SuperviZ : proposition de Thèse 1.1

Titre : « Identification et évaluation du niveau de risque associé à des scénarios d'attaques dans des ensembles d'infrastructures interdépendantes »

Doctoral school : ED IP Paris (ED626), Domaine Informatique, Données et Intelligence Artificielle

Équipe et laboratoire et équipe d'accueil : Équipe ACES, Laboratoire Traitement et Communication de l'Information, Télécom Paris, Institut Polytechnique de Paris

Localisation : Télécom Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France.

Encadrants : Jean Leneutre & Vadim Malvone

Date de démarrage : Janvier 2024

Mots clés : Cybersecurity, Security Supervision, Risk Analysis, Threat Modelling, Security Game, Game Theory, Multi-agent system verification

Contexte & objectif global

Pour des questions de coût ou de mise en œuvre, les systèmes numériques contiennent nécessairement des vulnérabilités résiduelles dont certaines seront exploitées par des attaquants. Dans ce contexte, la supervision est un service de sécurité essentiel permettant de renforcer les mécanismes de protection et de pallier parfois leurs éventuelles insuffisances. Initialement, ce service concernait principalement la détection puis la gestion, l'analyse et la corrélation des événements de sécurité. Aujourd'hui, il englobe plus généralement l'analyse de risque et l'orchestration de sécurité, prenant en compte en amont de la détection des informations relatives aux attaques en cours et en aval l'automatisation de la réponse aux attaques détectées.

Ces dernières années ont vu l'apparition d'attaques sophistiquées comme les « Advanced persistent threats (APT) » qui sont des attaques complexes avec un long cycle de vie, et un fort degré de furtivité. Celles-ci peuvent exploiter des « effets cascades » dus aux interconnexions des systèmes. Ces scénarios d'attaques s'avèrent particulièrement difficiles à détecter et mitiger et peuvent avoir un impact considérable. Un tel scénario d'attaque a eu lieu par exemple en Ukraine en décembre 2015, où une compromission à distance de systèmes d'information de trois sociétés de distribution d'énergie, a ensuite permis aux attaquants de prendre le contrôle du système SCADA contrôlant l'approvisionnement en électricité, entraînant des pannes de courant pour environ 230 000 consommateurs en Ukraine pendant 1 à 6 heures [LAC2016].

L'objectif global de ce doctorat est de proposer des méthodes et outils permettant de définir des stratégies de détection et de réaction afin de limiter les risques de sécurité liés à des scénarios d'attaques complexes et furtifs exploitant les interdépendances entre différents types d'infrastructures.

Travaux existants, verrous et approche envisagée

Des travaux sur le sujet ont été réalisés dans l'équipe d'accueil, notamment dans le cadre d'un doctorat antérieur [Ism2016]. En particulier une approche basée sur la théorie des jeux non coopérative permettant de capturer les interactions entre attaquants et défenseurs a été proposée et appliquée à l'étude interdépendances de sécurité entre une infrastructure de communications dans [ILB2018]. Cela permet de caractériser des stratégies de sécurité (de détection ou de réaction) optimales à travers la

caractérisation de solution de ces jeux comme l'équilibre de Nash. Cependant, ces travaux ne modélisent les risques de sécurité qu'à travers leur impact sur les infrastructures sans modéliser de manière explicite le comportement de l'attaquant. Cela permet le cas échéant de dimensionner l'effort de détection devant être mis en place pour minimiser l'impact, mais pas de prévoir des stratégies de réaction.

Des travaux complémentaires, se sont basés sur une modélisation explicite du comportement de l'attaquant sous la forme d'un graphe d'attaques (voir par exemple [Kay2016] pour un état de l'art sur le sujet). Sur la base des informations contenues dans un graphe d'attaque et d'un ensemble de contre-mesures de défense disponibles, un processus de décision markovien sous contraintes (CDMP) est construit afin de générer une politique de réponse optimale en tenant compte des différentes contraintes définies par le défenseur (par exemple, l'existence d'un budget de défense maximal et de seuils maximaux tolérés pour les probabilités de compromission des équipements et des services critiques après le déploiement des contre-mesures de sécurité) [ZLA2018]. Cependant, cette approche ne permet pas de capturer réellement les interactions entre l'attaquant et le défenseur, et en particulier de prendre en compte des attaquants adaptant leur comportement à celui des défenseurs. Par ailleurs, ces travaux initiaux font l'hypothèses que l'on observation parfaitement l'évolution du scénario d'attaque (c-à-d que l'on sait exactement dans quel état du graphe d'attaques se trouve l'attaquant). Cette hypothèse s'avère être trop forte dans la réalité : l'hétérogénéité des capacités de détection introduit des incertitudes sur l'observation de l'état courant de la propagation de la menace, et complexifie ainsi la tâche du (ou des) défenseurs.

Afin de combler les limitations précédentes, l'approche envisagée est la suivante : étant donné un modèle d'attaque du système (tel qu'un graphe d'attaque), modéliser les interactions entre l'attaquant et le défenseur comme un jeu sur ce modèle d'attaque et utiliser des techniques de vérification de systèmes multi-agents pour déterminer les stratégies de détection et de réaction optimales. Récemment, les approches classiques de vérification sur modèles (« model checking ») ont été étendues aux systèmes multi-agents. Ces derniers sont des systèmes qui encapsulent le comportement de deux ou plusieurs agents rationnels interagissant entre eux de manière coopérative ou antagoniste, dans le but d'atteindre un objectif défini [Jam2015]. Cela permet de vérifier automatiquement des propriétés logiques sur un jeu. L'équipe d'accueil a récemment initiée des travaux investiguant cette piste, pour traiter le problème de la sélection dynamique des contre-mesures de sécurité, dans le contexte de la réponse aux incidents ([CDL2023] et [CLM2023]). Ces travaux ne sont qu'à un stade embryonnaire et nécessite de nombreux développement afin de pouvoir être appliqués de manière réaliste dans un contexte de supervision de sécurité. En particulier les points suivants pourront être étudiés :

- Considérer des extensions de jeux avec information imparfaite afin de prendre en compte les incertitudes liées à l'observation de l'état de l'attaquant ;
- Considérer des extensions probabilistes de la logique permettant de définir des objectifs sur le jeu afin de prendre en compte les probabilités de succès des attaques/contremesures ;
- Proposer une méthode permettant de synthétiser des stratégies optimales satisfaisant un objectif logique dans le contexte d'agents rationnels (on pourra s'inspirer de [FKL2010]).

En se basant sur cette approche, le doctorant devra fournir une méthodologie et des outils d'aide à la décision (algorithmes) qui devront être implémentés et validés sur des études de cas représentatives (par exemple dans le contexte des réseaux électriques intelligents).

Cadre de travail

Ce sujet de thèse est financé dans le cadre du projet SuperviZ[1], dédié à la supervision et l'orchestration de sécurité, faisant partie du programme et équipements prioritaires de recherche (PEPR) Cybersécurité[2] et s'inscrivant dans le cadre de la stratégie nationale pour la cybersécurité. Le doctorant sera inscrit à l'école doctorale de l'institut Polytechnique de Paris (ED626), dans le domaine « Informatique, Données

[1] https://files.inria.fr/superviz/
[2] https://www.pepr-cybersecurite.fr/le-pepr/,

et Intelligence Artificielle ». Il sera accueilli au sein du « Laboratoire Traitement et Communication de l'Information (LTCI)[3] » de Télécom Paris dans l'équipe « Systèmes embarqués critiques autonomes (ACES)[4] », et sera localisé dans le bâtiment de l'école se trouvant 19 Place Marguerite Perey, 91120 Palaiseau.

Qualifications et compétences requises

- M2 ou équivalent en Informatique
- Connaissances développées en cybersécurité et en méthodes formelles
- Langues : français et anglais

Comment candidater ?

Envoyer par mail à jean.leneutre@telecom-paris.fr et vadim.malvone@telecom-paris.fr , avant le 30 novembre 2023 :

- Une lettre de motivation,
- Un cv détaillé à jour,
- Copies des diplômes universitaires et relevés de notes détaillés pour le M1 et M2 (ou équivalents),
- Un document scientifique (rapport de stage, rapport de projet d'étude, article, …) rédigé par vos soins, si possible en anglais.

Références

[CDL2023] D. Catta, A. Di Stasio, J. Leneutre, V. Malvone, and A. Murano, *A Game Theoretic Approach to Attack Graphs*, ICAART, 2023.

[CLM2023] D. Catta, J. Leneutre, and V. Malvone, *Obstruction Logic: a Strategic Temporal Logic to Reason about Dynamic Game Models*, ECAI 2023.

[FKL2010] D. Fisman, O. Kupferman, and Y. Lustig, *Rational Synthesis*, TACAS 2010, LNCS 6015.

[ILB2018] Z. Ismail, J. Leneutre, D. Bateman, and L. Chen, *Managing Security Risks Interdependencies Between ICT and Electric Infrastructures: A Game Theoretical Analysis*, book chapter in Game Theory for Security and Risk Management From Theory to Practice, Birkhauser, 2018.

[Ism2016] Z. Ismail, *Optimal defense strategies to improve the security and resilience of Smart Grids***,** PhD Thesis, Paris, France, 2016.

[Jam2015] W. Jamroga, *Logical Methods for Specification and Verification of Multi-Agent Systems*, ICS PAS Publishing House, 2015.

[Kay2016] K. Kaynar, *A taxonomy for attack graph generation and usage in network security*, J. Inf. Secur. Appl., 29(C):27–56, 2016.

[LAC2016] R. M. Lee, M. J. Assante, and T Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case*, E-ISAC, 18 mars 2016.

[ZLA2018] Z. Ismail, J. Leneutre, and A. Fourati, *Optimal Deployment of Security Policies: Application to Industrial Control Systems*, EDCC, 2018.

[3] https://www.telecom-paris.fr/fr/recherche/laboratoires/laboratoire-traitement-et-communication-de-linformation-ltci

[4] https://www.telecom-paris.fr/fr/recherche/laboratoires/laboratoire-traitement-et-communication-de-linformation-ltci/les-equipes-de-recherche/systemes-embarques-critiques-autonomes-aces