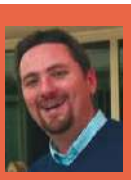


Frédéric Sagez
Consultant IT
fsagez@gmail.com

Threat Modeling, « Think like an Attacker »

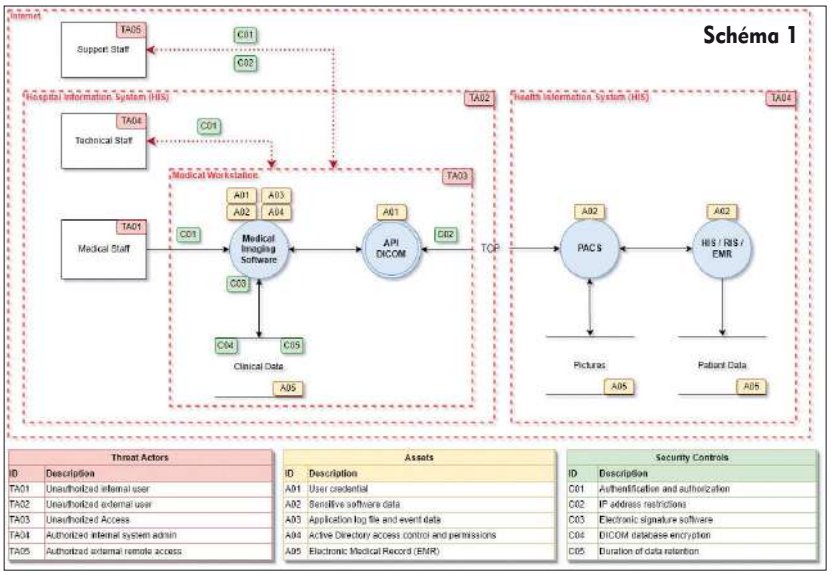
Se mettre à la place d'un attaquant, comprendre comment sont formulés des attaques, comment sont fabriqués des exploits et pour qui et surtout pourquoi il y a des faiblesses dans votre architecture, votre solution ou tout simplement votre logiciel. Le Threat Modeling permet de répondre à toutes ses questions tout en nous aidant d'un modèle de classification (STRIDE, PASTA, etc.) pour développer chaque type de menaces suivant un contexte bien précis.

Les objectifs de la modélisation des menaces va nous permettre de mettre en place dans une structure de développement, une technique de sécurité systématique et structurée qui est utilisée pour identifier les objectifs de sécurité, des menaces et les vulnérabilités d'une application ou d'un software et surtout pour nous aider à prendre des décisions de conception et d'ingénierie et surtout à déterminer où prioriser les efforts dans la conception, le développement et le déploiement d'applications ou de logiciels sécurisées.

Il est important d'acquérir une compréhension de tout ce qui est modélisé par la menace car cela va nous permettre de recenser toutes les informations requises afin de mieux protéger les ressources, référencer les points d'entrées/sorties de votre système, les flux d'échanges de données, s'il existe des mécanismes de contrôle pour ainsi mieux identifier les attaquants potentiels. Nous pouvons nous aider dans un premier temps en réfléchissant avec les équipes et en modélisant un diagramme de contexte (**Schéma 1**).

Une fois toutes les menaces recensées, on peut produire une liste d'attaques potentiels et s'intéresser sur l'éventuel chemin que peux utiliser un agent de menace pour atteindre un actif avec un objectif précis sans passer par un contrôle et surtout en le déjouant. Pour mieux résumer une situation type : un attaquant peut exploiter une vulnérabilité sur un composant du système et compromettre un élément important comme par exemple les données d'une application qui est aujourd'hui la cible privilégiée des pirates.

Schéma 1



ÉTAPE 1

La première phase est la plus importante : c'est ici que vous regrouperez toutes les informations utiles qui sont liées au contexte d'utilisation de votre système, que ce soit technique ou fonctionnel, il faudra surtout s'appuyer sur des scénarios d'utilisations et sur les utilisateurs finaux sans oublier l'équipe technique. Cela vous permettra de récolter des informations essentielles et de commencer à démarquer les périmètres d'utilisation de votre système.

ÉTAPE 2

La deuxième phase va nécessiter d'identifier tous les composants, cartographier tous les flux qui sont échangés dans votre système et identifier d'autres systèmes extérieurs, et c'est à partir de là que l'on va préciser les périmètres de confiance des échanges d'informations ! Pour finir de compléter toutes ses informations, nous allons décrire toutes ses interactions possibles sur le système en dessinant un diagramme : le Data Flow Diagram. Le **Schéma 2** nous permet ainsi d'avoir des détails spécifiques et nécessaires sur le fonctionnement du système.

Il existe différents types, de différents niveaux et dans votre cas, assurez-vous pour la suite de bien exhiber les informations suivantes : les principaux acteurs, les flux échangés, les données ou stockage de données, les zones de confiance où

il y a des échanges extérieurs ainsi que les principales fonctionnalités. Dans cet exercice beaucoup d'éléments doivent apparaître comme par exemple, si vous utilisez Internet ou un Intranet il doit y avoir un pare-feu, des ports utilisés et énumérés ou un VPN installé. Si vous utilisez des données, elles doivent être stockées dans un SGBDR. Si vous utilisez des systèmes tiers tels que des API, des Web Services ou des services pour s'identifier avec des échanges de flux spécifiques. Sans oublier les points d'entrées et de sorties de votre système avec des limites de confiance dans son utilisation avec des interactions avec les utilisateurs finaux.

ÉTAPE 3

La troisième étape consiste tout simplement à identifier et recenser toutes les menaces possibles suivant les scénarios d'utilisation vus dans l'étape précédente. Ici nous pouvons être aidés pour structurer notre approche sur l'identification de menaces en utilisant différentes bonnes pratiques ou méthodologies : arbres d'attaque (représentation visuelle des menaces), OCTAVE (méthode de modélisation des menaces fondées sur l'évaluation des risques), PASTA (simulation et analyse des menaces), TRIKE (modèles de menace comme outil de gestion des risques), DREAD (modèles de menace par catégorie) ou encore STRIDE (modélisation des menaces pour chaque composant du système) qui sera utilisé par Microsoft fin des années 90 pour aider les développeurs à identifier les menaces sur leurs propres produits.

Intéressons-nous ici à la méthode STRIDE de Microsoft pour comprendre son fonctionnement. STRIDE consiste à l'énumération des cinq facteurs suivants :

- S comme Spoofing qui consiste à usurper l'identité d'une autre personne ou d'un processus, le type d'attaque utilisé est le « Session Hijacking »,
- T comme Tampering, falsification ou modification non autorisées avec par exemple une attaque de type sabotage intentionnel comme le « SQL Injection »,
- R comme Répudiation : opération illégale ou malveillante dans un système par un attaquant non prouvé, le type d'attaque peut être l'« Audit Log Deletion »,
- I comme Information Disclosure consiste à une fuite d'informations qui est révélée à tous les utilisateurs, le type d'attaque est « Verbose Exception »,
- D comme Denial of Service (DoS) sont des attaques qui empêchent un utilisateur d'accéder à des ressources avec indisponibilité du service, le type d'attaque pratiqué est « Website defacement »,
- E comme Élévation de privilèges (EoP) qui permet à un utilisateur d'accéder à des données non autorisées ou d'avoir un niveau avec accès privilégié, type d'attaque « Logic Flow Attacks ».

Je rappelle toutefois que tous les types d'attaques citées plus haut sont recensées et notées par des organismes tel que la fondation OWASP ou le MITRE ATT&CK avec une base de données internationale conséquentes sur les vulnérabilités les plus courantes et les plus dangereuses.

Il existe des logiciels pour modéliser des menaces, par exemple l'application Microsoft Threat Modeling Tool est disponible gratuitement avec de la documentation. Simple d'utilisation, dans un premier temps vous devez créer votre modèle ou utiliser des templates spécifiques de modèles, ensuite vous devez élaborer le diagramme de modèle des menaces de votre application ou de votre logiciel tout en indiquant les process, les entités externes, les data flow, les espaces de stockage et les zones dites « trust boundary » tout en renseignant les propriétés de chaque élément (**Schéma 3**) suivant les informations fournies dans le Data Flow Diagram produit en amont. Ensuite il suffit de basculer sur la vue Analyse pour avoir une liste très détaillée des menaces générées par l'outil et affiché par catégories (STRIDE) et suivant les process et les échanges de flux. Vous allez devoir appréhender des sujets de sécurités auxquels vous n'aviez pas forcément pensé ! A partir de cet écran, vous devez commencer votre analyse tout en renseignant l'état de chaque menace, la justification et sa priorité (**Schéma 4**). Vous pouvez une fois votre travail terminé, édité un rapport que vous pourrez ensuite partagé avec les différents membres de vos équipes..

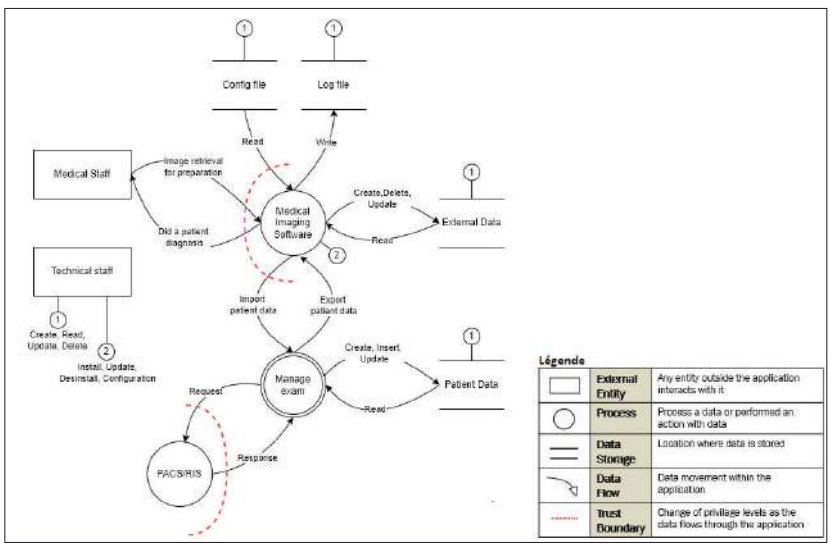


Schéma 2

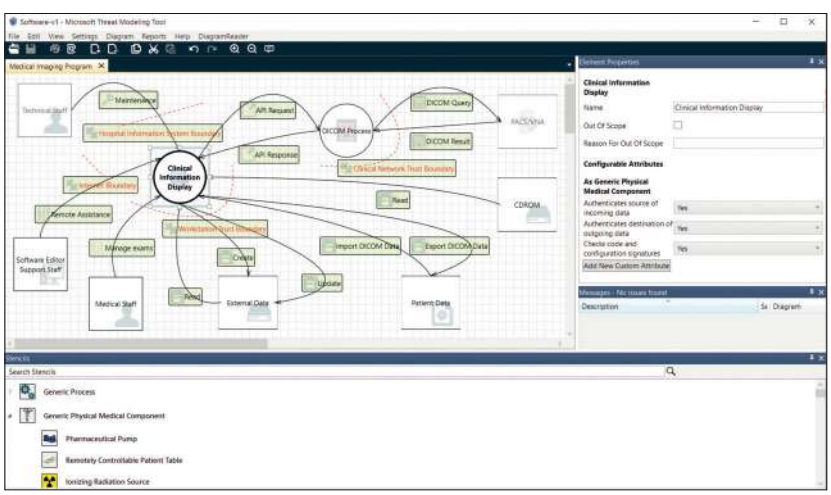


Schéma 3

ÉTAPE 4

La quatrième et dernière étape consiste tout simplement à classer toutes les menaces recensées selon le type de risques ainsi que les probabilités et les impacts. On peut classer les

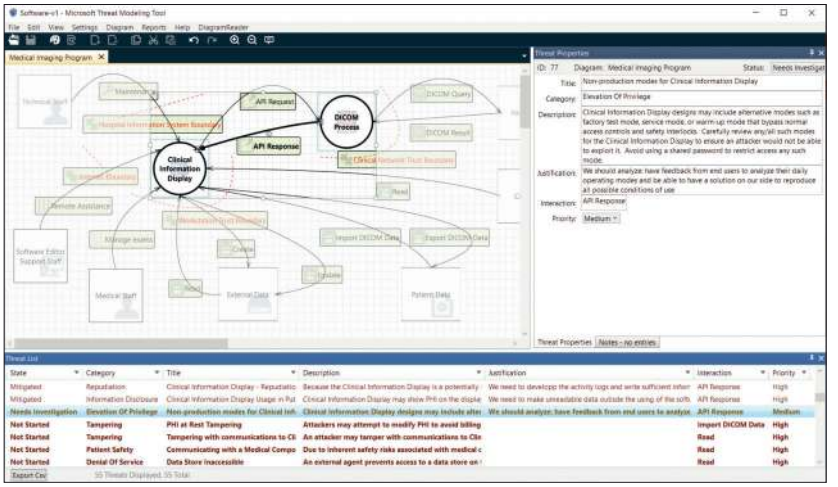


Schéma 4

menaces sur cinq types : accepté (risque résiduel atténué), atténué (qui va nécessiter une évolution ou une correction), transféré (vers une partie prenante ou accepter les conditions d'utilisation via un manuel), ignoré (à éviter !) ou contre mesure (solution à mettre en place pour rendre plus difficile l'exploitation d'une menace). Ensuite vous pouvez définir une probabilité d'attaque et son impact qui peuvent-être notés du plus élevé au plus faible. Chaque information peut être partagée avec les différentes parties prenantes de votre projet, car une modélisation efficace des menaces nécessite l'adhésion de la direction et du personnel technique pour être ensuite validée et documentée pour la sécurité globale de celui-ci.

Cette dernière partie intervient généralement dans la phase de Design Analysis dans le cycle de développement et permet de remettre en question la conception de la sécurité au sein des équipes, mais permet aussi de se remettre en question sur des erreurs de conception ou de codage, de passer le cap éventuellement sur l'absence d'exigences de sécurité ou par manque de connaissances en matière de normes sécuritaires. Je vous engage d'ailleurs à surfer sur le site de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui vous conseille tout en vous guidant sur les bonnes pratiques dans le développement de votre solution. Il est aussi recommandé d'effectuer des revues d'architecture avec modélisation et faire un point sécurité tout au long du cycle de vie d'un produit. Le National Institute of Standard and Technology (NIST) peut vous guider en utilisant des frameworks interactifs afin d'atténuer et mieux gérer les risques. (Guide SP 800-30 Rev 1)

J'ai redécouvert récemment le monde de l'industrie en accompagnant une équipe de développement de logiciels d'imagerie médicale pour mettre en place un plan de cyber sécurité. Le processus de modélisation du Threat Modeling a permis de sensibiliser les développeurs à la sécurité et de permettre la création d'une matrice de traçabilité des risques pour y enregistrer les contrôles manquants ou les faiblesses du logiciel liés à un environnement médical, tout en interagissant aussi sur les règlements gouvernementaux changeants tels que la MDCG ou le FDA qui sont principalement liés au risque patient.

Vous pouvez lire mon retour d'expérience à ce sujet sur mon espace Slide Share à l'adresse suivante : https://urlz.fr/jQt1.