INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

Glasir

Application au réseau STAR

Manuel utilisateur

Table des matières

Bienvenue dans le manuel utilisateur de Glasir, un logiciel d'aide aux experts en sécurité basé sur le formalisme des ADTrees [1] [2]. Grâce à Glasir, vous pourrez analyser efficacement vos ADTrees préalablement créés avec ADTool [1], un logiciel open source disponible sur Internet à l'adresse `http://satoss.uni.lu/members/piotr/adtool/`.

Ce manuel commencera par décrire le fonctionnement général du logiciel (création d'un nouveau projet, ouverture d'un projet existant, etc.), avant d'expliquer comment prendre en main les trois fonctionnalités principales que sont l'Éditeur de fonctions, le Filtre et l'Optimiseur.

Après cela, dans la SECTION 2 vous trouverez des détails concernant l'utilisation d'ADTool, et principalement sur les nouveautés qui lui ont été ajoutées lors de ce projet.

1. Abréviation d'« Attack-Defense Trees », ou « Arbres d'Attaque et de Défense » en français.

1 Glasir

Glasir est un logiciel d'analyse en sécurité open source, développé pour Windows. Il est fourni sous forme d'exécutable (fichier Glasir.exe) et accompagné d'un dossier contenant des exemples d'ADTrees sous format XML que vous pouvez utiliser pour débuter. Pour lancer le logiciel, veuillez double-cliquer sur Glasir.exe. Si vous rencontrez un souci dès cette étape, merci de lire le fichier ReadMe.txt joint au dossier de téléchargement de Glasir.

Agencement général de la fenêtre Lorsque vous démarrez Glasir, la fenêtre présentée sur la FIGURE 1 s'affiche. Voici une description rapide des éléments que vous trouverez dans cette fenêtre :

- la barre de menu située en haut vous permet d'ouvrir des ADTrees, de sauvegarder des projets, ou encore d'obtenir des indications si vous avez besoin d'aide ;
- le bloc central vous permet d'accéder à l'Éditeur de fonctions (*FunctionEditor*), au Filtre (*Filter*) et à l'Optimiseur (*Optimize*) ;
- la ligne de texte en-dessous du bloc central met en évidence l'ADTree sur lequel vous travaillez. Au démarrage, comme aucun ADTree n'est ouvert, le message « No ADTree selected » est affiché ;
- le bloc en bas, surmonté du message « ADTrees available », indique quels sont les ADTrees appartenant au projet courant. Ce bloc est vide au démarrage car aucun projet n'est ouvert ;
- la case cochable *Show complete path*, tout en bas, permet d'afficher le chemin complet des ADTrees listé dans le bloc situé au-dessus.

Nous allons maintenant détailler le fonctionnement de chacune des fonctionnalités de Glasir.

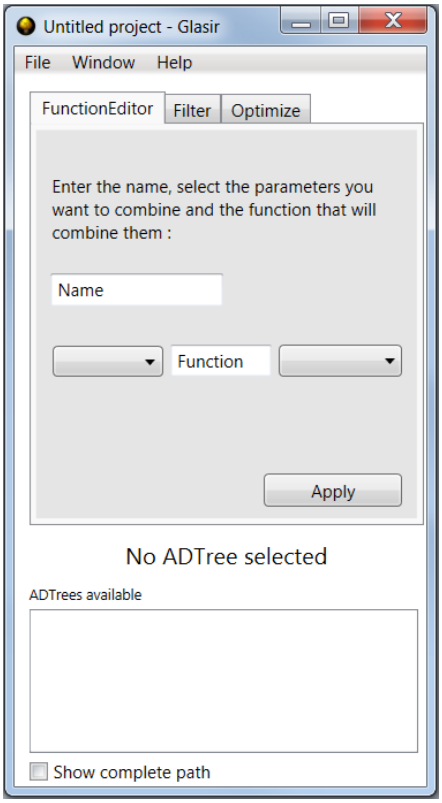

FIGURE 1 – Fenêtre principale s'affichant au démarrage de Glasir.

Ouvrir un ADTree Pour ouvrir un ADTree, cliquez sur le bouton *File* situé tout en haut à gauche, dans la barre de menu. Puis, dans le menu déroulant, cliquez sur *Open ADTree File*, comme indiqué sur la FIGURE 2. Une boîte de dialogue apparaît : parcourez vos dossiers pour sélectionner l'ADTree que vous souhaitez ouvrir. Notez que seuls les ADTrees au format XML générés par ADTool (consulter SECTION 7 du manuel utilisateur d'ADTool [3]) peuvent être analysés par Glasir. Il n'est cependant pas possible d'utiliser des arbres réalisés avec une autre version d'ADTool que celle de Glasir. Une fois l'ADTree sélectionné, cliquez sur le bouton *Open* de la boite de dialogue. ADTool se lance alors pour afficher votre ADTree. Notez qu'au démarrage, cette opération peut prendre quelques secondes. Une fois ADTool lancé, Glasir se présente sous la forme de plusieurs fenêtres, comme indiqué sur la FIGURE 3. Si la fenêtre d'ADTool ne s'affiche pas au bout d'une minute ou qu'un autre programme qu'ADTool se lance, cela signifie que vos fichiers *.jar* ne sont pas associés à Java (ou que vous ne possédez pas Java). Consultez et suivez les étapes du fichier *ReadMe.txt* (en anglais) fourni avec Glasir pour obtenir des informations supplémentaires et corriger le problème.

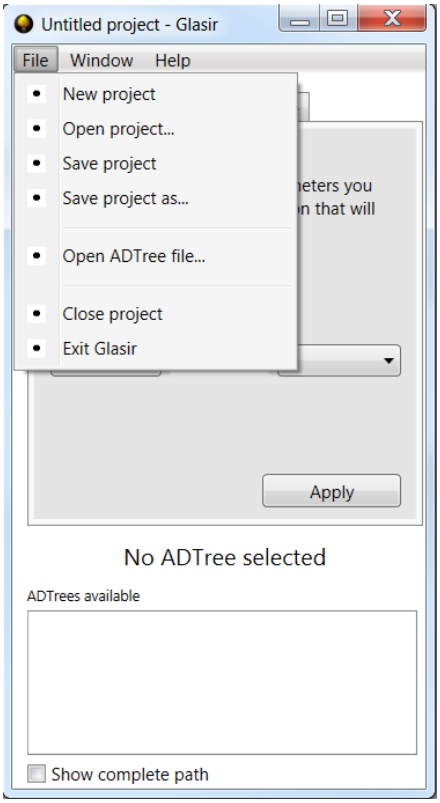

FIGURE 2 – Menu déroulant disponible en cliquant sur le bouton *File* de la barre de menu.

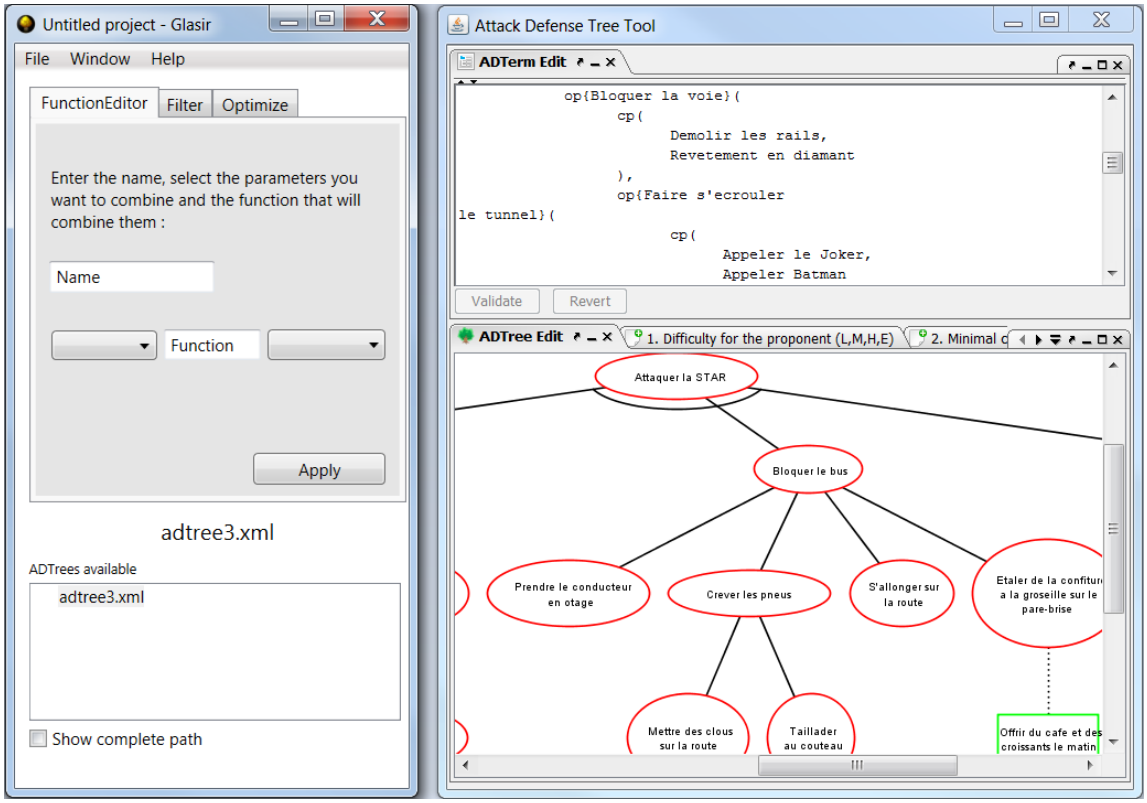

FIGURE 3 – Fenêtres visibles après ouverture d'un ADTree.

Enregistrer un projet Lorsque vous avez ouvert un ou plusieurs ADTrees, vous avez la possibilité de sauvegarder l'état actuel de votre projet, c'est-à-dire la liste des ADTrees ouverts. Pour ce faire, cliquez sur *File*, puis sur *Save project as* pour choisir l'emplacement où enregistrer le fichier du projet. Donnez-lui un nom, puis cliquez sur le bouton *Save* de la boite de dialogue. Une fois ceci fait, le titre de la fenêtre de Glasir portera alors le nom de votre projet. Vous pourrez par la suite cliquer directement sur *Save project* pour enregistrer vos modifications.

Ouvrir un projet Si vous avez déjà un projet enregistré, c'est-à-dire un fichier avec l'extension *.glpf* (*Glasir Project File*), vous pouvez recharger ce fichier : cliquez sur *File*, puis *Open project*. Parcourez vos dossiers pour retrouver votre fichier de projet, sélectionnez-le, puis cliquez sur le bouton *Open* de la boite de dialogue. Si vous aviez un projet ou des ADTrees ouverts, ils seront fermés pour que votre projet enregistré puisse être ré-ouvert. Notez que toute modification non-sauvegardée ne sera pas enregistrée lors de la fermeture.

Aide Si vous avez des problèmes avec le lancement d'ADTool, vous pouvez cliquer sur le bouton *Help* de la barre de menu pour obtenir des informations supplémentaires. Nous vous invitons aussi à suivre les consignes indiquées dans le fichier *ReadMe.txt* (en anglais) fourni avec Glasir.

Changer d'ADTree courant Pour pouvoir utiliser les modules de Glasir, vous devez sélectionner un ADTree courant, sur lequel les opérations des modules seront appliquées. Le bloc en bas de la fenêtre principale dresse la liste des ADTrees de votre projet. Vous avez la possibilité de cocher la case *Show complete path*, en bas, pour voir le chemin complet de chaque ADTree. Cliquez sur un ADTree dans la liste pour qu'il devienne l'ADTree courant. Son nom est alors indiqué à la ligne du dessus, en plus gros. Si aucun ADTree n'est disponible ou sélectionné, le message « No ADTree selected » est affiché à la place. Notez que lorsqu'un nouvel ADTree est ouvert, ce dernier devient automatiquement l'ADTree courant.

Éditeur de fonctions Cette fonctionnalité a pour intérêt d'exprimer un compromis entre deux valuations d'un ADTree en en créant une troisième, fonction des deux premières. Par exemple, si vous avez un ADTree qui a comme paramètres « Minimal cost for the proponent »(en euros) et « Minimal time for the proponent (sequential) »(en heures) et que vous estimez qu'une heure « coûte »par comparaison 20 euros, vous pouvez créer un nouveau paramètre de type « Minimal cost for the proponent »exprimant un compromis entre les deux paramètres qui sera égal à coût+20*temps.

ATTENTION : le nouveau paramètre aura pour type celui du premier paramètre sélectionné (à gauche), par exemple si le premier paramètre est de type « Minimal time for the proponent (sequential) », alors le nouveau paramètre calculé le sera aussi. Si vous sélectionnez un paramètre de type discret, un nombre de cases égal au nombre valeurs possibles s'affichera. Vous pourrez alors pondérer ces valeurs de la plus petite (à gauche), à la plus grande (à droite).

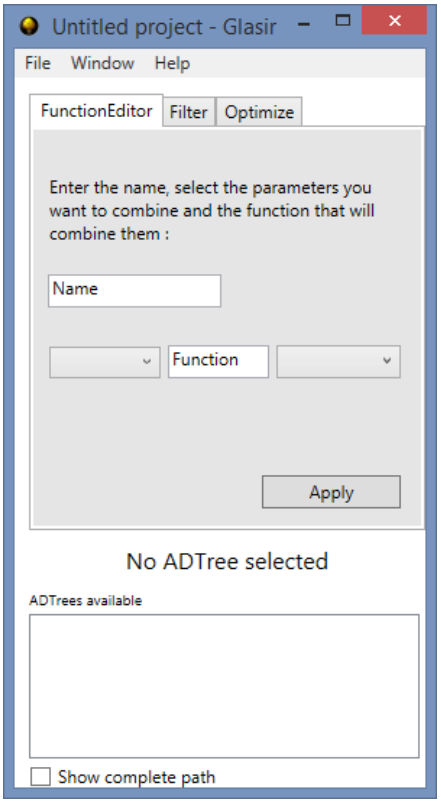

FIGURE 4 – Onglet FunctionEditor.

Pour utiliser l'Éditeur de fonctions, suivez les étapes suivantes :

- Assurez-vous que l'ADTree que vous voulez utiliser est ouvert et désigné comme l'arbre courant ;
- Sélectionnez l'onglet « FunctionEditor » (voir FIGURE 4) ;
- Sélectionnez les deux paramètres de l'ADTree que vous voulez combiner au moyen des deux ComboBox présentes dans l'onglet ;
- Inscrivez dans la textBox « Function » la fonction que vous voulez utiliser pour le calcul du nouveau paramètre. Par exemple, si vous voulez faire « newParam = firstParam + 2*second-Param », inscrivez « +2* » ;
- Entrez le nom que vous voulez donner au nouveau paramètre créé dans la TextBox « Name » ;
- Enfin, cliquez sur le bouton « Apply » pour créer le nouveau paramètre.

S'ouvrira alors un nouvel arbre dans une nouvelle fenêtre d'ADTool, qui sera nommé comme l'arbre initial suivi de « .functEdit » . Le nouvel ADTree sera enregistré par défaut dans le répertoire où se trouve le logiciel Glasir, mais rien ne vous empêche par la suite de le déplacer. Si un problème survient, l'exécution sera stoppée et une boite de message apparaîtra pour vous donner les raisons de l'interruption.

Filtre Cette fonctionnalité sert à élaguer les chemins d'un ADTree qui ne respectent pas une certaine condition. Par exemple, l'ADTree présenté à la FIGURE 5 a comme paramètre « Minimal cost for the proponent »(en euros) : si l'on cherche à identifier les chemins que pourrait emprunter un attaquant potentiel qui ne peut pas dépenser plus de 300 euros, le Filtre permettra alors d'élaguer l'ADTree pour respecter cette condition. L'élagage sera ainsi fait de manière à ne conserver que les feuilles de l'arbre qui apparaissent dans au moins un chemin permettant d'accomplir l'attaque avec 300 euros ou moins. Ce qui conduira à l'arbre présenté à la FIGURE 6

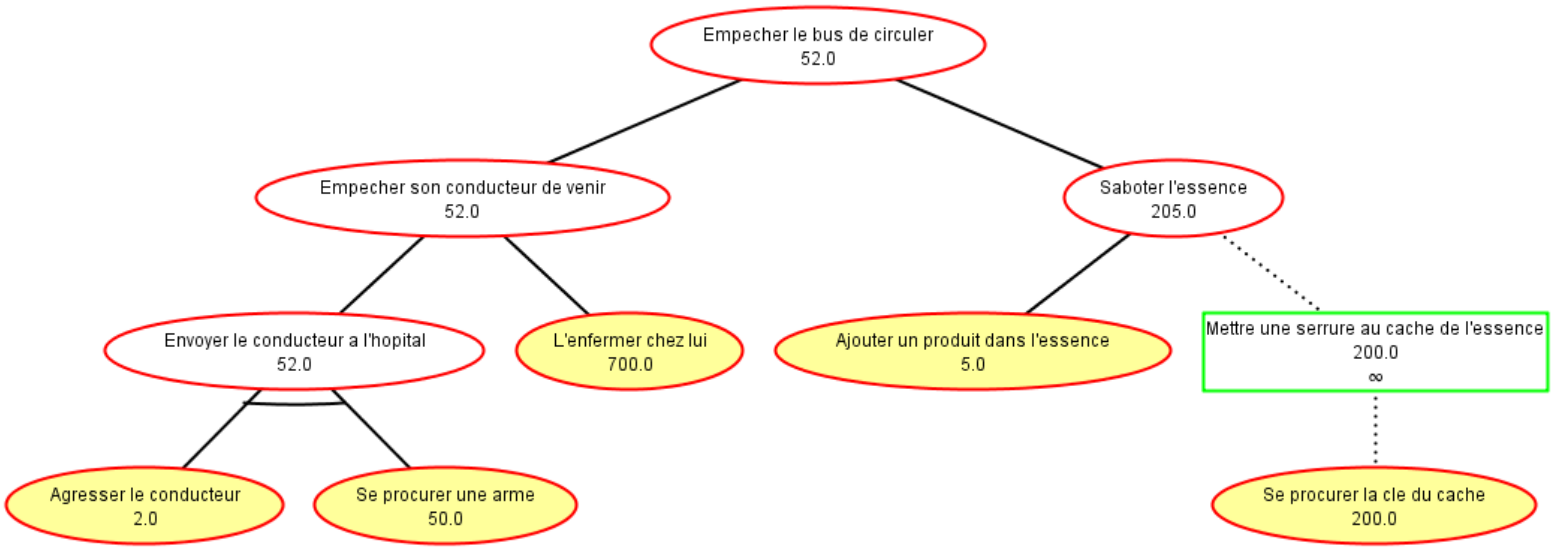

FIGURE 5 – ADTree d'origine.

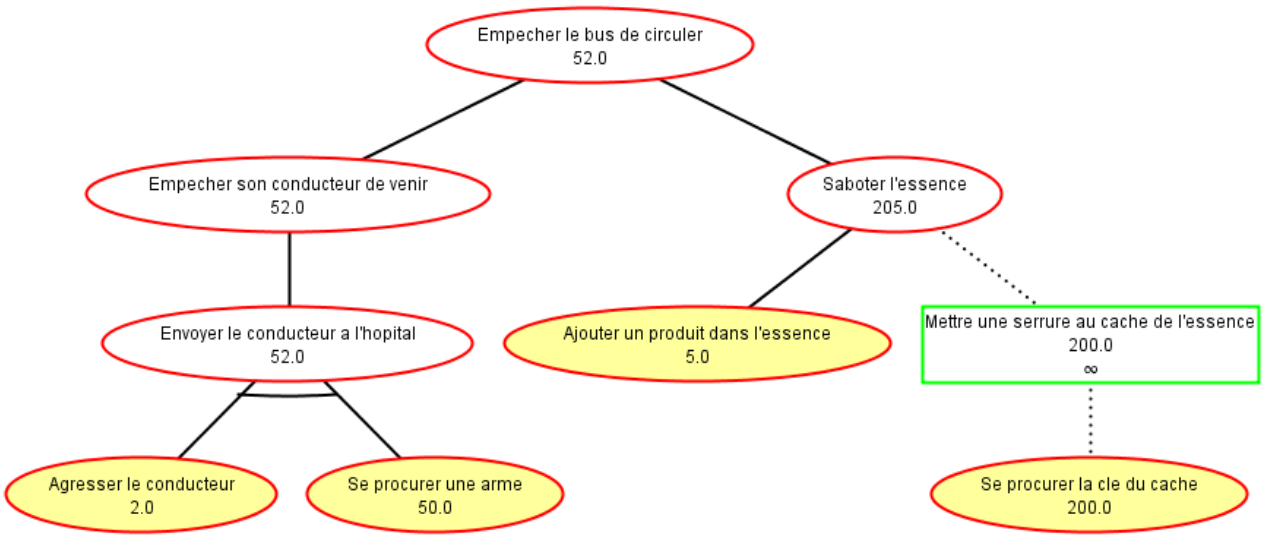

FIGURE 6 – ADTree après filtrage.

L'onglet permettant d'utiliser le filtre dans Glasir est présenté à la FIGURE 7 :

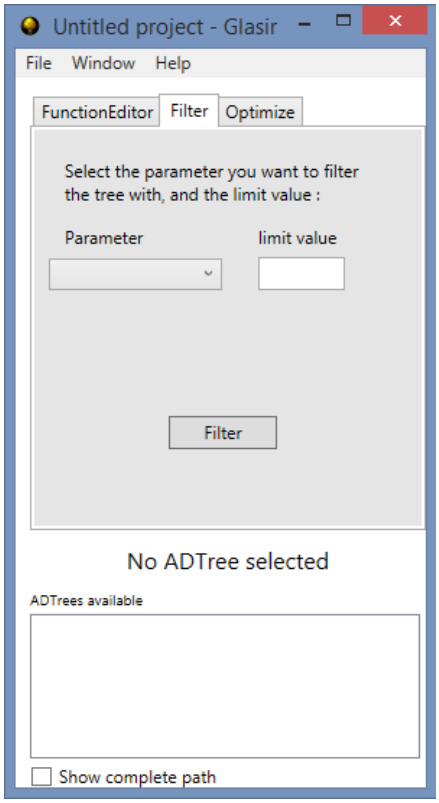

FIGURE 7 – Onglet Filter.

Pour utiliser le Filtre, suivez les étapes suivantes :

- Assurez-vous que l'ADTree que vous voulez filtrer est ouvert et désigné comme l'arbre courant ;
- Sélectionnez l'onglet « Filter » (voir FIGURE 7) ;
- Sélectionnez le paramètre selon lequel vous voulez filtrer l'arbre, grâce à la ComboBox présente dans l'onglet ;
- Indiquer dans la textBox « Limit Value » la valeur limite acceptable (min ou max selon les cas) par le Filtre pour le paramètre sélectionné. Vous pouvez rentrez une valeur textuelle correspondant à l'une des valeurs de l'ensemble du paramètre si l'ensemble est discret ;
- Enfin, cliquez sur le bouton « Filter ».

S'ouvrira alors un nouvel arbre, correspondant à l'arbre élagué, dans une nouvelle fenêtre d'ADTool. Il sera nommé comme l'arbre initial, suivi de « .filter ». Le nouvel arbre sera enregistré par défaut dans le répertoire où se trouve Glasir, mais rien ne vous empêche de le déplacer par la suite. Si un problème survient, l'exécution sera stoppée et une boite de message apparaîtra pour vous donner les raisons de l'interruption.

Optimiseur Cette fonctionnalité sert à élaguer les chemins d'un ADTree de manière a ne conserver que le(s) meilleur(s) chemin(s) selon un paramètre donné. Par exemple avec l'arbre de la FIGURE 5, l'arbre optimisé obtenu selon le paramètre « Minimal cost for the proponent »(en euros) ne conservera que les feuilles de l'arbre qui apparaissent dans au moins un chemin permettant à l'attaquant d'accomplir l'attaque avec 52 euros seulement. Le résultat est l'ADTree de la FIGURE 8

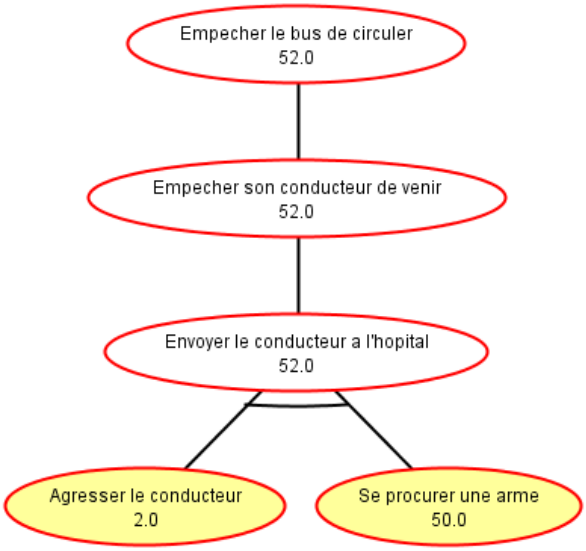

FIGURE 8 – ADTree après optimisation.

L'onglet permettant d'utiliser l'optimiseur dans Glasir est présenté à la FIGURE 9 :

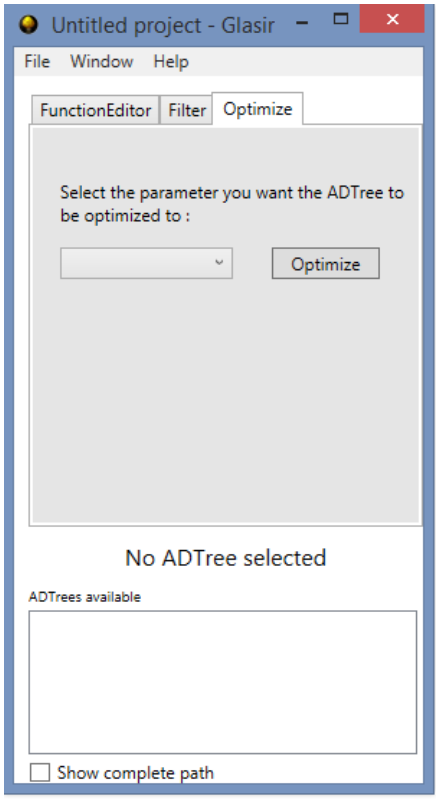

FIGURE 9 – Onglet Optimize.

Pour utiliser l'Optimiseur, suivez les étapes suivantes :

- Assurez-vous que l'ADTree que vous voulez filtrer est ouvert et désigné comme l'arbre courant ;
- Sélectionnez l'onglet « Optimize » (voir FIGURE 9) ;
- Sélectionnez le paramètre selon lequel vous voulez optimiser l'arbre, avec la ComboBox présente dans l'onglet ;
- Enfin, cliquez sur le bouton « Optimize ».

S'ouvrira alors un nouvel arbre correspondant à l'arbre élagué dans une nouvelle fenêtre d'ADTool, qui sera nommé comme l'arbre initial suivi de « .Optimizer ». Le nouvel arbre sera enregistré par défaut dans le répertoire où se trouve Glasir, mais rien ne vous empêche de le déplacer par la suite. Si un problème survient, l'exécution sera stoppée et une boite de message apparaîtra pour vous donner les raisons de l'interruption.

2 Nouvelles fonctionnalités d'ADTool

Pour le fonctionnement basique d'ADTool, vous pouvez vous référer au manuel utilisateur officiel [3] disponible sur Internet [2]. Le guide ici présent ne détaillera que l'utilisation des nouvelles

2. Voir à l'adresse suivante : http ://satoss.uni.lu/members/piotr/adtool/manual.pdf

fonctionnalités d'ADTool, qui sont le copier/couper/coller ainsi que l'annulation d'une action.

Copier/couper/coller Ces fonctionnalités vous seront utiles si vous désirez couper/copier un sous-arbre de l'ADTree courant afin de le coller ensuite à un autre emplacement dans ce même ADTree. Il est à noter que le sous-arbre coupé/copié sera ajouté en tant que fils du nœud auquel il sera collé. Aussi, la racine du sous-arbre coupé/copié doit être du même type (opponent ou proponent) que son futur nœud parent. Pour couper/copier un sous-arbre puis le coller, suivez les étapes suivantes :

1. Sélectionnez à l'aide d'un clic gauche le nœud racine du sous-arbre que vous désirez couper/copier. Si vous avez déjà sélectionné un nœud dans l'arbre, vous pouvez également vous déplacer jusqu'au nœud souhaité à l'aide des flèches (haut, bas, gauche, droite) du clavier.
2. Effectuez un clic droit sur le nœud sélectionné. Un menu déroulant doit apparaître à côté du nœud sélectionné, comme sur la FIGURE 10.
3. Sélectionnez l'option « Copy Subtree »/« Cut Subtree ») dans le menu déroulant. Vous pouvez également effectuer cette étape à l'aide d'un raccourci clavier, CTRL+C/CTRL+X.
4. Effectuez un clic droit sur le nœud auquel vous voulez coller le sous-arbre coupé/copié, puis sélectionnez dans la liste déroulante « Paste Subtree as Child ». Si cette option n'apparaît pas dans le menu déroulant, c'est que vous n'avez pas préalablement coupé/copié de sous-arbre. Vous pouvez ici encore utiliser un raccourci clavier, CTRL+V.

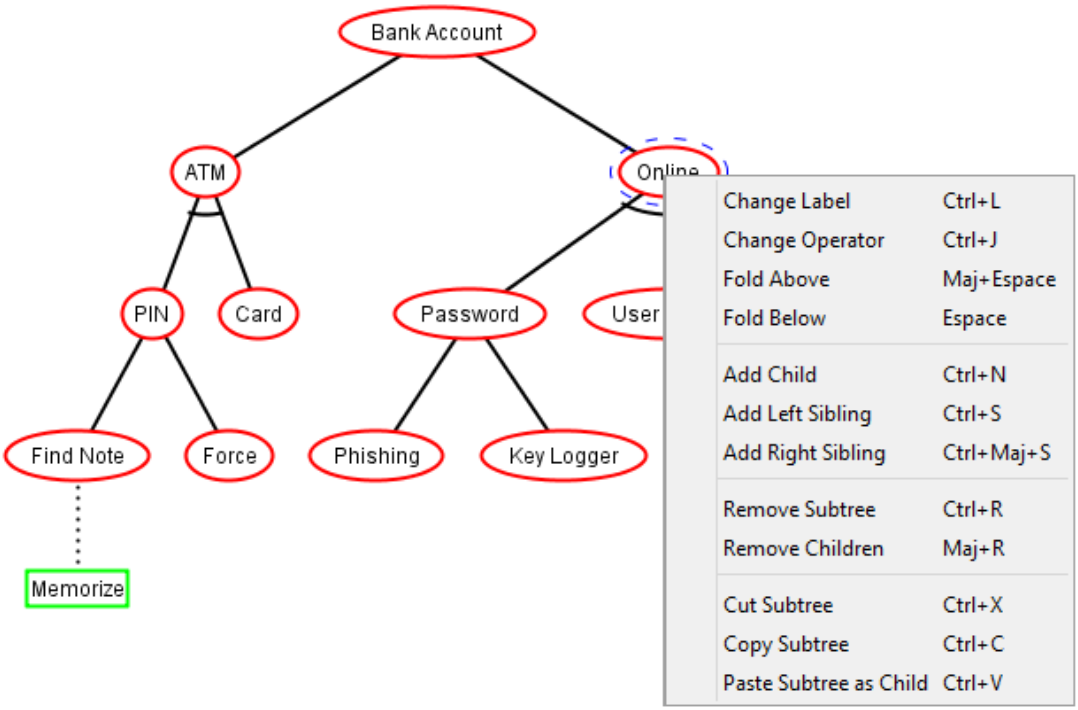

FIGURE 10 – Menu déroulant apparaissant après un clic droit sur un nœud.

Annulation d'une action Il s'agit ici d'annuler une ou plusieurs action(s) effectuée(s) précédemment sur l'ADTree courant. Pour cela, il vous suffit tout simplement d'utiliser le raccourci clavier CTRL+Z autant de fois que nécessaire, jusqu'à retrouver l'état souhaité pour l'ADTree.

Vous pouvez également cliquer sur l'icône « Undo last action (CTRL+Z) » en haut à gauche de la fenêtre principale d'ADTool, encadrée en rouge sur la FIGURE 11. Les actions pouvant être annulées sont les changements de labels, les ajouts ou suppressions de nœuds, les changements d'opérateur (conjonction ou disjonction) ainsi que les actions de couper/copier/coller.

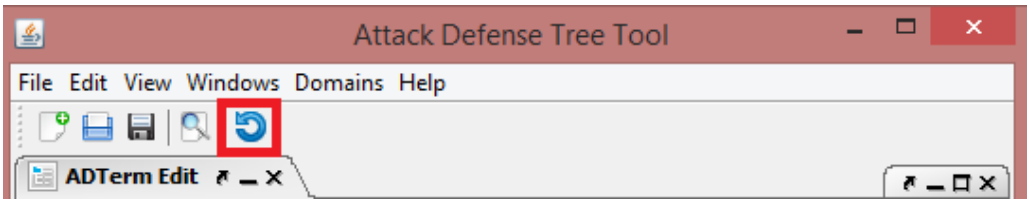

FIGURE 11 – Icône permettant d'annuler l'action précédente.

Références

[1] Barbara Kordy, Piotr Kordy, Sjouke Mauw, and Patrick Schweitzer. ADTool : Security Analysis with Attack–Defense Trees. In Kaustubh R. Joshi, Markus Siegle, Mariëlle Stoelinga, and Pedro R. D'Argenio, editors, *QEST*, volume 8054 of *LNCS*, pages 173–176. Springer, 2013.

[2] Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer. Attack–Defense Trees. *Journal of Logic and Computation*, 24(1) :55–87, 2014.

[3] Piotr Kordy and Patrick Schweitzer. The ADTool Manual. `http://satoss.uni.lu/software/adtool/manual.pdf`, 2012.

INSA Rennes
20 Avenue des Buttes de Coësmes
CS 70839
35708 Rennes Cedex 7

Tél. +33 (0) 2 23 23 82 00
Fax +33 (0) 2 23 23 83 96

www.insa-rennes.fr

INSA

UNIVERSITÉ EUROPÉENNE DE BRETAGNE

Commission des Titres d'Ingénieur

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE