Projet OptiTool
CR Réunion 3.1– 24/09/18

Contenu de la réunion :

- Explication de la conversion d'un arbre d'attaque et de défense graphique en sémantique.
- Point sur les items du plan + ordonnancement des items

A faire pour la semaine prochaine :

- Faire la table des matières (+ faire des points pour chaque partie et chaque sous-partie détaillant le contenu, les illustrations …)
- Vérifier la compilation d'ADTool
- Ajouter Barbara au Git
- Continuer d'analyser le code d'ADTool + DAGSolver (et envoyer les questions techniques dès que possible si besoin!)
- Créer le document Latex et le partager avec les membres de l'équipe et Barbara
- Envoyer l'ordre du jour de la prochaine réunion durant le week-end

---

Explication de la conversion d'un arbre d'attaque et de défense graphique en sémantique.

Defense strategy D = a sum of defense vectors *(ex : Ø, {d_1, d_2})*

Attack strategies A = a minimal set of actions of the attacker such that there exists a defense strategy D of the defender for which the execution of A achieves the root goal. *(ex : {a} pour D = Ø, {b,c,e} pour D = {d_2})*

Attention, la méthode expliquée dans la figure page suivante pour construire l'ensemble A peut ne pas marcher s'il y a une duplication d'actions (a a deux endroits par exemple – a à la place de e).

Defense semantic:

Méthode 1

(A,D) with A an attack strategy and D a defense strategy countering A (minimal set)

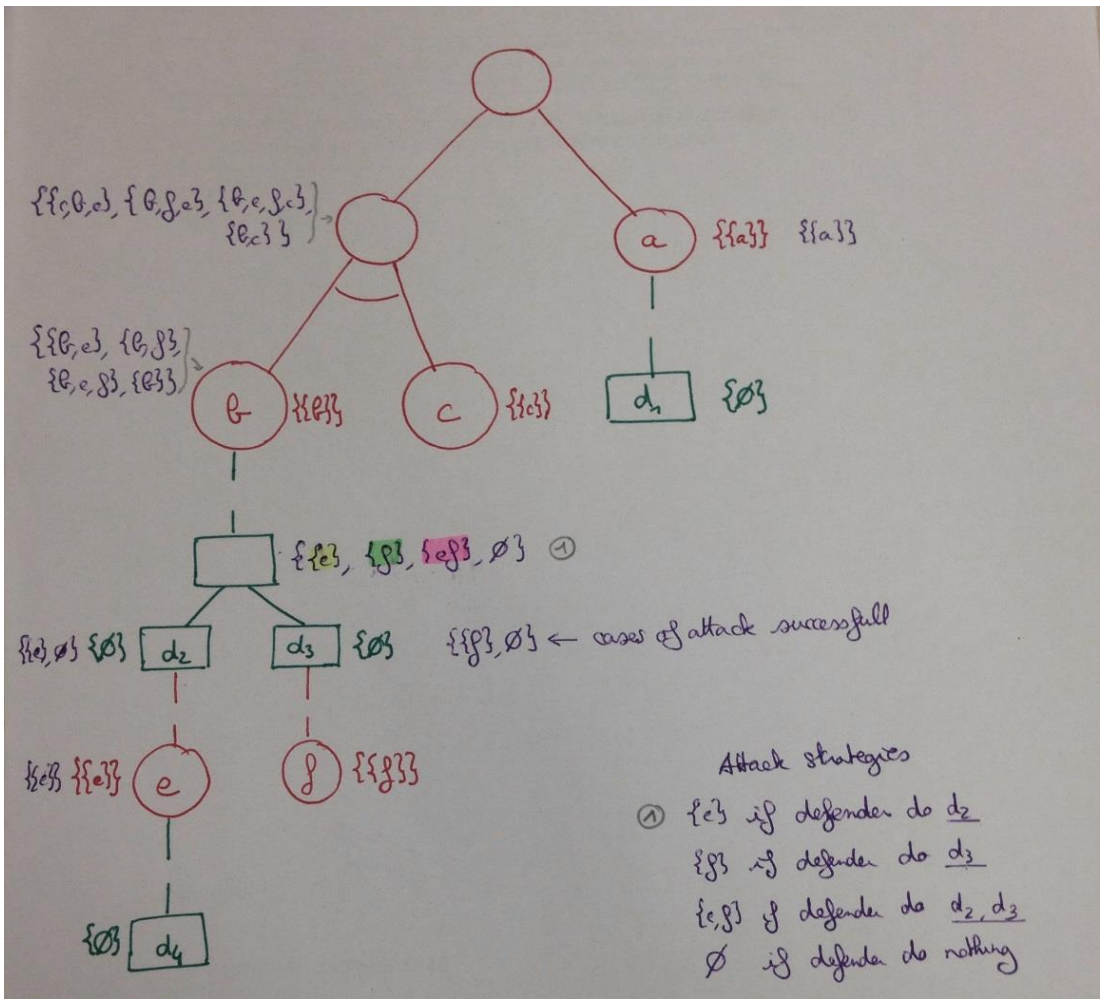
DefSem (T) = { ({a}, {d_1}) , ({b,c,e},{d_3}) , ({b,c,e},{d_2,d_4}) , …)

For A ∈ AttackSem(T)

A = {b,c,e}

1. {b,c} //noeuds les plus hauts
2. {b,c} : {d_2}
   {d_3}
3. DefenseSementics(T) ⟵ (A, {d_3})
4. ({b,c},{d_2})
5. Candidates = ({e},{d_2})
6. ({e},{d_2,d_4})
7. DefenseSementics(T) ⟵ (A, {d_2, d_4})

Attention, cette méthode peut ne pas marcher s'il y a une duplication d'actions (d1 a deux endroits par exemple).



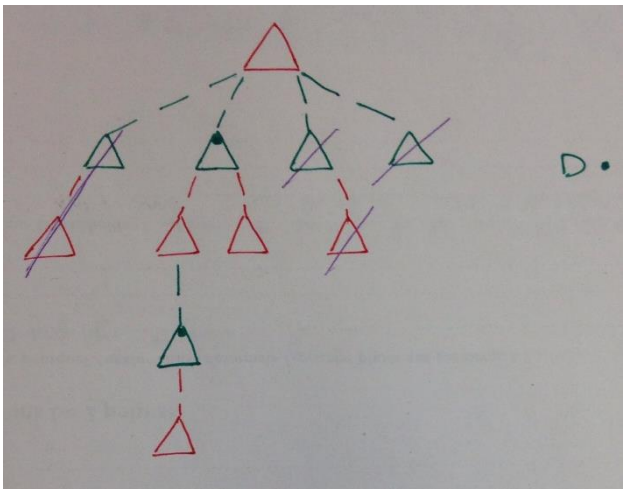
Méthode 2 (en cas de duplication) :

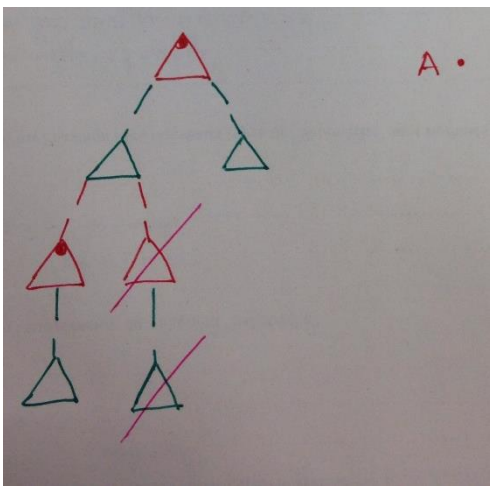
Attack Strategy → for D ∈ DefenseStrategy(T) : determine the attack strategy achieving the root goal when D is in phase

1. Pruning
2. Get A's counters D

Defense Semantic → for A ∈ AttackStrategy(T) : determine minimum sets D such that D counters A.

1. Pruning
2. Get D's counters A





Point sur les items du plan + ordonnancement des items

1. Contexte du projet (cf description du projet dans le poly – problèmes de sécurité, budget limité - + motivation papier Barbara/W)
2. Objectifs du projet (court + mis en valeur + ajouter utilisateur = expert en cybersécurité)
3. Présentation de l'optimisation linéaire (cf papier, livre de maths + parler investment et corevage ?)
4. Présentation des arbres d'attaques et de défense (mettre un exemple en file rouge : arbre + coverage + budget)
5. Présentation ADTool
6. Présentation DAGSolver + lp_solve
7. Cahier des charges (mettre ADTool et optimisation linéaire comme obligatoire)
8. Management de projet
    a. Planification
    b. Outils / gestion d'équipe …
    c. Gestion des risques (risques et prévention possible, évaluation low/medium/high, faire dans un tableau (matrice avec court texte + risque + explication après)

Rapport

Attention : au vocabulaire différent entre les différentes parties, les mots spécialisés non définis ou définis deux fois … → nommer une personne pour relecture générale au moins (pour la cohérence du rapport)

Plus les infos sont visuelles : items, image …, mieux c'est ! .

Mettre les références + titre à chaque figure (et les citer dans le texte !)