Risk Analysis of Water Grid Systems Using Threat Modeling

Mme Véronique Legrand – Enseignante

Yves Ruffenach – Auditeur

**Synthèse structurée**

*Contexte et problématique de l’approche proposée par les auteurs*

Le contexte de l’approche repose sur la sécurisation des systèmes de gestion d’eau ( W G S ), qui sont des systèmes critiques dans l’infrastructure des villes modernes. Ces systèmes, constitués de capteurs, pompes, réservoirs et contrôleurs, sont vulnérables aux attaques cyber. en raison de leur interconnexion croissante avec l’internet des objets ( I o T ). La problématique majeure est donc d’identifier, évaluer et contrer les menaces pesant sur ces systèmes afin de garantir leur intégrité, leur disponibilité et leur fiabilité. Ainsi, la problématique centrale est : comment identifier, évaluer et atténuer les menaces qui pèsent sur les systèmes de réseaux d'eau ( W G S ) face aux attaques susceptibles d'affecter la confidentialité, l'intégrité et la disponibilité des services ?

*Principe, formalisme, architecture et modèle adopté par les auteurs*

Les auteurs proposent une approche basée sur la modélisation des menaces pour classer les menaces, évaluer les risques associés et proposer des contre-mesures adaptées. Le principe adopté repose sur une méthodologie de modélisation des menaces, qui suit une approche structurée en cinq étapes :

* Identification des actifs du système : tous les composants critiques matériels et logiciels.
* Identification des points d’accès : les interfaces physiques et logicielles susceptibles d’être exploitées.
* Classification des menaces à l’aide du modèle S T R I D E  : Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
* Évaluation des menaces via le modèle D R E A D , qui attribue des scores basés sur la gravité, l’exploitabilité et l’impact.
* Propositions de contre-mesures pour atténuer les menaces selon leur criticité.

L’architecture utilisée par les auteurs, basée sur les différentes couches du système S C A D A , est appropriée car elle permet une analyse précise des flux de données et des zones de confiance pour chaque niveau (capteurs, contrôleurs, interfaces utilisateurs, réseaux). Cette granularité facilite l’identification des vulnérabilités spécifiques à chaque couche. *Un système SCADA (Supervisory Control And Data Acquisition) est un système industriel qui permet de superviser, contrôler et collecter en temps réel les données de processus industriels via des capteurs, des automates et une interface centralisée.* Le formalisme repose sur des diagrammes de flux de données ( D F D ) pour visualiser les composants critiques, les flux d'informations et les zones de confiance (trust zones). L'architecture en couches du W G S permet de décomposer les menaces selon leurs emplacements respectifs (couches 0 à 5). Cette modélisation est appropriée car elle tient compte de la séparation entre les environnements O T et I T , ainsi que des points d'accès spécifiques aux couches physiques, logicielles et réseau.

*Nos contribution respectives*

Dans notre groupe, nous avons utilisé GitHub comme plateforme principale pour collaborer sur notre projet. Chaque membre de l'équipe a pu créer des branches séparées à partir du dépôt principal pour développer de nouvelles fonctionnalités ou corriger des bugs sans affecter le code principal. Cette approche nous a permis de travailler en parallèle sans interférer avec le travail des autres. Une fois nos modifications terminées, nous les avons proposées sous forme de *pull requests*. Cela a permis aux autres membres de l'équipe de réviser, discuter et approuver les changements avant qu'ils ne soient fusionnés dans la branche principale. GitHub nous a également aidés à gérer les versions, suivre les issues (problèmes ou tâches) et documenter notre travail, ce qui a grandement facilité l'organisation et la communication au sein de l'équipe. Grâce à cette méthode, chaque contribution individuelle a été bien organisée et intégrée de manière fluide dans le projet global.

*L’expérimentation*

Notre code est un exemple de modélisation des menaces appliqué à la gestion des actifs et de leurs menaces associées, spécifiquement conçu pour le W G S . Il utilise une approche systématique basée sur des menaces et contre-mesures prédéfinies pour identifier et atténuer les risques.

Le système commence par établir une base de données de menaces et de contre-mesures correspondantes. Par exemple, pour contrer la menace d'usurpation d'identité des opérateurs, des mécanismes d'authentification robustes sont mis en place. Un dictionnaire "actifs\_info" centralise les informations sur les différents composants du système, incluant les capteurs de pression d'eau, les réservoirs, les pompes et les systèmes de contrôle S C A D A . Chaque actif est caractérisé par un niveau de risque (*Élevé, Moyen, Faible*) et dispose d'espaces dédiés pour répertorier les menaces et les mesures associées.

Pour quantifier les risques, un système de conversion a été mis en place via le dictionnaire *valeurs\_risque*, transformant les évaluations qualitatives *(Élevé, Moyen, Faible)* en valeurs numériques *(3, 2, 1).* Un dictionnaire inverse permet la conversion dans l'autre sens. Le système intègre également une liste *points\_acces* qui détaille les différents points d'entrée du système et leurs niveaux de confiance respectifs. Par exemple, les ports USB destinés à la maintenance des capteurs sont considérés comme ayant un niveau de confiance *Faible*, tandis que les ports réseau dédiés à la communication entre capteurs et contrôleurs bénéficient d'un niveau de confiance *Élevé*.

L'interface utilisateur permet d'enrichir dynamiquement la base de données des actifs via une boucle interactive. Pour chaque nouvel actif ajouté, l'utilisateur spécifie son nom et son niveau de risque, avec une validation des entrées pour garantir leur cohérence. Le système guide ensuite l'utilisateur dans l'identification des menaces spécifiques à chaque actif, associant automatiquement les contre-mesures appropriées issues de la base de données *menaces\_avec\_mesures*. Un inventaire quantitatif est également maintenu via le dictionnaire *installation\_info*, qui répertorie le nombre d'unités de chaque actif présent dans l'installation.

Le calcul du risque global utilise une approche pondérée, prenant en compte à la fois le niveau de risque de chaque actif et sa présence quantitative dans l'installation. Cette évaluation inclut également les risques liés aux points d'accès, aboutissant à une évaluation moyenne qui est ensuite traduite en termes qualitatifs.

Le système génère des rapports détaillés présentant, pour chaque actif, son niveau de risque, les menaces identifiées et sa présence quantitative dans l'installation. Il fournit également des recommandations de mesures spécifiques en fonction des menaces détectées et du niveau de risque global. Par exemple, un niveau de risque Élevé déclenche des recommandations pour la mise en place immédiate de mesures strictes, incluant des tests de pénétration et des évaluations régulières de vulnérabilité.

Cette approche structurée de la modélisation des menaces permet une gestion proactive et systématique des risques de sécurité, essentielle pour maintenir l'intégrité et la fiabilité du système W G S .

*Liens avec le cours SEC202*

L'étude *Risk Analysis of Water Grid Systems Using Threat Modeling* de FIZA ABDUL RAHIM et al. s'aligne avec plusieurs aspects du cours SEC202, notamment à travers l'application de la modélisation des menaces aux systèmes de gestion des réseaux d'eau ( W G S ). L'utilisation des méthodologies S T R I D E et D R E A D pour l'identification et l'évaluation des menaces reflète l'approche de sécurité globale enseignée. Bien que l'étude ne se concentre pas directement sur les architectures *Cloud*, *Fog* ou *Edge*, sa méthodologie d'analyse de sécurité des systèmes complexes est transposable à ces contextes. Elle démontre l'application pratique des exigences et normes de sécurité, mais gagnerait à approfondir les aspects spécifiques aux architectures cloud et à l'intégration des produits connectés.