ArchiTrace : Apprentissage de la sécurité par les traces

Veronique.legrand@insa-lyon.fr,
Pierre.parrend@ecam-strasbourg.eu,
Omar.Gaouar@insa-lyon.fr

Mots clé : Ingénierie inverse, ingénierie des traces, « logs », abduction, recherche de causes, approche systémique.

I Introduction

La sécurisation de grandes architectures de type Cloud montre une complexité immense qui mobilise d'ores et déjà une multiplicité de compétences. Il convient alors de compléter les enseignements classiques favorisant plutôt une compréhension par composant (pare-feu,..) par l'enseignement de l'architecture du SI dans sa globalité.

II Motivations

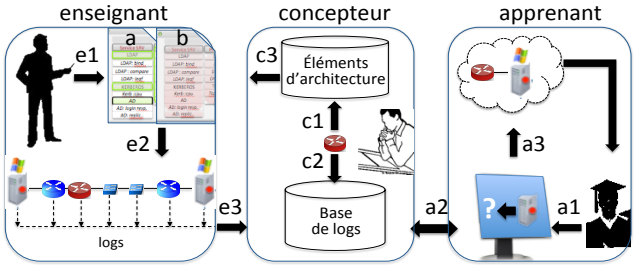
Afin de comprendre la sécurité d'architectures complexes, la variété des méthodes d'apprentissage et de formation est un atout. Aujourd'hui, l'enseignement par des cours, TD ou TP, développe bien le fonctionnement d'un mécanisme spécifique et par thème (IP, VPN, VOIP....) mais ne permet pas de comprendre les interactions qu'entretiennent ces divers mécanismes lors de leurs fonctionnement. Afin d'accomplir l'enseignement de la vision globale, nous pensons que l'apprenant doit s'entraîner à reconstituer ces interactions. Les traces informatiques résultent justement de telles interactions. Pour accomplir cette activité cognitive complexe, nous proposons d'entraîner l'apprenant à reconstituer l'architecture globale à partir des traces laissées par toute sorte de systèmes.

III Principe d'ArchiTrace

ArchiTrace est un modèle destiné à la fois aux enseignants et aux apprenants, il s'articule pour ce faire autour de trois modules :

1 - Le module « enseignant » permet de poser un problème appelé « situation pédagogique » en simulant un incident de sécurité (e1), par exemple une attaque XSS au sein d'une architecture WEB-PKI. Tout d'abord, l'enseignant simule la chaîne de liaison complète qu'il veut expliquer (menu a) : par exemple, les dépendances entre le serveur WEB et son client (Serveur, routeur, DNS, PKI…). Ensuite, l'enseignant choisit un incident parmi une liste d'incidents préconfigurés (menu b – c3): par exemple l'incident XSS (b) sur HTTP. ArchiTrace génère ensuite la situation pédagogique : le jeu, constitué des traces (e3).

2 - Le module « apprenant » permet de débuter un jeu avec l'affichage d'un composant en panne (a1). L'apprenant cherche à identifier et caractériser le composant à l'origine de l'incident de sécurité. Tant qu'il ne dispose pas d'information suffisante, il « pioche» un indice dans la base de logs (a2) pour reconstituer composant par composant la chaîne de liaison. L'intérêt est que lorsqu'il analyse cette situation, l'apprenant fait appel à ses connaissances théoriques et pratiques dans une activité cognitive d'ingénierie inverse. Si l'abduction de l'apprenant est correcte, l'itération se termine avec l'apparition du composant en panne sur son écran (a3) ; dans le cas contraire, il « pioche » une nouvelle trace dans la base de logs jusqu'à l'atteinte de l'objectif.



Présentation de ArchiTrace

3 - Le module de « conception » vise l'élaboration d'incidents de sécurité préconfigurés. ArchiTrace génère une librairie « d'éléments d'architectures (AE) » : routeurs, DNS, PKI, etc. Pour ce faire, chaque AE est relié à l'aide de classifieurs automatiques : 1) à leurs configurations génériques automatisées sur des VMs par des outils comme GNU/CFengine,…, 2) à une ou plusieurs activités normales ou d'attaques, 3) aux « logs » réels qui en découlent (c1,c2).

Ainsi, la base AE permet-elle au module « enseignant » de créer la chaîne de liaison adaptée à la situation pédagogique choisie par l'enseignant puis d'en générer les « logs » du jeu destiné à l'apprenant.

IV Conclusion

Ce travail vise un nouveau type d'enseignement adapté à la vision globale de systèmes complexes et en particulier à la sécurité du SI. La littérature est riche en travaux fondés sur les traces laissées par les systèmes numériques, généralement, leur but est de guider l'apprentissage[1] afin que l'effort de l'apprenant s'améliore. En l'état actuel de nos connaissances, nous n'avons pas relevé de travaux similaires suscitant les raisonnements d'ingénierie inverse à partir des traces. L'une des perspectives d'ArchiTrace pourra être les MOOCs, afin de permettre par ce biais un enseignement général d'IT complexes au travers d'une meilleure compréhension du fonctionnement d'un système complexe émergeant d'interactions entre l'homme et le système.

V References

[1] Ollagnier-Beldame, M., Mille, A. « Faciliter l'appropriation des EIAH par les apprenants via les traces informatiques d'interactions ? », Revue Sciences et Technologies de l'Information et de la Communication pour l'Éducation et la Formation, 2007.