Une école de l'IMT

UML pour les systèmes embarqués

Examen Polytech'Nice GSE 2018

Logiciel d'une "FortiSandbox"

Ludovic Apvrille

ludovic.apvrille@telecom-paristech.fr

http://soc.eurecom.fr/UMLEmb/

Pendant un examen, il est interdit de communiquer avec une autre personne. Les seuls documents autorisés sont les transparents du cours, les exercices faits en cours, ainsi que les sujets de TP. Les appareils électroniques sont interdits, sauf les traducteurs pour les étudiants étrangers.
Le barème est fourni pour chaque question. 1 point de bonus est donné pour la qualité de la rédaction.

1 Système à modéliser et consignes

Le système à modéliser est le logiciel d'un analyseur de fichiers appelé "FortiSandbox". Cette description est extraite de la spécification d'un système réel[1], mais vous ne devez modéliser que le logiciel de la "FortiSandbox" tel que décrit ci-dessous dans l'énoncé.

Vous avez deux heures pour réaliser votre modèle, et répondre aux questions. Le temps étant assez court, cela veut dire que vous devez faire des hypothèses de modélisation, comme indiqué dans la première question.

La notation prend en compte à la fois la qualité des modèles, et les éventuels commentaires qui accompagnent ces modèles afin de les rendre plus compréhensibles.

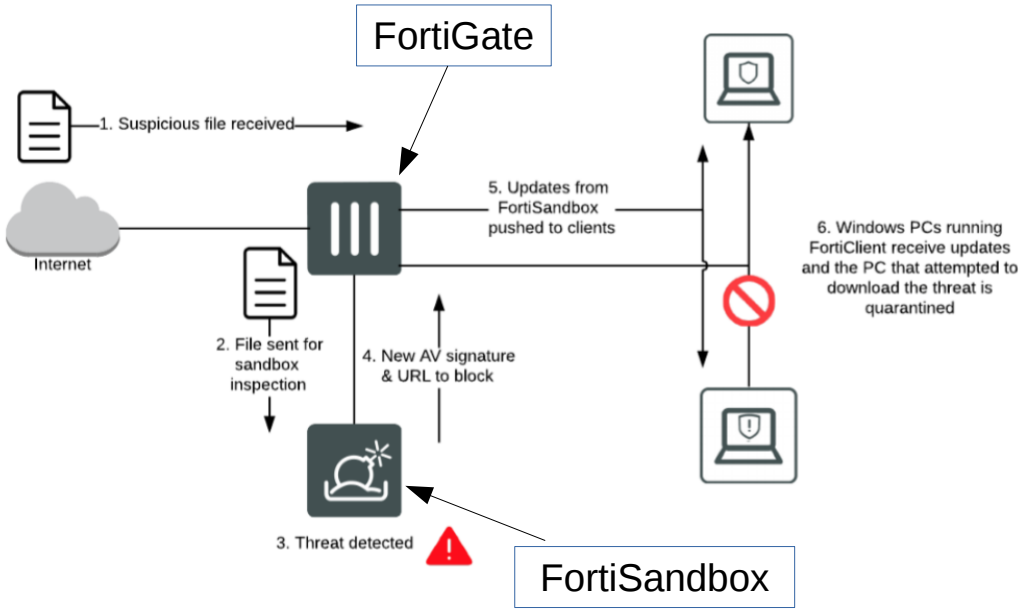
2 Spécification du système

2.1 Description

Description générale
L'inspection de fichiers à l'aide d'une *FortiSandbox* consiste à récupérer des fichiers transitants sur un réseau. Cette analyse permet de détecter des menaces capables de mettre en défaut la sécurité d'ordinateurs connectés sur ce réseau.
Les fichiers exécutables suspicieux sont détectés au sein des flux réseaux par des routeurs appelés "FortiGate". Quand un tel fichier est détecté, il est envoyé à un autre équipement réseau FortiSandbox. Le logiciel de cet équipement reçoit les fichiers des différentes FortiGates du réseau, et les teste en les exécutant dans une machine virtuelle (VM) permettant de faire fonctionner différents systèmes d'exploitation. Si l'exécution dans la VM permet de détecter un comportement suspicieux, ou alors si un virus est détecté au sein de l'application, une nouvelle signature de virus est créée, et elle est envoyée aux logiciels anti-virus fonctionnant sur les ordinateurs du réseau.
Une FortiSandbox comporte un ensemble de VMs (appelé "VM pool") afin de pouvoir

[1] `https://docs.fortinet.com/uploaded/files/4312/fortigate-sandbox-inspection-60.pdf`

analyser plusieurs fichiers simultanément. Le temps pour analyser le fichier dépend du matériel de la FortiSandBox, et du nombre de VMs utilisées pour exécuter et scanner ce fichier. Par exemple, cela peut prendre entre 60 secondes et 5 minutes pour analyser complètement un fichier. Enfin, une FortiSandbox possède un système optionnel de filtrage en entrée afin d'éviter d'analyser certains fichiers ou de réduire les inspections faites sur les fichiers.



1. Un fichier suspicieux transite sur le réseau
2. Ce fichier est envoyé à la FortiSandbox pour analyse
3. Une nouvelle signature de virus est créée et un filtre d'URL est créé
4. Les mises à jour créées par la FortiSandbox sont poussées vers les logiciels antivirus des ordinateurs
5. Les PCs sous Windows qui utilisent l'anti-virus "FortiClient" reçoivent les mises à jours. Le PC qui a tenté de télécharger le fichier dangereux est mis en quarantaine.

3 Travail à réaliser

I. Hypothèses

1. Listez vos hypothèses, en ayant soin de séparer les hypothèses liées à l'environnement de celles liées à vos diagrammes de modélisation. [2 points]

II. Exigences

1. Faites le diagramme d'exigences. [3 points]

III. Analyse

1. Faites un diagramme de cas d'utilisation. [3 points]
2. Continuez l'analyse avec un diagramme d'activités. [3 points]
3. Fournissez deux scénarios d'exécution du système : un scénario nominal et un scénario utile mais non donné explicitement par la spécification, et donnant lieu à des traces non nominales. [5 points]

IV. Validation

1. Quelles sont les propriétés qu'il vous parait judicieux de prouver sur la conception du système ? (L'on ne vous demande pas de faire cette conception). Choisissez une de ces propriétés pour laquelle vous devez fournir la machine à états de l'observateur correspondant. [3 points]

Bonne chance !