Rapport de pré-étude

Pierre-Marie Airiau
Valentin Esmieu
Hoel Kervadec
Maud Leray
Florent Mallard
Corentin Nicole

6 octobre 2014

Table des matières

Introduction

Un long chemin a été parcouru depuis le 18 mars 1662, où le brillant penseur Blaise Pascal réalise la première expérience de transports en commun urbains au monde. Il s'agit alors de sept carrosses publiques qui sont mis en service entre la Porte Saint-Antoine et le palais du Luxembourg à Paris. Depuis lors, les transports en commun ont beaucoup évolué. Ils sont aujourd'hui indispensable au fonctionnement d'une ville. En témoigne ces chiffres impressionants : selon les estimations du Gart, 6.5 million de trajet sont réaliséés par jours en France.A Rennes, l'agglomération sur lequel se portera notre étude, la société Keolis dénombre une moyenne de 250 000 trajets par jour.

Nous comprenons donc aisément, l'importance que revêt le bon fonctionemment de ces transports en commun. Une paralysie de ces derniers aura une incidence considérable l'ensemble de la métropole.

De plus la concentration de la population dans les transports implique un dommage humain. conséquent en cas d'attaque létale.

Cette étude consistera à se placer en tant qu'attaquant, pour essayer de trouver les failles qui permettraient à une personne mal intentionnée de paralyser les transports en commun de Rennes métropole. Dans ce but nous utiliserons la théorie des arbres d'attaques de Bruce Schneier.

En paralléle de cette étude nous réaliserons une suite logicielle. Celle-ci aura pour finalité d'assister les experts en sécurité.

Chapitre 1

Contexte

Le bon fonctionement des transports en commun dépends de nombreux facteurs. Que ce soit des facteurs humains, ou bien technique, le moindre dysfonctionnement impactera le systéme entier très rapidement. Ainsi, un simple tour d'horizon de la presse internationale fait remonter très vite à la surface de nombreux cas de paralysie des transports publiques urbain dans le monde entier.

Parmi tout ces cas de paralysie, les plus marquant à l'échelle internationale sont ceux impliquant des dégats humains parmis les passagers. Il s'agit dans la plupart des cas d'attaque terroriste. Bien que relativement rare, le lourd bilan humain de ces attaques marque durablement les esprits.

C'est le cas de l'attentat à la bombe dans la gare Saint-Michel du train inter-urbain parisien, le 25 juillet 1995 qui provoqua la mort de 8 personnes. Mais aussi 7 juillet 2005

En France, il arrive aussi que les réseaux de transports en commun soient mis en difficulté. La plupart du temps, ces troubles sont dûs à des grèves du personnel pouvant refléter différentes réclamations. Ainsi, à Marseille en décembre 2013, les chauffeurs de bus protestent contre les salaires, la pénibilité en fin de carrière et la suppression de deux jours de congés. Cela est également arrivé à Lille en mai 2014, où le tramway et les bus sont bloqués par les traminotsqui demandent une hausse des salaires.

Mais parfois, les grèves sont la conséquence de certains incidents survenus lors des trajets : le plus souvent, il s'agit d'agressions sur le personnel. Ces dernières sont plus fréquentes qu'on ne pourrait le penser.

À Dunkerque en mai 2013 par exemple, un chauffeur subit une agression de la part de voyageurs, qui après leur exclusion du véhicule l'ont poursuivi en voiture jusqu'au terminus de la ligne. Arrivés là, équipés d'extincteurs, ils ont bloqué le bus et menacé ses occupants. La CGT a été avertie, une plainte a été déposée et les conducteurs ont exercé leur droit de retrait, paralysant ainsi le réseau de bus pendant toute une journée.

C'est ensuite à Douai, en septembre de la même année, que trois contrôleurs sont agressés lors d'un contrôle par une vingtaine de personnes. Des coups sont échangés, les trois hommes finissent à l'hôpital avec des contusions et une entorse au poignet pour l'un d'entre eux. L'ensemble des contrôleurs du réseau exerce alors son droit de retrait, paralysant celui-ci pendant une journée entière...

Mais qu'en est-il au sein de l'agglomération rennaise, qui nous intéresse tout particulièrement dans le cadre de ce projet ? Commençons par décrire le réseau de transports actuellement en place, ainsi que sa gestion.

À Rennes, il existe une ligne de métro (une deuxième est en construction) et un réseau de bus, les deux étant gérés par un organisme nommé le STAR (Service des Transports en commun de l'Agglomération Rennaise). Ce dernier a également mis en place depuis quelques années un système de vélos en libre-service, les vélos STAR. Les usagers peuvent accéder aux différents services du STAR par plusieurs moyens : en achetant des tickets à l'unité (pour bus et métro), en utilisant une carte d'abonné rechargeable (la carte Korrigo)... Dans certaines

stations de vélos STAR, ils peuvent même payer directement par carte bancaire. L'information aux voyageurs passe par 870 écrans dans les bus, 70 dans les stations de métro et 50 bornes d'informations voyageurs (BIV) dans les abribus. Le système d'aide à l'exploitation et à l'information des voyageurs (SAEIV) permet d'indiquer en temps réel le passage du prochain bus, les perturbations, les correspondances, la disponibilité des Vélos STAR... Ces données sont disponibles en open data, et consultables via un service mobile mis à disposition par le STAR.

Toute cette organisation n'est cependant pas à l'abri des incidents et présente quelques failles : voici un récapitulatif des paralysies les plus importantes que nous avons trouvées.

En juillet 2009, la ligne de métro est entièrement bloquée pendant près de 20h à la suite d'un violent orage provoquant l'inondation des voies de circulation. Ceci n'est certes pas une attaque volontaire mais cela reste une faiblesse du système qu'il nous a paru intéressant de relever.

C'est ensuite en avril 2012 que le réseau STAR entier est paralysé, en pleine heure de pointe, suite à l'agression d'un chauffeur. À l'époque, la direction recense 18 agressions depuis le début de l'année, et promet un redéploiement de ses agents de médiation et de prévention. Une mesure insuffisante pour la CFDT, qui réclame "une police dédiée aux transports".

Environ un mois plus tard, en mai, la ligne de métro est bloquée dès 5h30 du matin. Selon le STAR, il s'agirait d'un problème informatique entre le centre de commandement du métro et les rames. En clair, la liaison qui permet de contrôler les rames à distance ne fonctionne plus. Jamais un tel incident ne s'était produit. Un service de bus a été mis en place pour limiter les conséquences.

Ces quelques faits montrent bien l'importance de la mise en place d'une évaluation des risques, ainsi que d'un répertoire des défenses à utiliser pour contrer ces derniers.

Chapitre 2

État de l'art

2.1 Théorie des arbres d'attaque et de défense

Le concept des arbres d'attaques a été créé en 1999 par Bruce Schneier, un expert américain en securité informatique qui est parti du constat que des systèmes réputés "inviolables" se font briser en permance non pas en passant au travers des défenses mises en place, mais par des méthodes d'accès qui n'avaient pas été imaginées par ses concepteurs car ils n'avaient pas les outils pour dresser une liste exhaustive des manières d'attaquer leur système. Il a donc créé le concept des arbres d'attaque dans ce but : pouvoir réaliser un inventaire exhaustif des méthodes d'attaque sur un système, quel qu'il soit, afin de pouvoir en concevoir la défense de la manière la plus complète possible.

Lors de ces recherches, Mr Schneier a retenu un formalisme prècis : Une représentation des menaces sous la forme d'arbres. Ces arbres sont réalisés en se posant la question suivant : Si je veux atteindre tel objectif, qu'est ce que cela pré-suppose que j'accomplisse d'abord ? Pour cela, on représente l'objectif final en haut de l'arbre, et l'on ajoute en descendant dans l'arbre les objectifs intérmédiaires (noeuds) plus simples à réaliser, qui nous garantissent l'accomplissement de l'objectif principal. L'on fait ensuite découler de ces objectifs intermédiaires d'autres objectifs les validant, etc... jusqu'à avoir en bas de l'arbre des actions simples (feuilles). Ensuite, il suffit de descendre dans l'arbre à partir d'un noeud pour savoir quelles sont les combinaisons d'actions possibles à effectuer pour atteindre le noeud.

L'arbre suivant illustre ce formalisme :

Depuis 1999, le concept a évolué grâce à la contribution de personnes ayant étendu et amélioré le concept de Mr Schneier : Barbara Kordy, Sjouke Mauw, Saša Radomirović, Patrick Schweitzer. Ces personnes ont en pareticulier étendu le concept d'arbre d'attaque à celui d'arbre de défense, où sont également reprséntés les defenses mises en place et que le potentiel attaquant aura besoin de désactiver pour atteindre son but. Un formalisme existe aussi pour ces types d'arbres ADT (Attack Defense Tree), où les defense sont représentés dans des rectangles et liés avec des pointillés. Le même arbre que précedemment avec des défenses ressemble à cela :

2.2 Implémentations des ADT

Plusieurs logiciels implémentant le concept des ADT ont été développés. Voici les principaux : Logiciels propriétaires :

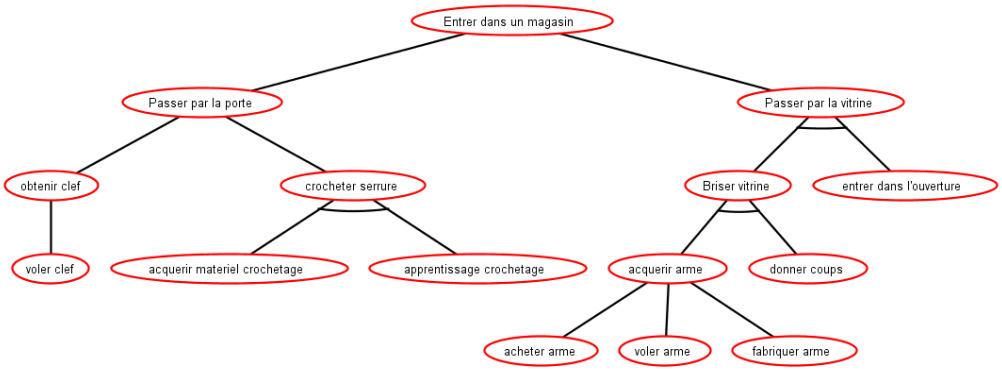
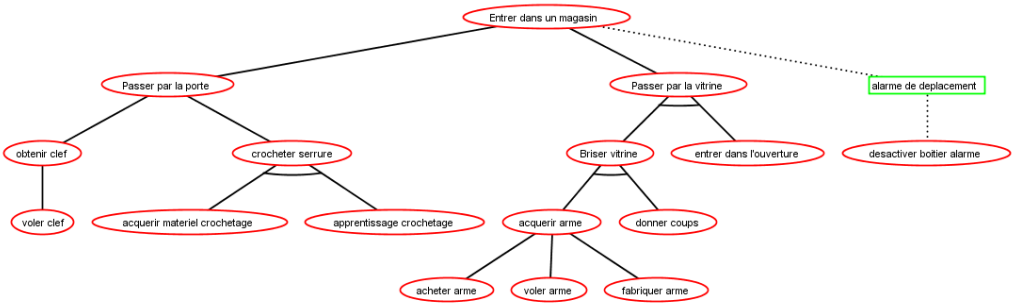


FIGURE 2.1 – C'est tres bien



— SecurlTree
— ATTACKTREE+

Logiciels Open-Source :
— ADTool

Chapitre 3

Cahier des charges

L'objectif principal de ce projet est de réaliser une suite logicielle, permettant à un utilisateur novice dans le domaine des arbres d'attaque défense et de la sécurité en général, d'évaluer les risques d'attaque sur son système.

Notre suite contiendra :
— Une bibliothèque de modèles d'attaques existantes.
— Base de valeurs.
— D'un guide (plus ou moins interactif) pour partir de zéro, même novice.
— Un editeur d'arbres.

3.1 Bibliothèque d'attaques

La bibliothèque d'attaques servirait à décrire des cas très généraux, que l'utilisateur pourrait détailler en fonction de sa situation.

Dans notre exemple (la STAR), nous pourrons fournir des arbres d'attaque de réseaux de transport communs à toutes les villes de France, que nous pourront ensuite détailler pour la ville de Rennes.

3.2 Base de valeurs

Le but de la base de valeurs serait de fournir d'aider l'utilisateur à valuer ses noeuds, et lui permettre d'enregistrer des valeurs qui reviennent souvent.

3.3 Guide interactif

Le guide doit être capable d'expliquer à l'utilisateur comment faire son analyse.

Il pourra par exemple poser une série de questions à l'utilisateur, afin de générer un arbre dit "de base" sur lequel l'utilisateur pourra commencer son analyse.

Chaque notion devra être expliquée de manière claire et concise.

Découper l'analyse en différentes étapes.

3.4 Éditeur d'arbres

L'éditeur d'arbre sera l'outil AD Tool[1], auquel nous rajouterons quelques fonctionnalités **(lesquelles ?)** pour rendre l'édition des arbres plus souple.

3.5 Multiplateforme

Disscuss : Intérêt du multiplateforme.

Pro :
— Ne limite pas l'utilisateur dans son choix d'OS.
— AD Tool est déjà multiplateforme.
Cons :
— Plus technique à réaliser.

3.6 License

GPL ? MIT ? BSD ? WTF ?

Déterminer ce que l'on veut pour notre projet.

Vérifier aussi license de AD Tool.

1. Développé par...

Chapitre 4

Outils

Voici une description des différents outils que nous allons utiliser pour développer notre projet.

4.1 Outils collaboratifs

Afin de versionner efficacement notre projet, nous avons décidé d'utiliser **Git** pour travailler comme des professionnels.

Pour le partage de fichiers lourds et l'édition de comptes-rendus de réunion, **GoogleDrive** s'est imposé comme le leader mondial de l'univers.

Enfin, pour la plannification, **MS Project** nous est imposé.

4.2 Langages de programmation

Etant donné que nous souhaitons réaliser une suite logicielle, la communication entre les différents programmes doit pouvoir se faire facilement.

	Java	**C++**	**C#**
Avantages	azerty	azerto	truc
Inconvénients	azerty	zfdsfs	dwfgdf

Après réflexion, on va prendre ce langage là. Par conséquent, on va utiliser **Visual Studio** pour développer à l'aise.

4.3 Interfaces graphiques

Afin de garantir un confort d'utilisation optimal pour des utilisateurs novices, on va fait de belles interfaces. GUI : WinForm WMA GTK+ Qt

Chapitre 5

Plannification et organisation

Durant nos six premières heures de projet, nous avons beaucoup discuté de notre organisation avec nos encadrants. Il a ainsi été décidé que les rôles seraient les suivants :

Coordinateur Le coordinateur s'occupe de planifier les réunions de projet, de les animer et est le contact des encadrants. Son rôle est aussi de s'assurer de l'avancée des rapports et de leur relecture. Il changera régulièrement afin que tout le groupe assure ce rôle. Hoël est le premier coordinateur, jusqu'à la livraison de ce rapport.

Sysadmin L'administrateur système s'occupe de maintenir à jour les plate-formes et outils utilisés durant le projet (GitHub, GoogleDrive). Valentin est en charge de ces plate-formes.

Scribe Un scribe est volontaire à chaque début de réunion afin de prendre les notes. Ce rôle est communément assuré par les personnes disposant de leur ordinateur à l'INSA afin de rédiger un compte-rendu en direct sur le GoogleDrive.

Nous nous sommes également familiarisés avec l'outil ADTool, développé par l'équipe de Barbara Kordy, ainsi qu'avec des cours sur la théorie des arbres. Nous avons aperçus des points d'amélioration que nous serons peut-être amenés à implémenter afin de rendre son utilisation plus complète.

Après cette introduction à ADTool, nous avons jugé utile un cours de cryptographie, afin de mieux saisir les protocoles de communication sécurisée. Gildas Avoine nous a donc dispensé ce cours durant deux heures de notre temps libre. Cela nous a permis d'appréhender les concepts de protection des cartes Korrigo, qui nous serons sûrement amenés à analyser dans le cadre d'une paralysie de la STAR.

Chapitre 6

Risques

Nous pouvons d'ores et déjà envisager des situations dans lesquelles nous ne serions pas en mesure de livrer le projet dans l'état que nous avions prévu en ce début d'année scolaire. Le facteur principal est bien entendu humain. En effet, la moitié du groupe partant étudier à l'étranger dans le cadre de la mobilité internationale. Il se peut que nous ayons légèrement sur-estimé nos capacités de travail et annoncé une tâche trop difficile à exécuter.

Des problèmes d'ordre technique peuvent également survenir. Des difficultés à mettre en place la chaîne logicielle prévue, des soucis de langage utilisée ou encore de compatibilité sont de l'ordre du possible.