Proposition de sujet de thèse

Titre du projet de thèse de doctorat :
Nouveaux procédés d'attaques et mécanismes de défense associés en cybersécurité.

Mots clefs : Attaques, Défense, Cybersécurité, Internet, Vulnérabilités, Détection d'intrusions, Plateforme Simusec, Stratégies de défense.

Contexte

Aujourd'hui avec l'explosion de l'Internet et la dématérialisation du monde numérique, lesréseaux informatiques jouent un rôle prépondérant dans la vie de tous les jours et dans notre société en général. Ouverts au monde extérieur les réseaux informatiques deviennent des cibles potentielles pour les personnes malveillantes qui tentent d'exploiter les vulnérabilités de ces systèmes. Et ces attaques peuvent affecter l'image de marque, la notoriété des grandes entreprises d'où la problématique de la sécurité de ces systèmes qui devient ainsi essentielle aussi bien pour les utilisateurs que pour les administrateurs de ces systèmes [1].

Selon Vectra Networks qui exprime que les attaquants utilisent les réseaux anonymes pour mener à bien leurs opérations de cyber crimes et le taux d'utilisation de ces réseaux anonymes ne cesse de croitre de jour en jour. De plus les auteurs utilisent des techniques d'attaques échappant aux moyens de défenses périphériques et arrivent ainsi à compromettre les réseaux d'entreprises et d'institutions dedivers secteurs d'activités (éducation, énergie, ingénierie, services financiers, gouvernement, santé, juridique, médias, vente au détail, technologie, etc.) [2].

Ainsi la sécurité devient un enjeu majeur des technologies numériques modernes. Infrastructures de télécommunication (GSM, GPRS, UMTS), réseaux sans fils (Bluetooth, WiFi, WiMax), Internet, systèmes d'information, routeurs, les serveurs, ordinateurs, téléphones, décodeurs de télévision, assistants numériques, systèmes d'exploitation, applications informatiques, toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration. Ces systèmes tombent en panne, subissent des erreurs d'utilisation et sont attaqués de l'extérieur ou de l'intérieur par des pirates ludiques, des cybercriminels, ou sont la proie d'espionnage industriel. Une approche globale de la sécurité des systèmes est donc essentielle pour protéger la vie privée, pour défendre le patrimoine d'une entreprise ou pour réduire les vulnérabilités des grands systèmes d'information [3,4].

Cette sécurisation peut être abordée par l'insertion de données cachées (tatouage, stéganographie, etc.) ou par des aspects cryptographie (cryptage sélectif, signature perceptuelle, etc.). Cela concerne principalement la confidentialité, l'intégrité, la disponibilité, l'authentification, et la protection des données personnelles [3]. En dépit des efforts conséquents qui ont été investis depuis un certain nombre d'années pour tenter d'endiguer les problèmes de sécurité, force est de constater que le nombre de vulnérabilités dans les systèmes informatiques et, de surcroît, les activités malveillantes qui essaient et qui réussissent à les exploiter, continuent régulièrement à se multiplier [5].

En 2016 les chercheurs de Kaspersky Lab, spécialisé dans la sécurité des systèmes d'information, tendent à confirmer ce phénomène. Notamment, il dénombrait pas moins de 70 000 serveurs voir 176 000 serveurs ont été compromis en 2016 [6] ont également constaté

l'étendue des difficultés qu'éprouvent les entreprises pour repérer rapidement un incident de sécurité :

- 28,7 % d'entre elles déclarent que cela leur a pris plusieurs jours,
- Et 19 %qu'il leur a fallu des semaines voir d'avantage,
- Pour une minorité non négligeable de 7,1%, ce délai a été de plusieurs mois.

Ainsi l'économie souterraine est plus vaste et élaborée que jamais. Il suffisait de regarder : une place de marché douteuse où se négocie plus de 70 000 identifiants volés donnant accès à des serveurs piratés.

Les attaquants font aujourd'hui de plus en plus preuve d'ingéniosité pour attaquer les systèmesInformatiques : les malveillances peuvent cibler les programmes qui s'exécutent surle système mais également le système d'exploitation lui-même et en particulier, son noyau.Corrompre le noyau d'un système d'exploitation est particulièrement intéressant du point devue d'un attaquant car cela permettrait potentiellement de corrompre plus facilement tous les programmes qui s'exécutent au-dessus du noyau, voire prendre complètement le contrôle du système [5]. À cet effet, il dispose de divers vecteurs d'attaques.

La plupart des scénarios d'attaque s'appuient sur des vecteurs d'attaque liés au logiciel s'exécutant sur le processeur principal : un attaquant peut, par exemple, utiliser des fonctionnalités trop permissives du système ou exploiter des erreurs d'implémentations logicielles (les débordements de tampons ou d'entiers, les chaînes de format, etc.). Cette classe d'attaques est relativement bien connue à ce jour, et de nombreux mécanismes (les piles non exécutables, la distribution aléatoire de l'espace d'adressage, la technique du canari, etc.) permettent de s'en protéger.

Depuis quelques années, nous constatons que les scénarios d'attaques évoluent et deviennent chaque jour plus complexes [7,8,9,10]. En effet, certaines attaques ne reposent plus exclusivement sur l'utilisation de composants logiciels, et nous observons de plus en plus d'attaques impliquant des composants matériels, tels que le chipset, les contrôleurs d'entrées sorties (un contrôleur Ethernet, un contrôleur de clavier, etc.) ou les périphériques (un iPod avec une connectique FireWire, une souris USB, etc.). Celles-ci détournent des fonctionnalités légitimes du matériel, tels que les mécanismes entrées-sorties (accès direct à la mémoire, interruption, etc.) à différentes fins malveillantes (escalade de privilèges, fuite d'informations, dénis deservices, etc.).

En résumé, le but de ce projet de thèse est de rechercher de nouvelles méthodes d'attaques, en visant à chaque fois, à produire leurs signatures et les mécanismes de défenses associés. Nous nous emploierons à mettre en place une plateforme (appelée plateforme SimuSec) d'entrainement d'attaques/défenses qui servira de support technique pour valider et illustrer les différends mécanismes sous-jacentsà cet important projet de recherche. Nous privilégierons également la recherche de brevets dans ce travail. Les cibles d'applications concernées pourraient inclure les services Internet classiques, l'Internet des Objets, les réseaux auto-configurables (adhoc, capteurs, etc.), ainsi que systèmes d'information des grandes entreprises et les infrastructures critiques.

Objectifs

La plateforme SimuSeca plusieurs objectifs :

- Construire un environnement de formation dans les systèmes d'attaques, afin de démontrer les stratégies techniques utilisées par les assaillants, l'effet de ces attaques et de contribuer au renforcement de capacités dans la réalisation d'activités de tests de pénétration.
- Fournir une plateforme d'entrainement et de maitrise de la sécurité des systèmes enquestion, y compris les outils pour l'évaluation des vulnérabilités, ladétection d'intrusions, la sécurité de l'information et de la gestion desévénements. Cela inclut la possibilité de générer des scénarios d'attaque,de tracer leur exécution et de comparer la réponse attendue à l'actiondes administrateurs de réseaux, afin d'évaluer leurs capacités et leurs réflexes.
- D'évaluer les systèmes d'attaques et de défense, en les intégrant à desendroits clés de la plateforme SimuSec, assurant à la fois le commandement et le contrôle ainsi que la mission liée à l'interface avec la plateforme, la collecte d'informations à propos de leur comportement et de leur capacité.
- D'étudier les différents mécanismes de traçabilité des événements en s'intéressant à l'analyse préventive découlant d'une bonne compréhension de la corrélation d'événements par la mise en place de systèmes intelligents.

Pour atteindre ces objectifs, la plateforme SimuSec peut être considéréecomme un système intégré « nuage » de services, qui remplissent les missionsconcernées requises, telles que la gestion de la plateforme, l'intégrationd'outils d'attaques, l'intégration des machines vulnérables, l'intégration d'outilsde sécurité et l'évaluation du comportement général de la plateforme.

Dans ces thèses, nous allons essayer de traiter trois points fondamentaux dans la problématique des attaques cybernétiques : d'abord, mettre en œuvre laplateforme Simusec, élaborer ensuite de nouveaux scénarios d'attaques, puis identifier de nouvelles signatures d'attaques ainsi que des stratégies de défense.

Pour chacun de ces thèmes, nous décrivons la problématique en jeu, puis nouspasserons en revue les solutions qui ont été proposées dans l'état de l'art. Endernier lieu, nous détaillerons les solutions que nous proposerons, etprésenterons leurs avantages comparativement aux solutions existantes.

Méthodologie de recherche

Le processus de recherche requiert la mise en application d'une méthodologie efficace afin de garantir un rendu innovant et fiable. Pour ce faire nous allons procéder comme suit :

- Le travail se fera en équipe avec au minimum deux doctorants (attaquant/défenseur), voir idéalement quatre doctorants (2 attaquants (système & réseau) / 2 défenseurs)
- Formulation et définition de notre problématique
- Etude de quelques mécanismes d'attaques et de défense existants

- Proposition de nouveaux scénarios d'attaques et de mécanisme de défenses associés
- Tests et validation via la plateforme SimuSec
- Dépôts de brevetséventuels

Collaborateurs

- **Porteur du projet de thèse :** Dr. Cherif Diallo, Maître–assistant (CAMES) ;
- **Directeur de thèse :** Ousmane Thiare, Professeur Titulaire (CAMES) ;
- **Autrescollaborateurs:**
  - Pr. Mohamed Mejri, Professeur Titualire, Université de Laval, Canada ;
  - Pr. Doudou Fall, Laboratory for Cyber Resilience, Nara Institute of Science and Technology, NAIST, Japon ;
  - Dr. Augustin Pathé Sarr, Maître–assistant (CAMES) ;

Planning

- Projet de thèse de doctorat sur 36 mois, pour deux candidats, voir quatre. Le (ou les deux) premier(s) candidat(s) s'intéressera(ont) à la production de nouvelles attaques tandis que l' (ou les deux) autre(s) se focalisera(ont) davantage sur les mécanismes de défense.
- Note : il est possible qu'une demande de dérogation d'une année supplémentaire (pour chacun des deux doctorants retenus) soit adressée au CEA–MITIC, à l'issue de la troisième année en vue de faire des recherches supplémentaires pour mieux valider les résultats qui auront été déjà acquis.

Sources de financement

- Une bourse de thèse sur 36 mois pour les deux (ou quatre) candidats qui seront retenus.
- Note : il est possible qu'une demande de moyens supplémentaires dont le montant sera communiqué le moment venu, soit adressée au CEA–MITIC pour l'acquisition de matériel et la mise en œuvre de la plateforme SimuSec en vue d'un prototypage des solutions qui seront proposées.

Profil de doctorants recherchés

- Titulaire d'un master en systèmes, réseaux et télécommunications avec éventuellement un mémoire orienté recherche. Une expérience dans le domaine de la sécurité serait très appréciée.
- Background ensécuritéréseaux
- Bon niveau en administration système et en programmation
- Bonne maitrise des outils d'attaques, de détection d'intrusions, d'audits et de simulation
- Très bon niveau en anglais (oral et écrit), éventuellement bilingue.

Références

[1] LucieSaunois, Sécurité informatique : introduction aux menaces, les pirates informatiques : qui sont-ils ?, octobre 2016.

[2] ICT Journal Attaques ciblées, Vectra Networks:les techniques d'intrusions de réseaux informatiques évoluent juin 2015.

[3] Pré-GDR Sécurité Informatique, Groupe de travail: sécurité et données multimédia GT commun avec : GDR Information, Signal, Image et Vision(ISIS), décembre 2017.

[4] Michel Riguidel, La sécurité des réseaux et des systèmes.

[5] Fernand LoneSang, Protection des systèmes informatiques contre les attaques par entrées et sorties.

[6] Bulletin Kaspersky Security Revue et statistiques globales de l'année 2016.

[7] J. Fattahi, M. Mejri and E. Pricop. The Theory of Witness-Functions. In Recent Advances in Systems Sa- fety and Security.Springer International Publishing, Editor Pricop, Emil and Stamatescu, Grigore, pp 1–19, year 2016. isbn=978-3-319-32525-5, doi=10.1007/978-3-319-32525-5_1, url="http ://dx.doi.org/10.1007/978-3-319- 32525-5_1".

[8] J. Fattahi, M. Mejri. R. Ghayoula and E. Pricop. Tracking Security Flaws in Cryptographic Protocols Using Witness-Functions. The IEEE International Conference on Systems, Man, and Cybernetics. (IEEE SMC 2016). Budapest, hungary, October 2016.

[9] M. Mejri, E. Theodore Sadio and K. Arrachid. AVTAC : A Framework for Automatic Auditing of Access Control in Windows and Linux Systems. The 13th International Conference on Intelligent Software Methodologies, Tools and Techniques. Langkawi, Malaysia, September 2014.

[10] D. Kpekpassi, S. Balde, M. Toure, and A. B. Seck. Mise en place d'une plateforme d'entrainement à la sécurité informatique. Mémoire de Maîtrise sous la direction de Chérif Diallo, 2014.