Titre

- Cyber Sécurité en Réalité Virtuelle : améliorer le processus de détection d'intrusion, d'investigation et de décision via l'utilisation de techniques de visualisations 3D immersives

Contexte

- L'une des raisons de la mise en échec de la détection d'intrusion découle d'un manquement de certains types d'éléments en entrée de moteurs de corrélation, de diagnostics et de réponses. Généralement, ces éléments ne sont pas des événements purement informatiques (suppression d'un processus, changement de l'horloge interne du système, etc.), ils ne se produisent pas de façon fréquente et correspondent à des objets observables (comportements suspects ou non habituels d'un insider ou d'un outsider évoluant dans l'environnement du système par exemple). L'intégration de ce type d'éléments dans de nouveaux types de systèmes de surveillance permettrait la réduction des taux de faux négatifs, donnerait la possibilité de découvrir de nouveaux chemins d'attaques, aiderait la prise de décision de sécurité dès lors où le processus et l'algorithme de corrélation entre ce type d'éléments hétérogènes ont été correctement définis, analysés et/ou anticipés.

Objectif

- Il s'agit de proposer de nouveaux moyens d'aide à la détection d'intrusion basés sur la détection de signaux dits « faibles » en provenance de capteurs de types variés, allant par exemple des fichiers de traces associés à des pare-feux jusqu'à des capteurs de mouvements (présence) dans des locaux. Ces moyens seront basés sur de nouvelles métaphores 3D de représentations de ces signaux permettant à des utilisateurs de « monitorer » les éléments à surveiller. Pour leur faciliter la tâche, on leur donnera des moyens pour s'immerger dans un univers virtuel 3D dans lequel on devra proposer des moyens adaptés pour naviguer dans ces représentions qui pourront parfois s'inspirer du réel (comme la modélisation 3D de bâtiments à surveiller) mais qui devront aussi intégrer des représentations plus abstraites à ces environnements 3D de façon à caractériser visuellement ces signaux faibles. Il s'agira donc de :
  - définir, concevoir, implémenter, tester et évaluer des métaphores de représentation 3D adaptées à la surveillance de signaux faibles en provenance de capteurs variés,
  - étudier l'apport de la gestion d'un historique de l'évolution de ces signaux, la détection d'intrusion pouvant parfois se faire à partir d'une analyse dynamique et spatiaux-temporelle de ces signaux (3D+T ou 3D augmentée de représentations abstraites),
  - proposer des métaphores de représentation 3D permettant de comparer ces signaux à des signaux de même nature s'étant produits lors d'intrusions avérées, et de mettre en relation différents signaux pour les corréler et en déduire des risques d'attaques,
  - évaluer les techniques proposées en les validant au travers d'études expérimentales faisant intervenir des personnes réellement en charge de la détection d'intrusion.

Plan proposé :

- M0-M12 :
  - prise de connaissance du domaine de recherche en visualisation pour la sécurité
  - prise de connaissance du domaine applicatif de la détection d'intrusion, identification de la nature des capteurs usuels et des signaux qu'ils produisent
  - rédaction d'une première version d'un état de l'art sur les types de capteurs utilisables en détection d'intrusion et de leurs signaux associés
  - rédaction d'une première version d'un état de l'art sur les moyens de représentation de ces capteurs et signaux
- M12-M18 :
  - spécification de métaphores de représentation adaptées pour les cibles d'intrusion, leurs capteurs de détection d'intrusion et des signaux qu'ils produisent
  - premiers essais de prototypage
- M18-M30 :
  - mise au point d'une bibliothèque de métaphores de représentations de cibles, capteurs et signaux, ainsi que des moyens d'interagir avec eux afin de les exploiter au mieux
  - première version d'un prototype permettant la visualisation des câbles, capteurs et signaux
  - instrumentation du prototype pour permettre son évaluation
- M30-M33 :
  - finalisation du prototype de visualisation
  - validation sur un ou plusieurs scénarios d'intrusions
  - évaluations par le biais d'expérimentations conduites avec des utilisateurs du domaine de la détection d'intrusions
- M33-M36 :
  - révision des états de l'art (mise à jour au fil de l'eau durant la seconde année et la troisième année de thèse)
  - rédaction du manuscrit de thèse, préparation de la soutenance

Références :

- Security attacks discovery through visualization: beauty in badness
  - Dan Hubbard
  - https://www.youtube.com/watch?v=FF4B97sNCn8
- VizSec 2014 keynote
  - Dan Hubbard
  - https://labs.opendns.com/2014/12/03/vizsec2014/
- Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain
  - Bloom, B.S. (Ed.). Engelhart, M.D., Furst, E.J., Hill, W.H., Krathwohl, D.R. (1956)
  - New York: David McKay Co Inc.
- Graphics for Learning : Proven Guidelines for Planning, Designing, and Evaluating Visuals in Training Materials
  - Clark, R., Chopeta, L. (2004)
  - Jossey-Bass/Pfeiffer
- SAGG: Simultaneous Attacks Graph Generator
  - Léa Samarji, Nora Cuppens-Boulahia, Frédéric Cuppens, Wael Kanoun, and Samuel Dubus
  - Journal of Computer and Science (COSE), 2015
- Situation calculus and graph based defensive modeling of simultaneous attacks
  - Layal Samarji, Frédéric Cuppens, Nora Cuppens-Boulahia, Wael Kanoun, and Samuel Dubus.
  - In Cyberspace Safety and Security, volume 8300 of Lecture Notes in Computer Science, pages 132–150. Springer International Publishing, 2013.
- A Service Dependency Model for Cost-Sensitive Intrusion Response
  - Nizar Kheir, Nora Cuppens-Boulahia, Frédéric Cuppens, Hervé Debar
  - ESORICS 2010: 626-642
- From Cyber Security Activities to Collaborative Virtual Environments Practices through the 3D CyberCOP Platform
  - A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, C. Ponchel
  - in proceedings of ICISS 2018 (14th International Conference on Information Systems Security), p. 272-287, Bengaluru, India, December 16-20, 2018
- 3D CyberCOP: a Collaborative Platform for Cybersecurity Data Analysis and Training
  - A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, C. Ponchel
  - in proceedings of CDVE 2018 (15th International Conference on Cooperative Design, Visualization and Engineering), Springer, p. 176-183, Hangzhou, China, October 21-24, 2018
- HeloVis: a Helical Visualization for SIGINT Analysis using 3D immersion
  - A. Cantu, T. Duval, O. Grisvard, G. Coppin
  - in proceedings of PacificVis 2018 - IEEE Pacific Visualization Symposium, 11th international visualization symposium, Notes track, IEEE, p. 175-179, Kobe, Japan, April 10-13, 2018
- Why should we use 3D Collaborative Virtual Environments for Cyber Security?
  - A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, C. Ponchel
  - in proceedings of of 3DCVE 2018 (IEEE VR 2018 International Workshop on 3D Collaborative Virtual Environments), 2 pages, Reutlingen, Germany, March 19, 2018
- Identifying the relations between the visualization context and representation components to enable recommendations for designing new visualizations
  - A. Cantu, O. Grisvard, T. Duval, G. Coppin
  - in proceedings of IV2017 - 21st International Conference on Information Visualisation, InfVis track - Information Visualisation Theory & Practice, IEEE, p. 20-28, London, UK, July 11-14, 2017