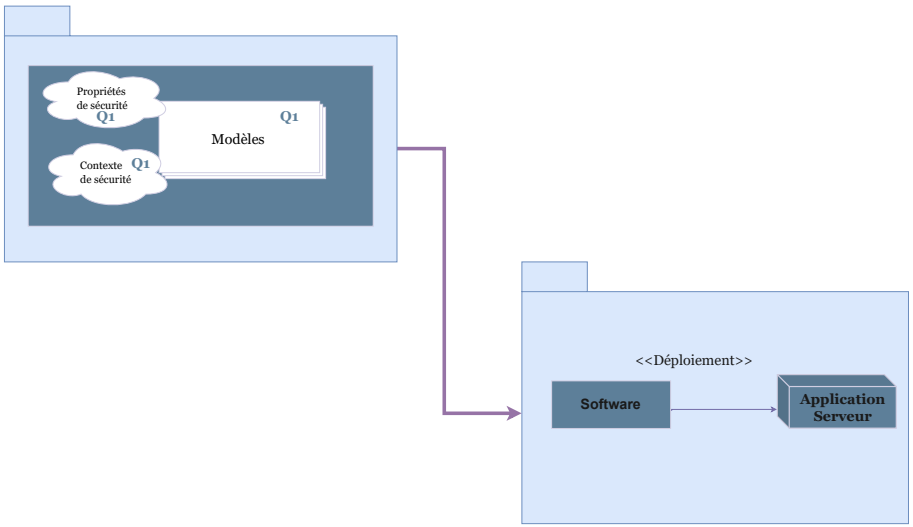
Problématique

Résultat : ces changements peuvent rendre les systèmes non sécurisés

- Évaluer qu'un changement n'affecte pas la sécurité d'un système nécessite au moins :
  - Des moyens de représenter l'état de sécurité actuel
  - Les moyens d'évaluer les propriétés de sécurité, lors d'une évolution
  - Dans le cas ou la sécurité du système est affectée, quelles parties sont affectées ?

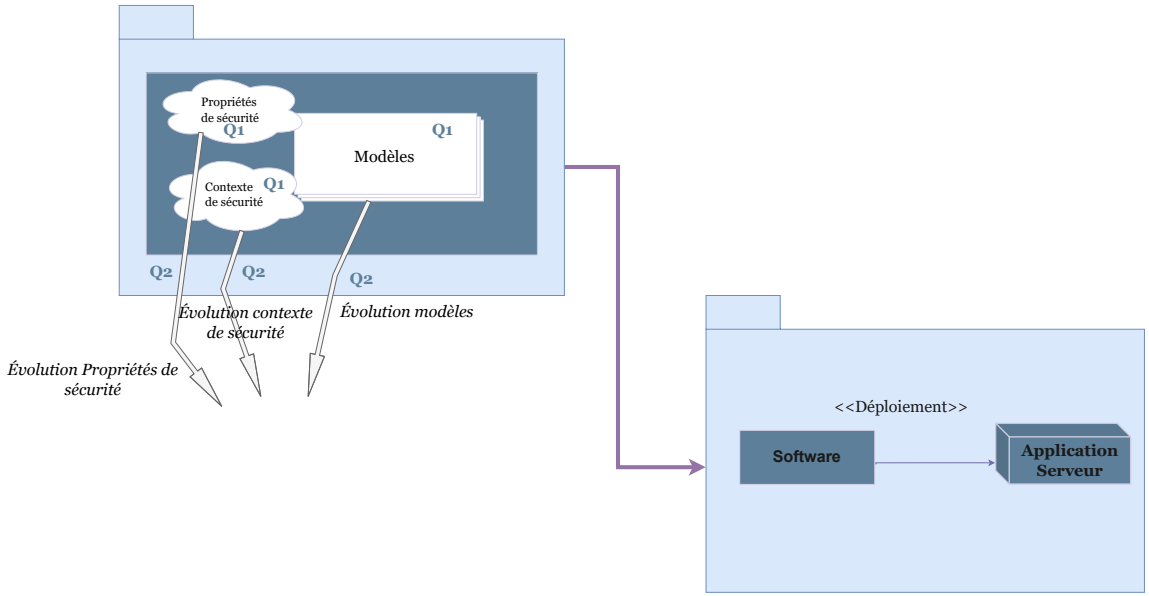
Problématique : objectif de la thèse

Q1- Comment représenter l'état de sécurité et les artefacts d'un système ?



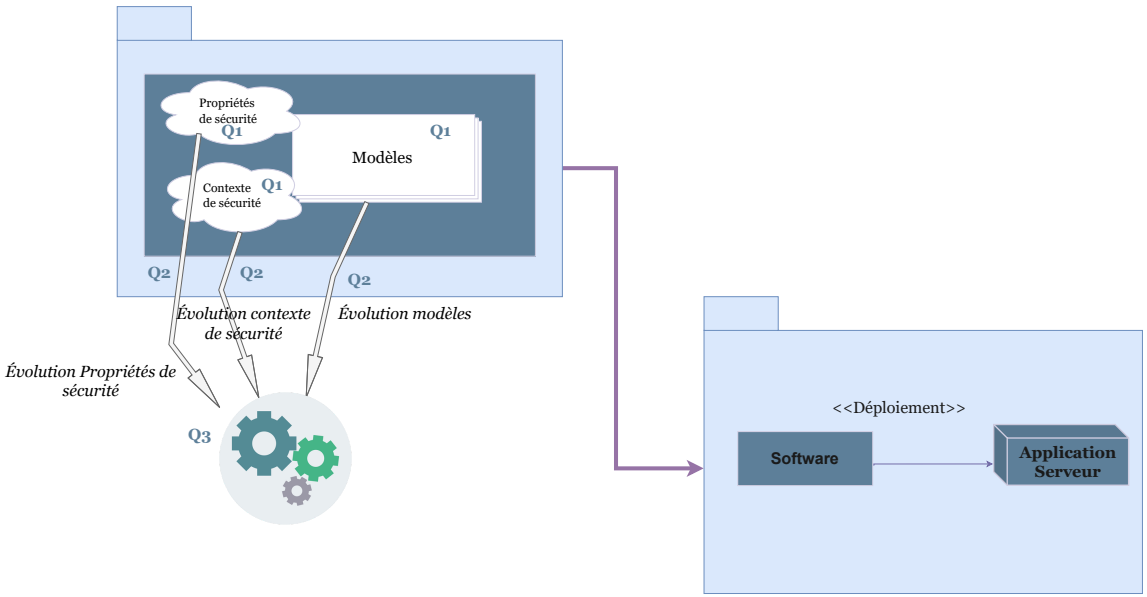
Problématique : objectif de la thèse

Q2- Comment détecter les évolutions du système, des propriétés de sécurité et du contexte de la sécurité ?



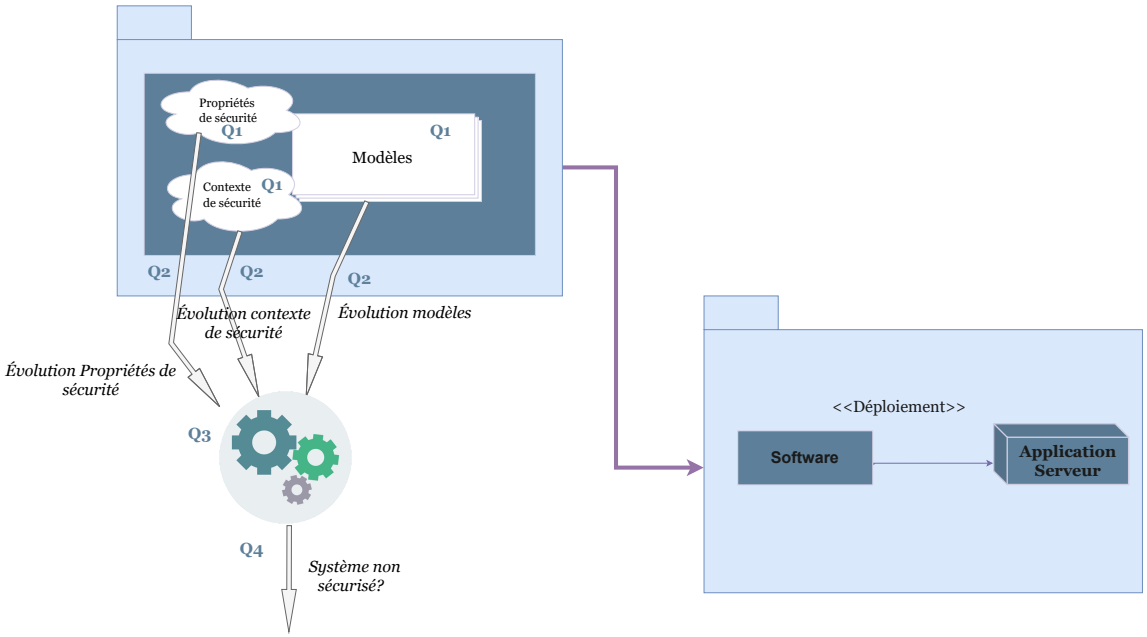
Problématique : objectif de la thèse

Q3- Comment évaluer la sécurité du système ?



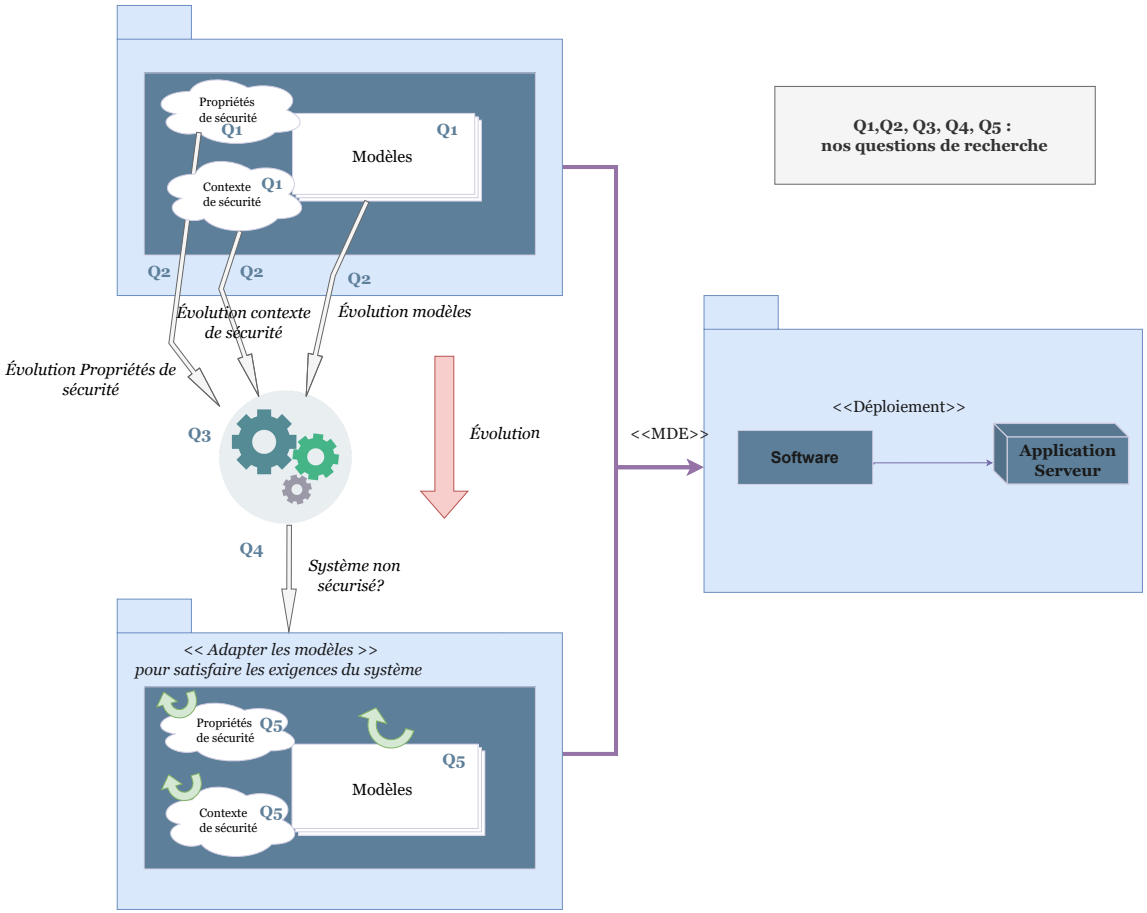
Problématique : objectif de la thèse

Q4- Quelles sont les évolutions qui affectent la sécurité du système ?



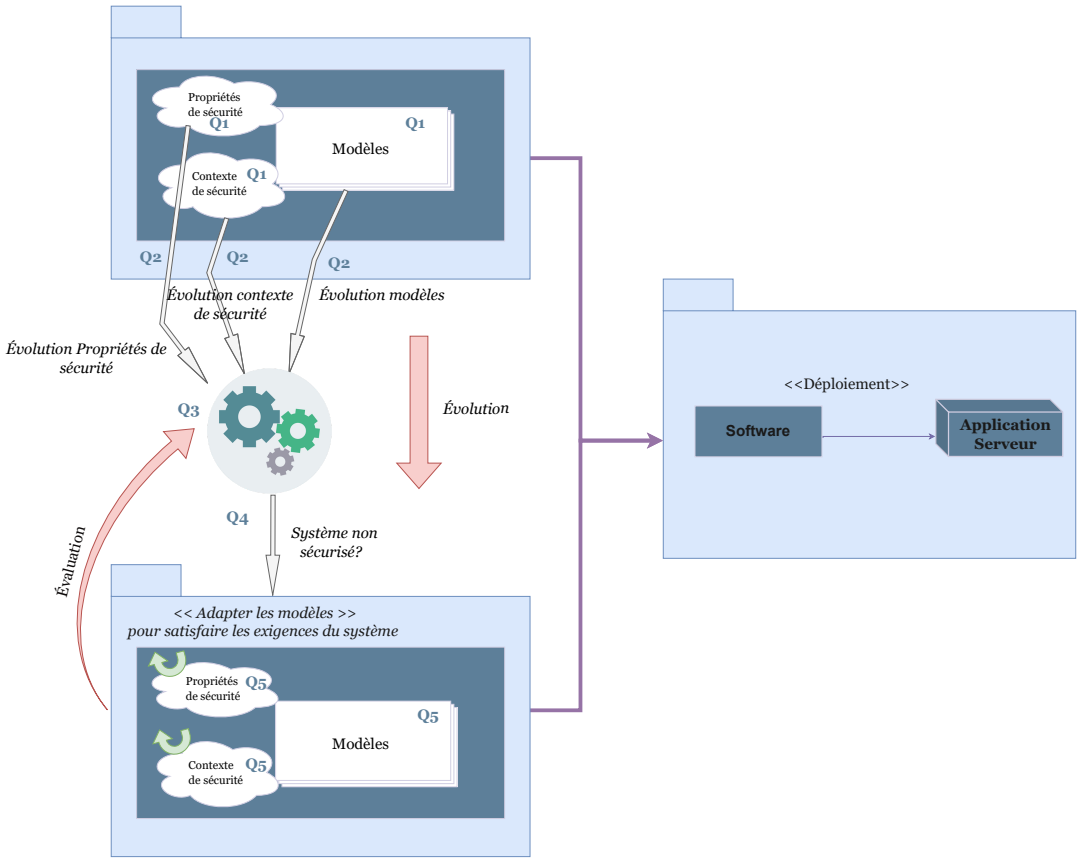
Problématique : objectif de la thèse

Q5- Comment adapter le système après l'évolution des modèles, des propriétés de sécurité et du contexte de sécurité ?



Problématique : objectif de la thèse

Q3- Comment évaluer la sécurité du système ?



État de l'art : les recherches réalisées

- Les approches de l'ingénierie des exigences de sécurité

État de l'art : les recherches réalisées

- Les approches de l'ingénierie des exigences de sécurité

  (NHLABATSI ; NUSEIBEH ; YU, 2012)

  - Des approches orientées but (goal-based)
    - KAOS

      (LAMSWEERDE, 2004)

    - secure i*

      (LIU ; YU ; MYLOPOULOS, 2003)

    - secure Tropos

      (MOURATIDIS ; GIORGINI ; MANSON, 2003)

    - SysMLsec

      (NEJATI et al., 2012)

État de l'art : les recherches réalisées

- Des approches basées sur des modèles(model-based)
  - UMLsec

    (PELDSZUS et al., 2021)
  - SysMLsec
  - SecureUML

    (LODDERSTEDT ; BASIN ; DOSER, 2002)
  - secureBPMN

    (GUYCHARD et al., 2013)

État de l'art : les recherches réalisées

- Des approches pour identifier les problèmes (problem-Oriented)
  - Miseuse case

(MAŽEIKA ; BUTLERIS, 2020)

  - Abuse Frames

(LIN et al., 2004)

État de l'art : les recherches réalisées

- Des approches orientées processus (process oriented)
  - SQuare (Security Quality Requirements Engineering)
    (MEAD ; STEHNEY, 2005)

État de l'art : Analyse des approches par rapport aux objectifs de la thèse

- Représentation des systèmes par un ou plusieurs modèles
- Introduire les aspects de sécurité dans les modèles
- Détection des évolutions : Évolution des composants du système, du contexte de sécurité et des propriétés de sécurité.
- Évaluation de la sécurité des systèmes
- Problème de traçabilité entre les différents artefacts du système

État de l'art : Représentation du système et des aspects de sécurité

- Représentation du système :
  - Diagrammes : Diagramme d'architecture, classe, déploiement
  - Langage de modélisation : SysMLsec, UMLsec
- Représentation des aspects de sécurité
  - Ajouter des annotations de sécurité aux modèles (des étiquettes, contraintes, stéréotypes)
  - Modèle d'exigences de sécurité
  - Des contraintes OCL

État de l'art : Évolution des composants du système, du contexte de sécurité et des propriétés de sécurité

- Détection de changements :
  - Utilisation du *framework* SiLift (PELDSZUS et al., 2021)
  - Outil MoDisco (PELDSZUS, 2020)
  - OpenFlexo (GUYCHARD et al., 2013)

État de l'art : Évolution des composants du système, du contexte de sécurité et des propriétés de sécurité

- Évaluation des changements :
  - Model-checking
  - Thérorème Proving

(BÜRGER et al., 2013)

  - CaRisma

(BÜRGER et al., 2015)

  - Proverif
  - Des contraintes OCL

(IDANI ; CORTES-CORNAX, 2020)

État de l'art : problème de traçabilité entre les différents artefacts du système

- Ils sont appuyés sur le concept MBSE : représentation du système par un ensemble de modèles
- Grande variété des approches :
  - Transformation de modèles : *framework* GRAViTY, Moteur réactif de transformation de modèles, SMR (*Security Maintenance Rules*)
  - Fusion méta-modèle(modèle) : unification, *Bridge* méta-modèle.
  - Composition de langage : language-based multi view
  - Fédération de modèles : OpenFlexo

Bilan état de l'art : analyse des différentes approches

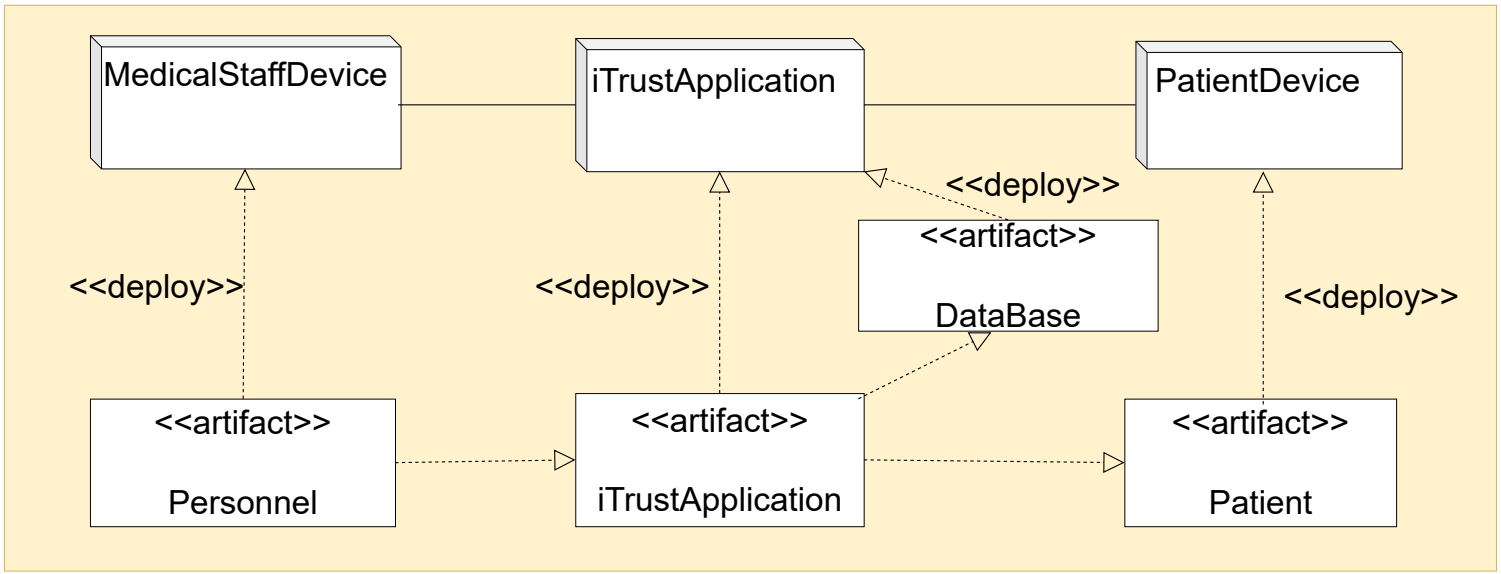
- Il manque des travaux de recherche pour quelque artefacts (composants) du système
- Les recherches ont étudié des cas d'études spécifiques (un seule modèle)
- Ne traitent pas des modèles hétérogènes
- Traitement des changements dans des modèles plus concrets

Démarche : cas d'étude

- Une application médicale pour la gestion des dossiers médicaux
- Rassemble les informations médicales d'un patient à partir de nombreuses sources afin de fournir un résumé détaillé de l'état de santé du patient qui sera utile pour les soins de santé du personnel.
- L'application iTrust aide les étudiants à comprendre l'importance de la sécurité et de la confidentialité
- La possibilité de représenter l'application iTrust par plusieurs modèles
- Les propriétés de sécurité du l'application iTrust : confidentialité, la non répudiation, l'authentification, l'autorisation

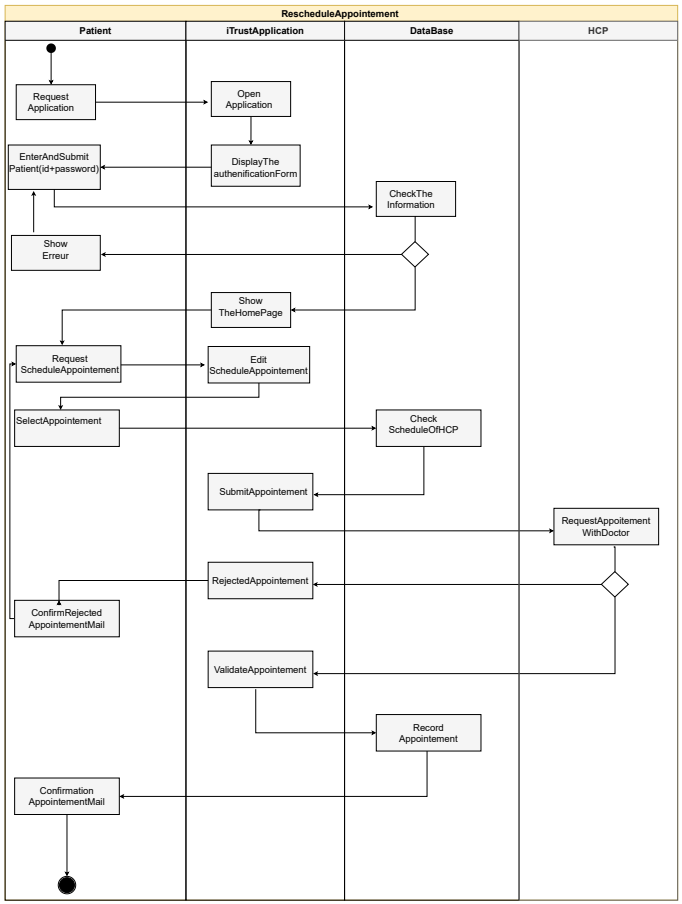
Démarche : cas d'étude

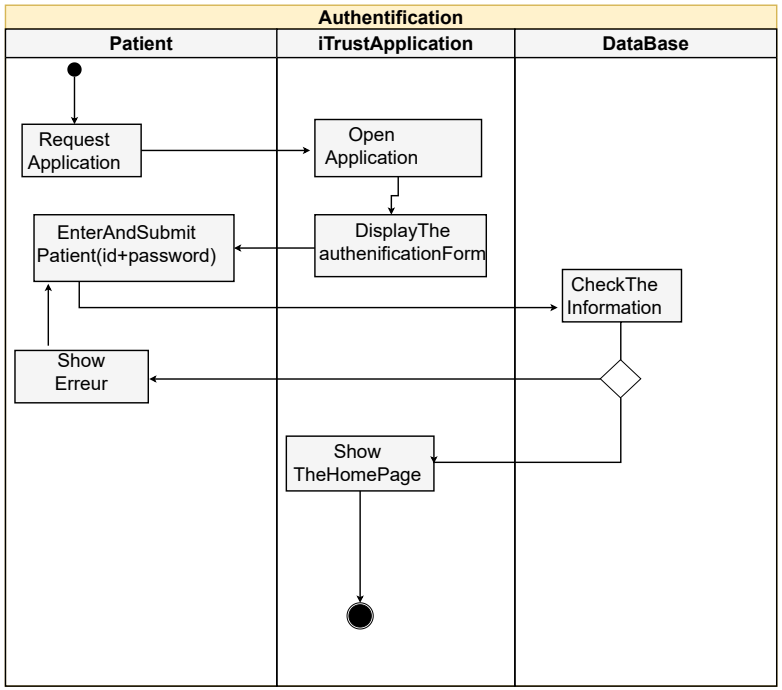
- Les différents diagrammes de l'application iTrust
  - **Diagramme de déploiements**



Démarche : cas d'étude

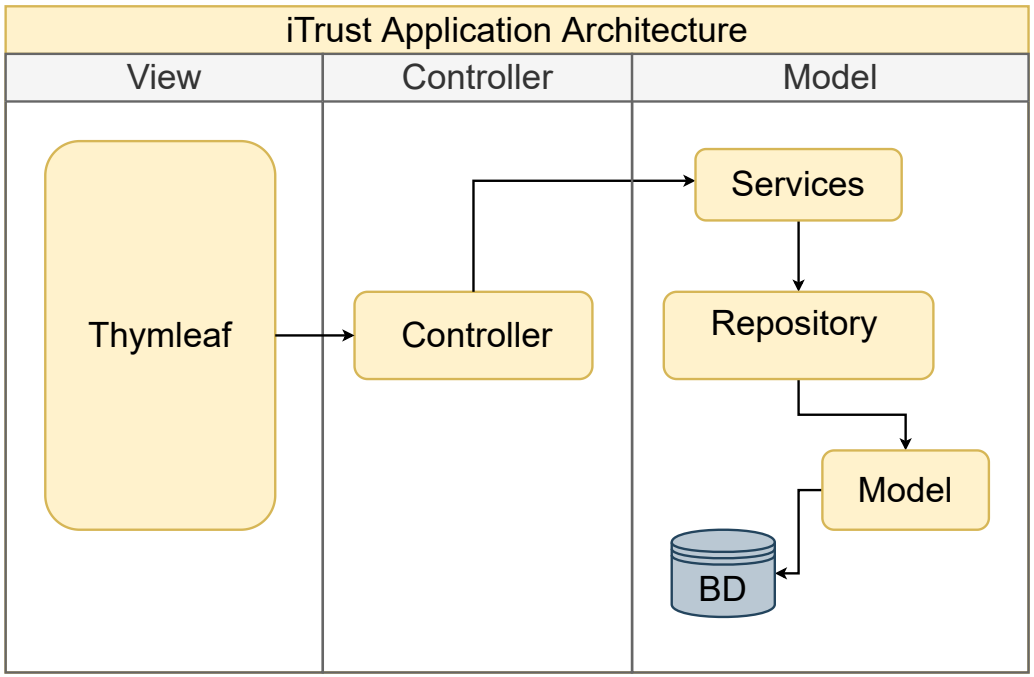
- Les différents diagrammes de l'application iTrust
  - **Diagramme d'activité**





Démarche : cas d'étude

- Les différents diagrammes de l'application iTrust
  - **Diagramme d'architecture**

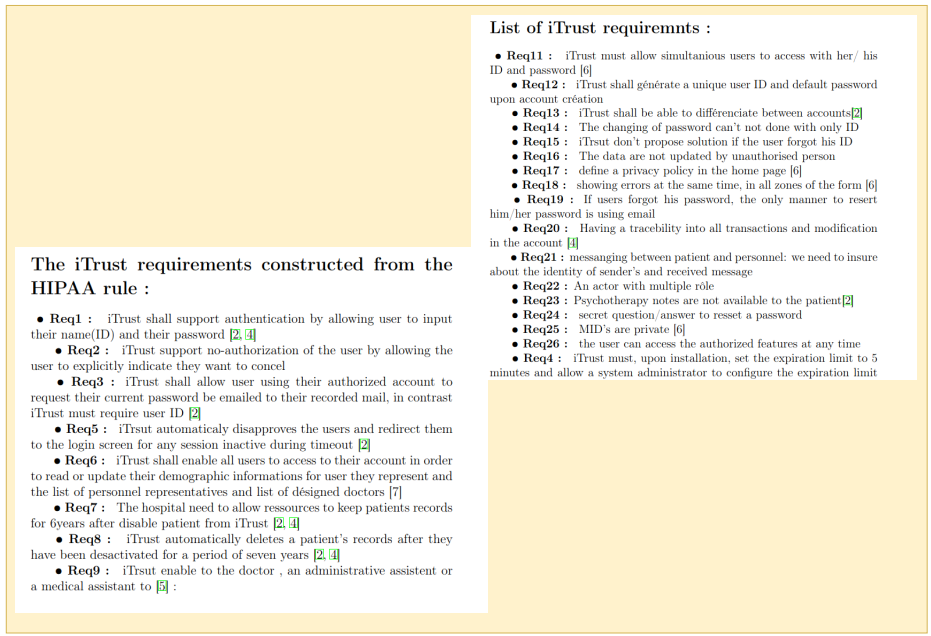


Démarche : cas d'étude

- La liste des exigences de l'application iTrust

- Les exigences de l'application iTrust

- Les règles de HIPAA



The iTrust requirements constructed from the HIPAA rule :

- **Req1 :** iTrust shall support authentication by allowing user to input their name(ID) and their password [2, 4]
- **Req2 :** iTrust support no-authorization of the user by allowing the user to explicitly indicate they want to concel
- **Req3 :** iTrust shall allow user using their authorized account to request their current password be emailed to their recorded mail, in contrast iTrust must require user ID [2]
- **Req5 :** iTrsut automaticaly disapproves the users and redirect them to the login screen for any session inactive during timeout [2]
- **Req6 :** iTrust shall enable all users to access to their account in order to read or update their demographic informations for user they represent and the list of personnel representatives and list of désigned doctors [7]
- **Req7 :** The hospital need to allow ressources to keep patients records for 6years after disable patient from iTrust [2, 4]
- **Req8 :** iTrust automatically deletes a patient's records after they have been desactivated for a period of seven years [2, 4]
- **Req9 :** iTrsut enable to the doctor , an administrative assistent or a medical assistant to [5] :

List of iTrust requiremnts :

- **Req11 :** iTrust must allow simultanious users to access with her/ his ID and password [6]
- **Req12 :** iTrust shall générate a unique user ID and default password upon account création
- **Req13 :** iTrust shall be able to différenciate between accounts[2]
- **Req14 :** The changing of password can't not done with only ID
- **Req15 :** iTrsut don't propose solution if the user forgot his ID
- **Req16 :** The data are not updated by unauthorised person
- **Req17 :** define a privacy policy in the home page [6]
- **Req18 :** showing errors at the same time, in all zones of the form [6]
- **Req19 :** If users forgot his password, the only manner to resert him/her password is using email
- **Req20 :** Having a tracebility into all transactions and modification in the account [4]
- **Req21 :** messanging between patient and personnel: we need to insure about the identity of sender's and received message
- **Req22 :** An actor with multiple rôle
- **Req23 :** Psychotherapy notes are not available to the patient[2]
- **Req24 :** secret question/answer to resset a password
- **Req25 :** MID's are private [6]
- **Req26 :** the user can access the authorized features at any time
- **Req4 :** iTrust must, upon installation, set the expiration limit to 5 minutes and allow a system administrator to configure the expiration limit

Démarche : les pistes envisagées

- Privilégier les liens entre les modèles, ce qu'on appel la fédération de modèles
- La détection et l'évaluation deviennent un problème de cohérence de la fédération
- Intégration de notre solution dans Openflexo
- Évaluer l'approche par notre cas d'études

Démarche : Avant et durant année de thèse

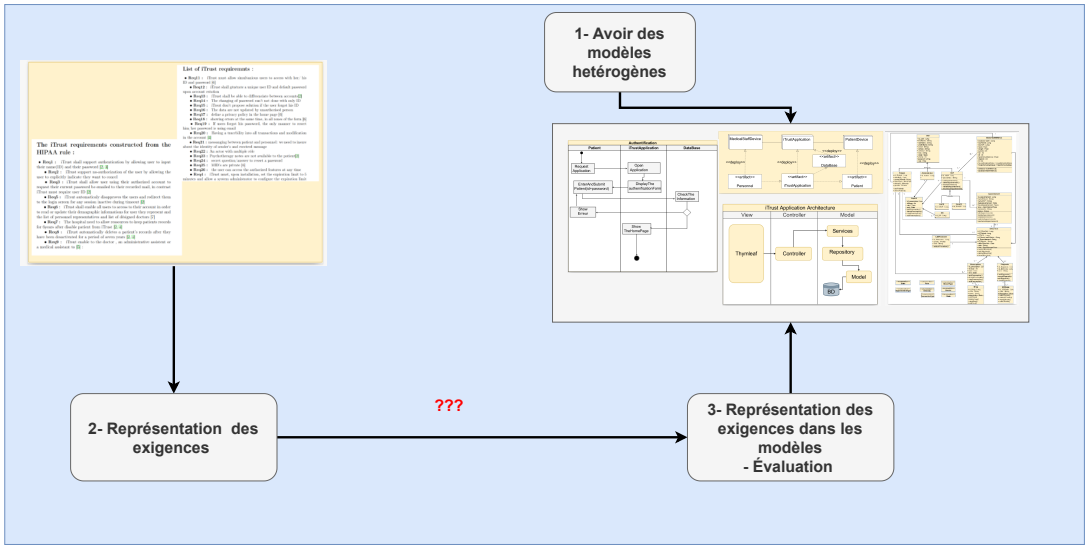
- Durant la thèse
  - Découvrir le monde des modèles et l'ingénierie des modèles, les exigences de sécurité, préparation d'un poster
  - Une formation EASE (Être Acteur de sa satisfaction dans son emploi), formation pédagogique.
  - Le choix d'un cas d'étude : application médicale iTrust

Démarche : Avant et durant année de thèse

- Durant la thèse
  - Découvrir le monde des modèles et l'ingénierie des modèles, les exigences de sécurité, préparation d'un poster
  - Une formation EASE (Être Acteur de sa satisfaction dans son emploi), formation pédagogique.
  - Le choix d'un cas d'étude : application médicale iTrust
- Durant 2022-2024
  - Formation JAVA EE Spring, éthique de la recherche
  - Explorer plus d'articles
  - Entamer la réalisation de mon approche

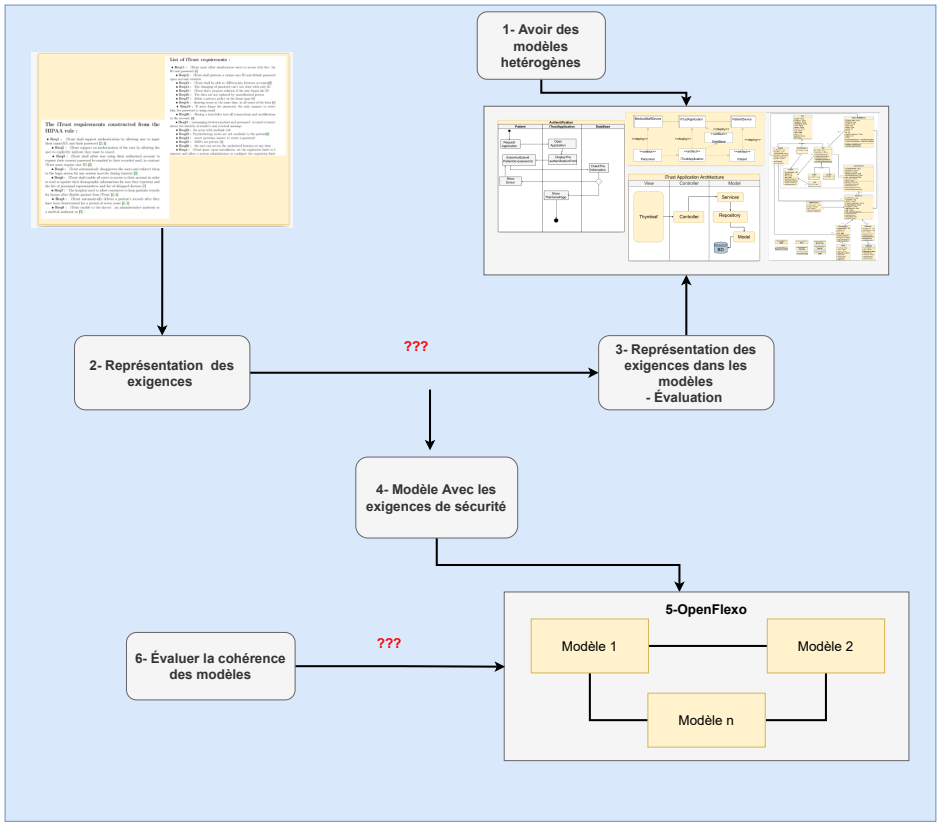
Démarche : Avant et durant année de thèse

Première étape :



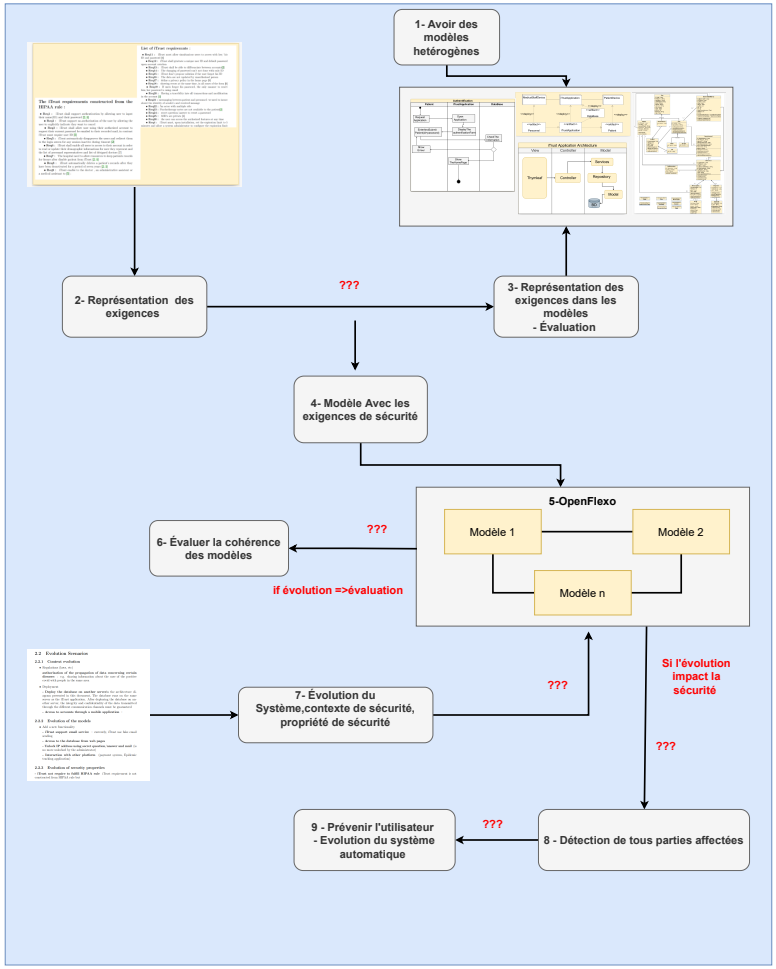
Démarche : Avant et durant année de thèse

Deuxième étape :



Démarche : Avant et durant année de thèse

Troisième étape :

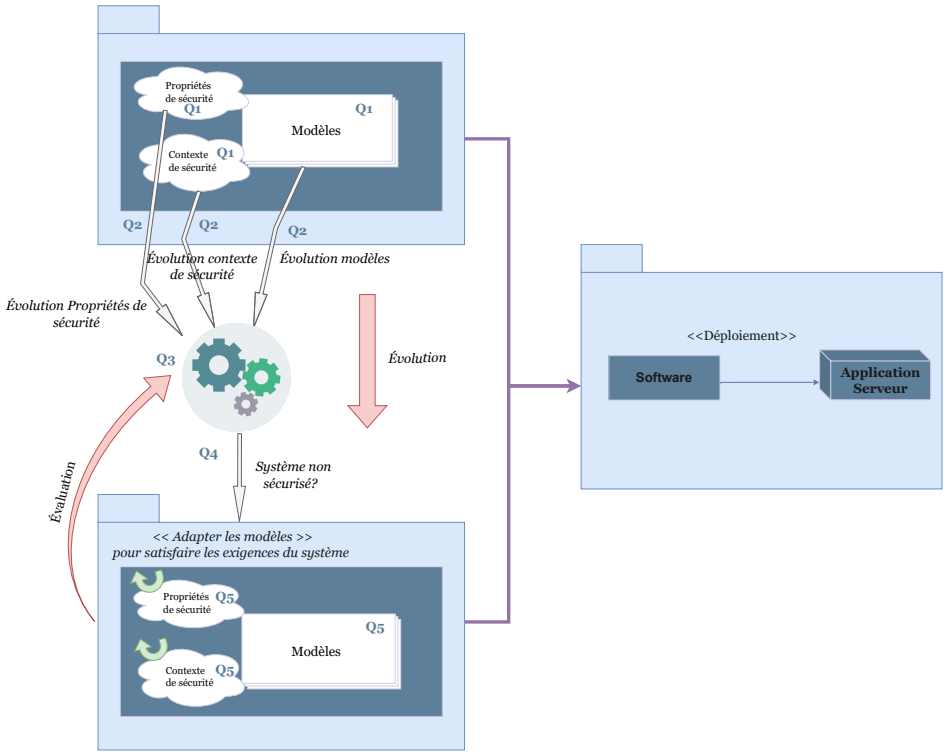


Conclusion

1- Des moyens de représenter l'état de sécurité actuel du système

2-Les moyens d'évaluer, lors d'une évolution

3- Quelles parties sont affectées ?



Références I

BÜRGER, J. et al. Restoring security of long-living systems by co-evolution. In : IEEE. *2015 IEEE 39th Annual Computer Software and Applications Conference*. [S.l.], 2015. v. 2, p. 153–158.

BÜRGER, J. et al. Model-based security engineering : Managed co-evolution of security knowledge and software models. In : *Foundations of Security Analysis and Design VII*. [S.l.] : Springer, 2013. p. 34–53.

GUYCHARD, C. et al. Conceptual interoperability through models federation. In : *Semantic Information Federation Community Workshop*. [S.l. : s.n.], 2013. p. 23.

Références II

IDANI, A. ; CORTES-CORNAX, M. Towards a model driven formal approach for merging data, access control and business processes. In : *Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems : Companion Proceedings*. [S.l. : s.n.], 2020. p. 1–5.

LAMSWEERDE, A. V. Elaborating security requirements by construction of intentional anti-models. In : IEEE. *Proceedings. 26th International Conference on Software Engineering*. [S.l.], 2004. p. 148–157.

LIN, L. et al. Using abuse frames to bound the scope of security problems. In : IEEE. *Proceedings. 12th IEEE International Requirements Engineering Conference, 2004.* [S.l.], 2004. p. 354–355.

Références III

LIU, L. ; YU, E. ; MYLOPOULOS, J. Security and privacy requirements analysis within a social setting. In : IEEE. *Proceedings. 11th IEEE International Requirements Engineering Conference, 2003.* [S.l.], 2003. p. 151–161.

LODDERSTEDT, T. ; BASIN, D. ; DOSER, J. Secureuml : A uml-based modeling language for model-driven security. In : SPRINGER. *International Conference on the Unified Modeling Language*. [S.l.], 2002. p. 426–441.

MAŽEIKA, D. ; BUTLERIS, R. Mbsesec : Model-based systems engineering method for creating secure systems. *Applied Sciences*, Multidisciplinary Digital Publishing Institute, v. 10, n. 7, p. 2574, 2020.

Références IV

MEAD, N. R. ; STEHNEY, T. Security quality requirements engineering (square) methodology. *ACM SIGSOFT Software Engineering Notes*, ACM New York, NY, USA, v. 30, n. 4, p. 1–7, 2005.

MOURATIDIS, H. ; GIORGINI, P. ; MANSON, G. Modelling secure multiagent systems. In : *Proceedings of the second international joint conference on Autonomous agents and multiagent systems*. [S.l. : s.n.], 2003. p. 859–866.

NEJATI, S. et al. A sysml-based approach to traceability management and design slicing in support of safety certification : Framework, tool support, and case studies. *Information and Software Technology*, Elsevier, v. 54, n. 6, p. 569–590, 2012.

Références V

NHLABATSI, A. ; NUSEIBEH, B. ; YU, Y. Security requirements engineering for evolving software systems : A survey. In : *Security-aware systems applications and software development methods*. [S.l.] : IGI Global, 2012. p. 108–128.

PELDSZUS, S. Model-driven development of evolving secure software systems. In : *Software Engineering (Workshops)*. [S.l. : s.n.], 2020.

PELDSZUS, S. et al. Ontology-driven evolution of software security. *Data & Knowledge Engineering*, v. 134, p. 101907, 05 2021.