Un exemple d'usage des graphes d'attaques pour l'évaluation dynamique des risques en cyber-sécurité

Emmanuel MICONNET[1], Olivier BETTAN[1], Daniel GIDOIN[1], Eric JOUENNE[2]

[1]Laboratoire d'Innovation ThereSIS, Thales Services, Campus Polytechnique, 1 avenue Augustin Fresnel 91767 Palaiseau France

[2]Thales Research & Technology, Campus Polytechnique, 1 avenue Augustin Fresnel 91767 Palaiseau Cedex, France

emmanuel.miconnet@thalesgroup.com, olivier.bettan@thalesgroup.com, daniel.gidoin@thalesgroup.com, eric.jouenne@thalesgroup.com

Résumé – La cyber-sécurité des systèmes d'information est encore souvent assurée au travers d'une multitude d'outils, comme par exemple des sondes de détection d'intrusion (IDPS), des antivirus ainsi que des systèmes de gestion et de corrélation d'événements (SIEM). La mise en perspective de ces outils, dans l'objectif d'obtenir une vue tactique de la situation en termes de sécurité du SI, constitue une tâche ardue et coûteuse en investissement techniques et humains. En effet, il est difficile de corréler et d'analyser toutes les sources d'information disponibles en temps réel afin de détecter les anomalies et les incidents et d'évaluer la gravité d'une situation suffisamment vite pour réagir efficacement. Il est extrêmement difficile aujourd'hui de comprendre l'impact métier réel d'une vulnérabilité ou d'une alerte. Cela implique de tenir compte toutes les informations techniques en notre possession sur le SI, et d'évaluer les conséquences d'une attaque sur tous les services ou processus métiers dépendant des équipements impactés par l'alerte ou la vulnérabilité. L'article proposé vise à apporter une réponse pertinente à cette problématique, au travers d'une démarche d'analyse topologique des vulnérabilités» basée sur les graphes d'attaque [2]. Dans cet article, nous présentons les résultats obtenus en appliquant cette démarche innovante de visualisation, corrélation et de prédiction d'attaques des systèmes d'information complexes.

1. Introduction

Nous pouvons partir du constat que tout Système d'Information (SI) est vulnérable. En assurer sa sécurité est donc nécessaire par nature. Les protocoles de communication sont pénétrables, les logiciels et les équipements d'infrastructure qui le composent sont pour la plupart vulnérables, et former les utilisateurs finaux ainsi que les administrateurs aux risques de « Cyber attaque » prend beaucoup de temps. La Cyber-sécurité est donc coûteuse en terme d'effort, elle exige des connaissances spécialisées multiples ; et elle est également sujette aux erreurs en raison de la complexité et des changements fréquents de configurations du SI. Les administrateurs et les experts en charge de la sécurité peuvent facilement être submergés par la masse d'information à traiter et réduits souvent à réagir aux seuls événements remontés par de nombreuses sondes placées à différents endroits du SI, sans pouvoir évaluer la criticité réelle de la situation.

Face à cette incapacité d'appréhender la situation et donc de réagir en toute connaissance de cause aux événements de sécurités, une approche préventive semble nécessaire.. Il faut pouvoir anticiper ces menaces le plus en amont possible, voir idéalement être en mesure de mettre en œuvre des actions correctives prévenant leur apparition, Un tel comportement limitera l'exposition au risque des métiers supportés par le SI et réduira considérablement l'impact des actions malveillantes dont ils sont la cible.

Vu la complexité des systèmes d'information, des priorités doivent en effet être fixées pour se concentrer sur la sécurisation des parties vitales du SI. Les administrateurs et les experts ont souvent une vision verticale de la partie du SI dont ils ont la charge, les vues horizontales relatives aux différentes niveaux du SI (infrastructure physique, virtuelle, réseau, couche applicative, …) sont souvent manquantes. Ceci met d'ailleurs en évidence l'importance de disposer de cette connaissance des dépendances entre niveaux dès lors que l'exploitation de certaines vulnérabilités permet d'atteindre des couches apparemment sécurisées

Les préoccupations de sécurisation d'un SI sont également fortement interdépendantes, à savoir, l'occurrence d'une attaque peut dépendre de multiples vulnérabilités dans les différentes parties d'un SI. Des hackers peuvent combiner ces vulnérabilités pour progressivement pénétrer le SI et compromettre les

processus critiques qu'il sous-tend (i.e. réalisation d'Exploits).

Cependant, les outils de sécurité traditionnels sont généralement des solutions parcellaires qui s'adressent chacune à une petite partie du problème global de la sécurité. Ils peuvent nous donner quelques indices sur la façon dont les hackers pourraient enchaîner l'exploitation de vulnérabilités afin de faire prospérer leurs attaques contre le SI. Il est très difficile de combiner les résultats de plusieurs outils et sources de données pour comprendre la vraie situation : la présence d'une attaque d'une grande complexité se développant au travers de multiples étapes, elles-mêmes sophistiquées et parfois sur de longues périodes pour en assurer la discrétion. Il peut être très difficile, même pour un analyste expérimenté d'identifier les risques auxquels est exposé le SI ; cette tâche devient particulièrement ardue quand il s'agit de grands SI qui évoluent dynamiquement.

Les développements assez récents entrepris dans bon nombre de laboratoires universitaires [1][2] et industriels ont par ailleurs montré que des modèles topologiques de SI peuvent être crées automatiquement à partir de « scans » réseau, et notamment par l'exploitation des journaux fournis par les différents équipements du SI. Les « Exploits » des hackers potentiels sont aussi modélisés à partir de bases de données de vulnérabilités existantes [9[10][11][12[13][14]..

L'approche présentée au sein de cet article, montre que nous pouvons actuellement calculer efficacement des graphes d'attaque pour des SI de dimension réaliste. La difficulté réside maintenant dans le fait que les graphes d'attaque qui en résultent peuvent souvent poser des problèmes de compréhension et d'interprétation (taille, complexité, …), d'où l'idée de faire appel à des techniques et outils de type « Visual Analytics » capables d'apporter des capacités avancées de navigation et de visualisation de gros volumes d'information. Dans nos différents projets, menés depuis plus de 2 ans, nous développons des techniques et des outils pour rendre plus compréhensible les graphes d'attaque ainsi obtenus. Il s'agit également de mettre ces techniques au service d'une analyse d'impact consécutive à des changements de configuration réseau et/ou d'applicatifs, et permettre une gestion efficiente des alarmes d'intrusion dans le contexte général de la supervision du risque d'un SI.

Nous appliquons notre approche généraliste au domaine de la visualisation de graphes d'attaque, ceux-ci étant basés sur l'exploitation de vulnérabilités connues. Cette approche a pour objectif de rendre les graphes d'attaque plus lisibles et interprétables par les acteurs de la sécurité en fonction de leurs métiers et priorités respectifs. Nous montrons également comment cette représentation aider à la compréhension des changements survenus dans un graphe d'attaque suite à des changements de configuration du SI. Fonction qui prend également tout son sens quand il s'agit par exemple de simuler des scenarios « What-if » en prévision d'évolutions alternatives du SI.

2. Construction et mise en œuvre des graphes d'attaques

La représentation de combinaisons d'attaques de SI sous forme de graphes n'est pas nouvelle et est bien établie [1][2][4][8]. Encore aujourd'hui, les graphes d'attaque de ce type sont souvent créés manuellement par des équipes « sécurité » (architectes sécurité, testeurs de pénétration, …). Plusieurs travaux ont démontré l'usage de capacités de calcul pour la génération de graphes d'attaque [2][7][8], plutôt que de s'appuyer sur une création manuelle fastidieuse, non exhaustive et souvent source d'erreurs.

Cette approche est basée sur la modélisation topologique du SI (figure 1), de ses conditions de sécurité (analyse des vulnérabilités connues [9[10][11][12[13][14], ainsi que de la connaissance d'exploits (exploitation des vulnérabilités) par des attaquants potentiels. Les approches traditionnelles traitant uniquement des données du SI ainsi que des événements de sécurité, sans tenir compte du contexte fourni par les graphes d'attaque, sont nettement insuffisantes.

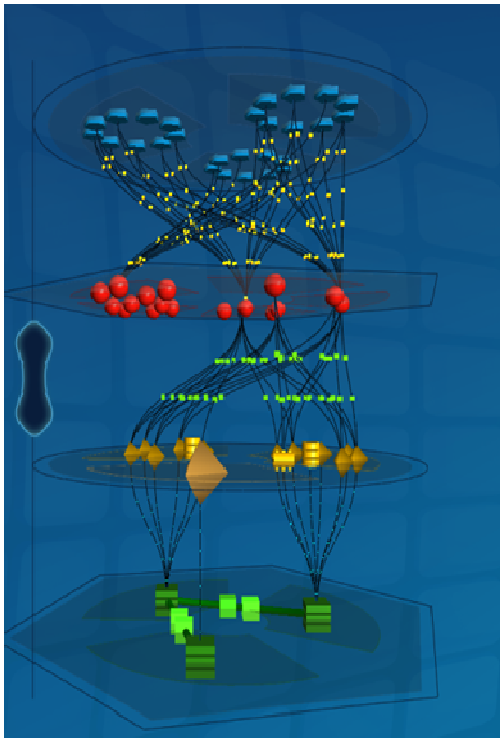

FIG. 1 : Exemple de modélisation d'un SI sur 4 niveaux
(processus, applications, composants réseaux, infrastructure)

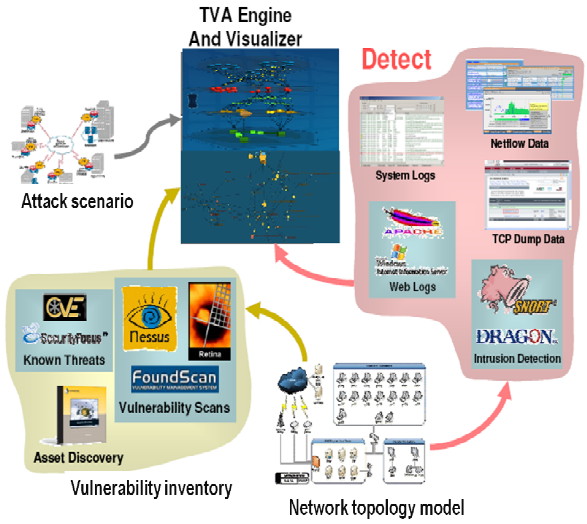

FIG. 2 : Constituants nécessaires au calcul d'un graphe d'attaque

L'approche innovante de la cyber-sécurité proactive via les graphes d'attaque est communément appelée Analyse Topologique de Vulnérabilité (ou TVA en anglais) [2]. La « TVA » consiste à combiner les vulnérabilités à la manière d'un réel attaquant, en découvrant étape par étape tous les chemins d'attaque à travers un SI, compte tenu de l'exhaustivité des données utilisées pour construire le graphe.

Pour définir ces graphes, nous analysons les interdépendances entre vulnérabilités et construisons une carte complète indiquant tous les chemins de pénétration possibles, directs ou en plusieurs étapes, d'un SI. La « TVA » nécessite de modéliser les composants du SI, y compris les applications, leurs vulnérabilités et la connectivité/dépendances aux processus/services en jeu au sein du SI. Elle compare ensuite la configuration du SI avec une base de données d' « Exploits » modélisés afin de simuler le déroulement d'attaques chaînées. Le graphe d'attaques ainsi obtenu permet donc de cartographier toutes les voies potentielles d'exploitation des vulnérabilités, montrant ainsi comment les attaquants peuvent s'introduire au sein du SI et quelles sont les processus et ressources qu'ils pourraient compromettre.

FIG. 3 : Exemple de graphe d'attaque
(ex. le composant i du SI est relié par un lien au composant j montrant l'exploitation d'une vulnérabilité du composant j)

La « TVA » permet également d'identifier les vulnérabilités les plus critiques et propose des stratégies de protection des « actifs » du SI. Cette approche permet d'anticiper les menaces, de durcir le SI préventivement (application de contre-mesures logicielles, matérielles, …), avant que les attaques ne se produisent. Elle permet aussi de positionner et configurer de façon optimale les systèmes de détection d'intrusion de manière à en améliorer l'efficacité, et d'apporter une réponse appropriée aux attaques potentielles.

3. Apports de la démarche

La démarche « TVA » décompose la génération de graphes d'attaque en deux phases: 1/ la capture d'un modèle du SI, et 2/ l'utilisation du modèle pour simuler la pénétration du SI via plusieurs étapes. Ce modèle contient la configuration du SI et les « exploits » d'attaquants connus. En simulation d'attaque, le modèle d'entrée est analysé pour former un graphe d'attaque des exploits selon les contraintes spécifiées par l'utilisateur.

Les graphes d'attaque peuvent donc servir à définir des stratégies optimales pour la prévention des attaques, combinant par exemple, le « patching » de vulnérabilités critiques et le « durcissement » des systèmes et des services. Cependant en raison de contraintes opérationnelles, comme la disponibilité de correctifs, l'incompatibilité de certaines applications avec des montées en version des systèmes, d ou encore de limites budgétaires, les experts de la sécurité doivent prendre en compte un risque résiduel

Les graphes d'attaque fournissent le contexte nécessaire pour faire face à des tentatives d'intrusion. Cela inclut des conseils pour le déploiement et la configuration des systèmes de détection d'intrusions (sondes IDS), la corrélation des alarmes d'intrusion, et la prévision des prochaines étapes d'attaque possibles. Par exemple, le graphe d'attaque peut guider le placement des sondes de détection d'intrusion pour couvrir en priorité les chemins d'attaque critiques (ceux conduisant par exemple à l'indisponibilité de services critiques), tout en minimisant leur redondance. Une contrainte de cette démarche réside la nécessité de maintenir les graphes d'attaque à jour par rapport aux changements du SI (configuration, vulnérabilités, …) afin de présenter une situation fidèle à l'état courant des chemins d'attaques.

Un autre avantage des graphes d'attaque réside dans le fait qu'ils peuvent permettre le filtrage de fausses alarmes (réduction du bruit dû à des événements de sécurité non pertinents), basées sur des chemins connus de vulnérabilités résiduelles. Le graphe fournit également un cadre pour corréler des alarmes isolées et détecter précocement une attaque de grande envergure Il révèle également les vulnérabilités qui pourraient être exploitées successivement par un attaquant, si elles se trouvent sur des chemins d'accès possible ressources et processus critiques du SI.

Au global, cette cartographie de tous les chemins à travers le SI fournit une capacité de défense « en profondeur », avec de multiples options d'atténuation des attaques potentielles (« mitigation »), plutôt que de compter uniquement sur les défenses habituelles du SI (pare-feu par ex.).

La sécurité d'un SI n'est pas définie une fois pour toute, mais plutôt au travers d'un processus continu, comme dans le cycle « protéger-détecter-réagir ». Pour se protéger des attaques, nous tentons de prendre des mesures pour les empêcher d'aboutir. Cependant, nous savons que toutes les attaques ne peuvent être évitées à l'avance et qu'il subsiste généralement certaines vulnérabilités résiduelles, même après l'application de mesures de protection raisonnables.

En effet, la question la plus importante n'est pas la vulnérabilité en elle-même, mais l'ampleur des dommages provoqués par une attaque. Le processus de détection doit donc prendre en compte les vulnérabilités résiduelles, en particulier celles qui se trouvent sur les chemins menant aux ressources critiques du SI et qui les exposent à des utilisations malveillantes, d'où l'importance de les identifier.

A travers la démarche présentée, on peut ainsi réduire l'impact des attaques avant qu'elles ne se produisent, en connaissant les chemins de vulnérabilités à travers le SI et être alerté de leur occurrence au plus tôt afin d'être en mesure de réagir efficacement et en toute connaissance de cause. Pour voir émerger une telle attitude « proactive », nous avons besoin de transformer les données brutes sur les vulnérabilités du SI, en attaque potentielle qui nous aide à 1/ prioriser et à gérer les risques, 2/ maintenir la connaissance de la situation et 3/ planifier de façon optimale les « contre-mesures » nécessaires à la réduction des risques identifiés.

La démarche « TVA », au travers des graphes d'attaque, permet de soutenir les défenses proactives du SI sur l'ensemble du cycle « protect-detect-react ». Cette démarche rationnelle consiste à identifier les vulnérabilités critiques, calculer des métriques de sécurité, optimiser le positionnement et la configuration des systèmes de détection d'intrusion, corréler et la prioriser les alarmes d'intrusion, permettant ainsi de réduire les fausses alarmes, et de planifier une réponse optimale à l'attaque.

Enfin, grâce à des techniques de visualisation sophistiquées apportées par des outils 3D, nous pouvons explorer de façon interactive les graphes d'attaque. Ces visualisations sont conçues pour gérer efficacement la complexité des graphes en offrant une vision priorisée de la situation et des facilités de navigation au sein de grand volume de données.

4. Conclusion

Dans cet article, nous avons décrit les résultats obtenus grâce à l'application d'une démarche de type « TVA » basée sur les graphes d'attaque, démarche innovante pour la visualisation, la corrélation et la prédiction d'attaques de SI complexes en plusieurs étapes. Cette approche tient compte à la fois des vulnérabilités logicielles, de la connectivité réseau, des comportements d'équipements de type pare-feu, ainsi que des exploits d'attaquants potentiels.

L'approche nous mène à construire des graphes d'attaque complexes mais adaptés aux opérateurs de sécurité, ceci au travers d'outils de visualisation 3D avancés. L'analyse combine les vulnérabilités de la même manière que pourrait le faire des agresseurs réels.

La propagation d'indicateurs de vulnérabilité individuels au travers des graphes d'attaque, permet d'introduire une nouvelle mesure de la cyber-sécurité d'un SI. Notre démarche conduit à utiliser cette mesure pour comparer les options de réduction des risques en termes de maximisation de la sécurité et de minimisation des coûts, dans l'optique de quantifier la sécurité globale des SI.

Références

[1] Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense, Philippe Lagadec, NATO C3 Agency

[2] Advanced Cyber Attack Modeling analysis , and visualization,. George Mason University, final Technical Report, March 2010

[3] “Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs,” S. Noel, S. Jajodia, Journal of Network and Systems Management, special issue on Security Configuration Management, September 2008

[4] “Building Attack Scenarios through Integration of Complementary Alert Correlation Methods,” P. Ning, D. Xu, C. Healey, R. St. Amant, , in Proceedings of the 11th Annual Network and Distributed System Security Symposium, February 2004.

[5] “Applied Security Visualization”, R. Marty, Addison Wesley, August 2008

[6] EBIOS - Expression des Besoins et Identi□cation des Objectifs de Sécurité, ANSSI, http://www.ssi.gouv.fr/site_article45.html.

[7] “Advanced Vulnerability Analysis and Intrusion Detection through Predictive Attack Graphs,” S. Noel, S. Jajodia, Critical Issues in Command, Control, Communications, Computers, Intelligence (C4I), Armed Forces Communications and Electronics Association (AFCEA) Solutions Series, Lansdowne, Virginia, May2009

[8] “MulVAL : a logic-based network security analyzer”, X. Ou, S. Govindavajhala, A. Appel, in proceedings of the 14th USENIX Security Symposium, held 31 July, 5 August 2005 in Baltimore, Maryland, USA, Vol. 14, pp. 113-128, USENIX, Association, Berkeley, California, USA, August 2005

[9] CAPEC, Common Attack Pattern Enumeration and Classification, http://capec.mitre.org/

[10] Security Database, http://www.security-database.com/

[11] CVE, Common Vulnerabilities and Exposures, http ://cve.mitre.org/

[12] NVD, National Vulnerability Database, http ://nvd.nist.gov/

[13] CPE, Common Platform Enumeration, http ://cpe.mitre.org/

[14] OVAL, Open Vulnerability and Assessment Language, http ://oval.mitre.org/