Leurrage et Jumeau Numérique

Marwan ABBAS - SesameIT (mabbas.sesit@gmail.com),
Hervé DEBAR - Télecom Sud-Paris (herve.debar@telecom-sudparis.eu),
Jerome GOUY - SesameIT (jerome.gouy@sesame-it.com).

Résumé

La croissance des menaces et des enjeux liés aux attaques informatiques pousse à la mise point de nouveaux moyens pour renforcer la sécurité des systèmes d'information. L'utilisation de leurres complète l'arsenal existant dans le but d'améliorer les procédés de défense en profondeur. Par ailleurs, le déploiement de systèmes industriels cyber-physiques a encouragé l'émergence de jumeaux numériques, permettant d'étudier le fonctionnement de ces systèmes cyber-physiques par des mécanismes d'animation et de simulation. Les méthodes et les techniques spécifiques à la mise au point de jumeaux numériques peuvent servir à améliorer la mise au point de leurres et la *"deception"* en général. Nous chercherons ici à dresser un état des lieux concernant la conception de systèmes de leurre ainsi que la mise au point de jumeaux numériques. Nous montrerons ensuite que ce domaine offre des perspectives intéressantes du point de vue du leurrage.

Mots clé

Leurre, Honeypot, Interaction, Jumeau numérique

Abréviations

SSI: Sécurité des Systèmes d'Information

SI: Système d'Information

IDS: Intrusion Detection System (système de détection d'intrusions)

SR: Système Réel

JN: Jumeau Numérique

SIN: Système industriel

ICS: Industrial Control System (système de contrôle industriel)

Introduction

A l'heure où les systèmes numériques occupent une place de plus en plus importante dans le fonctionnement de toutes les organisations, la sécurité des SI est un enjeu primordial à tous les niveaux, des simples utilisateurs aux États. Celle-ci est souvent présentée comme un "jeu" opposant les "attaquants" aux "défenseurs". Celui-ci est néanmoins extrêmement déséquilibré. Pour arriver à ses fins, un attaquant se doit de compromettre une seule fois l'intégrité, la confidentialité ou la disponibilité d'une ressource numérique tandis que le défenseur n'a pas le droit à la moindre erreur. De plus, ces premiers possèdent une forte initiative du fait qu'il est très difficile de se prémunir d'un type d'attaque auquel on n'a jamais été confronté.

Ainsi, dans le but de rendre plus ardue la tâche de l'attaquant, de plus en plus d'organisations envisagent la mise en place de systèmes de *"deception"* ou de leurrage. Ceux-ci ont l'avantage de compléter efficacement les autres mesures défensives en s'inscrivant dans une démarche de "défense en profondeur". Ainsi, même s'il réussit à outrepasser les autres mesures de protection d'un SI, un attaquant peut "tomber dans le piège" du leurre, permettant aux défenseurs de détecter son activité ou d'analyser ses outils.

I-Leurre

1-Concepts

Le leurre n'est pas un concept nouveau. On le retrouve dans de nombreux domaines, du motif des papillons aux chars d'assaut gonflables de l'opération Fortitude. Dans le domaine de la SSI, le leurrage consiste à positionner au sein d'une architecture de SI des éléments laissés volontairement vulnérables à certaines attaques, mais sans intérêt réel pour les attaquants ou bien diffusant de fausses informations.

Ainsi, cette pratique se positionne sur trois axes de la sécurité [^Mairh]:

- La prévention
- La détection
- La réaction

Du fait de la présence de leurres piégés, l'initiative bascule pour partie du côté du défenseur. L'attaquant ne peut plus se contenter de cibler un équipement vulnérable, mais doit s'interroger sur la nature de celui-ci. De plus, en cas d'exfiltration de données, il doit aussi se demander si les informations obtenues sont pertinentes ou si elles ne sont qu'un piège prévu par les administrateurs. En dernier lieu, les informations obtenues grâce à l'analyse des opérations effectuées sur les leurres par des attaquants piégés peut mener à la construction de nouvelles règles de prévention (IPS). Grâce à cela, les leurres jouent un rôle dans la prévention des attaques au sein des infrastructures numériques.

Pour ce qui est de la détection des attaques, les leurres peuvent aussi jouer un rôle important. En effet, ceux-ci n'offrant pas de services réels aux utilisateurs, toute connexion ou tentative d'accès au leurre est un événement suspect. En plus de cela, un leurre avec lequel interagit un attaquant peut être observé et toutes ses opérations peuvent être conservées. Grace à cela, les nouveaux procédés ou les vulnérabilités exploitées avec succès peuvent être détectées. Ces méthodes peuvent ensuite être analysées, ce qui permet d'améliorer le reste de l'arsenal de détection, par exemple avec des nouvelles règles pour les IDS.

Enfin, le leurre offrant la possibilité à un attaquant de compromettre un système et d'en extraire des documents, il peut être envisagé comme un outil de réaction face aux intrusions. En effet, rien n'empêche d'insérer parmi les documents fictifs présents sur le leurre des fichiers "mouchards" permettant de retrouver les attaquants, ou même des fichiers malveillants dans le cadre d'une politique de hack-back. Pour cela, les aspects légaux spécifiques à chaque pays doivent être étudiés au cas par cas.

L'élément central du réseau de leurres est le "pot de miel" ("honeypot"). Il peut être constitué de plusieurs manières, un système réel, un système virtuel, une session d'utilisateur ou tout autre élément protégé. On peut classifier les honeypots en fonction de leur niveau d'interaction et de leur objectif [^Mokube]

et les situer ainsi sur deux axes. En mettant en place une architecture hybride avec plusieurs types de leurres différents, on peut s'adapter au mieux à nos besoins, comme montré sur la figure 1.

- **Niveau interaction**. Les différents honeypots sont divisés en fonction de leur niveau d'interaction et de leur complexité, allant du simple service émulé et non exploitable par un attaquant jusqu'à un système d'exploitation complet. Ceci permet une meilleure distinction des possibilités et des nécessités d'entretien de chaque type de leurre. Les impératifs de durcissement et de surveillance ne sont pas les mêmes dans les différents niveaux, ainsi que le coût en ressources et la complexité du déploiement.
- **Objectif**. Les leurres étudiés sont principalement divisés en deux catégories: les leurres de renseignement apportant des informations sur les usages des attaquants et les leurres de production directement installés au sein d'un réseau dans le but d'améliorer la sécurité de ceux-ci. [^Mairh]

Une architecture de leurres complète se doit donc d'intégrer plusieurs équipements placés différemment sur ces deux axes, pour permettre d'assurer au mieux le rôle de piège tout en s'adaptant au mieux aux ressources et aux besoins de l'utilisateur.

2-Enjeux de développement

Dans le cadre de la mise au point de systèmes de leurres à intégrer au sein des SI, il y a 4 enjeux principaux à prendre en compte[^Han]:

- **Réalisme**. Il est nécessaire que le fonctionnement de ces leurres soit proche du système dans lequel ils sont intégrés, afin de ne pas être détectés et/ou évités facilement par les attaquants. En contrepartie, il est nécessaire que l'intégration des leurres ne soit pas pénalisante pour le système, ne perturbe pas son fonctionnement ou ne permette pas d'obtenir des informations relatives à sa configuration.
- **Mise en œuvre**. Le réalisme peut être associé à un effort de mise en oeuvre (CAPEX) et de surveillance (OPEX) de ces leurres. Cet effort doit être proportionnel au gain et au risque. Dans cette optique, il convient de regarder dans quelle mesure les activités "PROTECT" et "DETECT" du NIST Cybersecurity Framework (CSF) peuvent être réalisées en partie sous forme de leurres.
- **Coût**. L'intégration de ces leurres dans un système opérationnel peut amener des effets de bord sur le fonctionnement nominal du système dans lequel ils sont intégrés. Par exemple, ils vont consommer des ressources (bande passante réseau, plages d'adresse IP) ou induire des modifications de fonctionnement (délai, etc.). Cette consommation de ressources peut souvent être irréversible; par exemple la mise en place d'adresses IP pour

des leurres peut les rendre à long terme inutilisables pour un fonctionnement nominal.

- **Efficacité**. Finalement, ces leurres doivent être attractifs pour les attaquants, et ce d'une manière qui ne perturbe pas indûment le système dans lequel ils sont intégrés ni éveille les soupçons quant à la nature réelle du système.

Ces enjeux peuvent être regroupés dans le tableau en figure 2, sourcé par la figure 3.

Des difficultés subsistent néanmoins dans la mise au point de systèmes de leurrage.

Une des difficultés est d'ordre légal et administratif. Les enjeux concernant la juridiction européenne et les leurres sont étudiés par Sokol [^Sokol]. Par exemple, la réglementation Européenne autour des données définit comme information personnelle *toute information pouvant être liée à une personne naturelle identifiable ou identifiée.* L'identification pouvant être indirecte, cette définition couvre un large périmètre. Par exemple, un adresse IP peut être considérée comme une donnée personnelle. Dans le cadre d'un leurre de production, la conservation de données pendant un temps court ou la résolution d'un incident ne pose pas de problème, mais dans le cadre d'un leurre de recherche dont les résultats seraient conservés longtemps, la question du consentement des personnes peut se poser.

Une autre difficulté dans la mise au point de systèmes de leurre vient du fait que le leurre peut être exploité par l'attaquant pour devenir un point de rebond menant vers d'autres attaques. Lors du déploiement du système, celui-ci doit offrir une surface d'attaque à l'attaquant tout en ne pouvant pas être réellement compromis. Cela implique un contrôle total et dans la durée de la sécurité du système et nécessite un entretien important et prolongé qui peut être un frein à la mise en place de solutions de leurrage.

II-Jumeau Numérique

1-Concepts

Le jumeau numérique est défini par Zhuang [^Zhuang] comme:

«Un modèle virtuel et dynamique dans le monde virtuel qui est pleinement cohérent avec son entité physique correspondante dans le monde réel et peut simuler les caractéristiques, le comportement, la durée de vie et les performances de son homologue en temps réel»

Plus simplement, on peut l'envisager comme un clone virtuel d'un système réel prévu pour évoluer en même temps que lui grâce à des algorithmes de simulation et à la collecte de données. Ces premiers permettent de lui assurer

un comportement cohérent avec celui du SR tandis que les seconds permettent de suivre en temps réel l'évolution des variables pertinentes du SR.

Le concept est étudié très tôt par la NASA. L'agence spatiale utilise des modèles physiques équivalents de certains modules des missions Apollo. L'augmentation de la puissance de calcul et des capacités des ordinateurs rendent plus tard possible la création de modèles numériques pour un coût bien plus faible et une utilisation plus flexible. L'idée est de pouvoir étudier à moindre coût "des conditions imprévisibles ou des erreurs qui auraient des effets catastrophiques" sans engager l'intégrité du système réel.

C'est pour cela, de nombreux autres acteurs industriels sont intéressés par le JN:

- Dassault l'envisage pour le suivi de systèmes complexes.
- General Electrics pour le suivi de l'état de santé de ses produits dans le temps.
- SIEMENS pour améliorer le rendement de ses machines outil.
- Tesla aspire à mettre au point un jumeau numérique pour chaque véhicule.
- etc.

Dans l'idée, le JN peut servir dans toutes les étapes du cycle de vie d'un système[^Eckhart], lors de sa conception, son fonctionnement et sa fin de vie.

- **Conception**. Le JN peut servir à la mise au point et aux premiers tests du système. Il permet plus de flexibilité et est moins cher qu'un ou plusieurs prototypes. De plus, si plusieurs éléments d'un système possèdent un JN, l'extension de celui-ci et les études d'intégration peuvent se faire numériquement.
- **Opération**. La maintenance peut être adaptée au besoin réel du système grâce aux données et aux simulations issues de l'analyse du JN. Ces possibilités de simulation permettent aussi de planifier et d'optimiser le fonctionnement du système réel sans risquer d'impacter la continuité opérationnelle de celui-ci.
- **Fin de vie**. Pendant la phase de fin de vie du système, le JN peut être utilisé pour enregistrer et retenir des informations sur le cycle de vie du produit pour améliorer les procédures de fonctionnement ou optimiser le retraitement de celui-ci.

C'est cette deuxième étape qui nous intéresse le plus dans le cadre de la mise au point de leurres.

2-Enjeux de développement et d'intégration

Les JN sont donc globalement envisagés dans l'industrie à des fins de sûreté, de sécurité ou de surveillance. Le concept n'est pas nouveau mais il est chaque fois plus d'actualité grâce aux progrès dans la simulation, la puissance de calcul et les

réseaux de capteurs. L'avènement de nouvelles technologies de communication telles que la 5G renforce cette tendance.

La modélisation se fait en deux parties, un modèle prédictif construit de façon abstraite et un modèle descriptif construit et amélioré grâce aux données collectées tout au long du cycle de vie du JN. Le premier simule le comportement du SR grâce à une théorisation de son comportement attendu tandis que le deuxième vise à représenter son fonctionnement par les mêmes mécanismes.

Lors de la conception, on doit garder à l'esprit trois enjeux principaux qui peuvent être regroupés dans un tableau en figure 4:

- Les enjeux techniques
- Les enjeux d'ingénierie
- Les enjeux "Business"

On peut néanmoins relever des obstacles au développement des JN. Grieves en relève trois majeurs[^Grieves]:

- **Compréhension du monde physique** La simulation au cœur du concept de JN nécessite d'avoir une compréhension très fine de la réalité physique du SR que l'on cherche à modéliser. Là où certains aspects sont très bien compris et modélisables, d'autres restent encore délicats à représenter malgré les progrès techniques, par exemple la résistance aux contraintes ou la dégradation des matériaux. Un JN efficace se construisant sur une modélisation la plus fidèle possible du monde réel, des progrès dans ce domaine sont attendus pour faciliter leur faisabilité.
- **Nombre d'états**. Une autre difficulté technique vient de la nécessité de traiter un très grand nombre de données issues d'un grand nombre de capteurs. Très vite, la gestion de centaines ou de milliers de paramètres pouvant être pris en compte pour les simulations risque de provoquer une variabilité trop élevée dans les états possibles du système virtuel, imposant une charge trop importante en terme de stockage ou de puissance de calcul.
- **Organisation cloisonnée**. Une difficulté majeure du déploiement d'un JN n'est pas technique mais culturelle et organisationnelle. Elle provient de le grande quantité de fonctions et de services impliqués dans son développement et son fonctionnement. Il est difficile de faire travailler de concert des services d'ingénierie électrique et mécanique, de télécommunications, de programmation et d'intégration des systèmes. De plus, cette coopération doit se faire tout au long du cycle de vie du produit, de la conception au démantèlement. Les attentes et besoins spécifiques ainsi que la difficulté des échanges d'information dans le temps et entre les services rendent la mise au point de JN très complexe.

L'intégration du jumeau numérique peut être flexible. Pour commencer, il peut fonctionner sur un équipement dédié comme être directement intégré dans l'équipement industriel. Ces deux possibilités offrent des avantages et des inconvénients. Néanmoins, pour des raisons de sécurité, il semble plus rigoureux

de séparer le leurre de l'équipement qu'il est censé protéger, les risques de débordement n'étant jamais nuls. Ce choix peut aussi impacter les coûts et les difficultés d'entretien. Cet aspect du cycle de vie du JN en tant que leurre ne doit pas être ignoré non plus. L'entretien du JN doit se faire avec deux idées en tête. Dans un premier temps, les briques logicielles employées dans la mise au point d'un double virtuel doivent être, de façon classique, mises à jour et adaptées en fonction de leurs évolutions et des vulnérabilités découvertes. Par exemple, les vulnérabilités concernant les plateformes de virtualisation doivent être traitées de façon prioritaire du fait du risque critique qu'elles font courir au JN et à l'ensemble du réseau sur lequel il fonctionne. Dans un second temps, l'entretien du JN doit aussi permettre de prendre en compte toutes les modifications qui sont apportées au système réel, dans sa configuration ou en cas de mises à jour de ses composants. Cela peut se faire de façon automatique en cas de changements fréquents ou simples (configuration, paramètres de fonctionnement, etc.) ou bien à la main s'ils sont exceptionnels ou impliquent un changement important (mise à jour du firmware, ajout de modules supplémentaires, etc.).

Les problématiques propres aux systèmes d'information telles que l'interconnexion, la gestion des accès ou la politique de sauvegardes existent aussi pour le JN mais elles n'offrent pas de spécificité particulière et peuvent être gérées de façon classique.

III-Applications Conjointes

1-Risque Cyber dans l'industrie

Les SI sont maintenant des systèmes critiques pour le bon fonctionnement des infrastructures cyber-physiques. Au delà de cela, les SIN sont chaque fois plus connectés pour leur contrôle et le transfert de données dans le cadre de l'industrie 4.0, mais ils ne sont pas construits avec les mêmes priorités que les SI. La où ces derniers accordent une grande importance à la confidentialité et à l'intégrité des données, les SIN sont pour leur part axés autour de la continuité opérationnelle et donc de la disponibilité[ˆKnowles]. En ce qui concerne les ICS, ils sont une cible de premier choix pour les attaquants. En effet, le rapport annuel de Dragos [ˆDragos] stipule que ses client ont déclaré en 2017 détecter en moyenne 14 vulnérabilité par mois dans leurs ICS. Malgré un travail de correction, 64% des patchs proposés pour mitiger ces vulnérabilités n'éliminaient pas complètement le risque. Sur ces vulnérabilités, 61% sont considérées comme sévères car provoquant une perte de contrôle et de visibilité sur les opérations industrielles.

Une compromission de la partie numérique d'un système ou service peut impacter des chaînes d'approvisionnement ou le fonctionnement d'infrastructures critiques dans des domaines tels que la distribution d'énergie [ˆKshetri] ou la santé. Pour cela, les attaques et les malfonctionnements au sein des SI peuvent avoir des impacts catastrophiques sur les domaines d'application que sont les services

essentiels, énergie, transports, etc. C'est pourquoi il est nécessaire d'envisager la sécurité des SI avec autant de rigueur que la sûreté de ces domaines industriels. Pour cela, les JN peuvent être un outil supplémentaire afin de compléter l'arsenal existant de la SSI.

Ces deux constats, des vulnérabilités fréquentes et difficiles à mitiger ainsi que le fort impact potentiel des attaques, font qu'il est nécessaire de renforcer la sécurité des SIN. Pour cela, un travail de fond est nécessaire sur le développement de leur Hardware et leur Software qui intègrent encore des vulnérabilités structurelles [ˆDragos]. Il est aussi nécessaire de compléter les outils de sécurité existants.

2-Le Jumeau Numérique comme outil de leurrage

Une piste intéressante pour compléter l'arsenal des solutions de sécurité proposé aux acteurs industriels est offerte par la conjonction entre le JN et les solutions de leurrage.

De par ses fonctions détaillées dans la section précédente, le JN peut être considéré comme un outil nouveau permettant de créer des leurres et de les inclure dans les systèmes opérationnels. Cela permet de détourner l'attention des systèmes réels, réduisant drastiquement les impacts potentiels des attaques réussies. L'analyse des traces et des journaux du JN permet d'analyser les méthodes des attaquants ainsi que leurs outils sans avoir à déployer de système réel coûteux ni risquer d'affecter la continuité opérationnelle. On peut aussi découvrir en amont les opérations d'attaque organisées grâce aux alertes soulevées au plus tôt par le JN.

Quatre objectifs principaux sont à garder à l'esprit lors de la mise au point d'un JN en vue de l'utiliser à des fins de leurrage. Ces objectifs sont à la fois liés à la nature du jumeau numérique et à sa fonction de leurre.

- La scalabilité du JN. C'est la capacité du JN utilisé en tant que leurre à être pertinent à plusieurs échelles et donc à être déployé dans n'importe quel réseau. On retrouve aussi là l'impératif du leurre qu'est l'adaptation aux ressources disponibles ainsi que la capacité à gérer un grand nombre d'alertes et de données sans surcharger le réseau hôte. L'importance de ce dernier point ne doit pas être sous estimée, en effet, un jumeau numérique qui consommerait un trop grand nombre de ressources en capacités de calcul, capacités de réseau ou en besoins d'entretien risquerait, comme toute autre solution mal calibrée, de devenir un poids ne compensant pas les avantages qu'il apporte.
- L'interopérabilité renvoie à la capacité que doit avoir le leurre à assurer sa fonction dans des cadres très différents. La même structure "cible offerte -> collecte de données -> analyse" doit être utilisable et pertinente avec un leurre simulant un serveur web aussi bien qu'un équipement réseau ou un automate industriel. Les coûts de production et de développement sont par exemple grandement optimisées si plutôt que de mettre au point

une fonctionnalité de leurre pour chaque jumeau numérique, un outil de leurrage intégrable aux jumeaux numériques existants est crée qui puisse être configuré et adapté pour différents types d'équipement.

- La capacité d'expansion renvoie au fait que les leurres doivent pouvoir être à la fois interactifs et indépendants. Ils peuvent simuler du trafic entre eux pour s'approcher au mieux d'un système réel mais l'ajout ou le retrait d'éléments de leurre doit être suivi d'une reconfiguration des interactions pour veiller à maintenir un leurre crédible.
- La fidélité rejoint la problématique de réalisme du leurre. Un leurre dont la configuration est le reflet des informations obtenues par les capteurs d'un système réel apparaît comme plus réaliste face à un attaquant. La structure et l'architecture peuvent renforcer cette fidélité.

3-Le Jumeau Numérique dans la Cybersécurité

Au delà du seul rôle de leurre, le jumeau numérique peut offrir d'autres outils dans le cadre de la cybersécurité. Une de ses possibilités vient par exemple de sa capacité à simuler des comportements humains [^Becue] ce qui peut permettre d'adapter les systèmes aux actions des utilisateurs et d'améliorer les procédures de sensibilisation et de formation. De plus, cette fonctionnalité peut aussi être intéressante dans l'optique du leurrage, du fait de la grande proportion d'attaques causées par des imprudences dans le comportement des utilisateurs.

Comme pour les avantages qu'il apporte dans le champ industriel, le JN offre des opportunités pour renforcer la sécurité non pas uniquement pendant le fonctionnement des SIN, mais tout au long de leur cycle de vie.

- **Conception**. Dès la phase de conception, le JN peut servir à intégrer la sécurité dés les premières étapes du développement. Que ce soit en simulant des attaques ou en mettant en évidence la surface d'attaque offerte par le système. Au delà, des premiers tests ou audits peuvent être réalisés sur le JN pour permettre de détecter des vulnérabilités fonctionnelles avant la finalisation du système.
- **Opération**. Pendant la phase de fonctionnement du SIN, le JN apporte plusieurs opportunités pour renforcer la sécurité. Des attaques peuvent être détectées grâce à la recherche d'anomalies dans les simulations[^Rubio] effectuées à partir des données récoltées sur le SR. L'observation continue du JN peut aussi permettre de détecter les erreurs de configuration accidentelles créant un risque ou bien malveillantes, et donc indices d'intrusion. En plus de cela, le JN offre une surface d'audit ou d'entraînement permettant de tester la sécurité du SIN sans risquer d'affecter la continuité opérationnelle.
- **Fin de vie**. Sur la phase de fin de vie, le JN offre deux opportunités majeures. Premièrement, il permet la conservation de données[^Grieves]

concernant la sécurité après la décommission des SIN. Ces données pourront être réutilisées pour améliorer les procédures et les configurations lors du déploiement d'un nouvel équipement. De plus, le jumeau permet d'aider à l'assainissement des médias[^Eckhart] conformément aux directives NIST SP 800-88[^Nist]

Conclusion

A l'heure ou la sécurité informatique devient un enjeu primordial non seulement pour les systèmes numériques mais aussi pour les systèmes physiques ou industriels connectés, il convient d'apporter de nouveaux outils dans le but d'améliorer les éléments de défense existants. Nous avons discuté en quoi les systèmes de leurres offrent un outil de sécurité adapté aux enjeux évoqués et nous avons mis en avant les possibilités qu'offre le jumeau numérique dans la mise en place de tels systèmes. Nous avons listé les difficultés à prendre en compte lors du développement et du déploiement de systèmes de leurres et de jumeaux numériques. Plus de travaux sont nécessaires sur ce sujet et la mise en place d'expérimentations en laboratoire et avec des acteurs industriels permettrait de confronter les attentes théoriques aux risques réels rencontrés par les systèmes Cyber-Physiques.

Ressources

[^Mairh] Mairh, A., Barik, D., Verma, K., & Jena, D. (2011, February). "Honeypot in network security: a survey. In Proceedings of the 2011 international conference on communication, computing & security" (pp. 600-605). ACM.

[^Mokube] Mokube, I., & Adams, M. (2007, March). "Honeypots: concepts, approaches, and challenges." In Proceedings of the 45th annual southeast regional conference (pp. 321-326). ACM.

[^Han] Xiao Han, "Mesure et Supervision de la Sécurité du Point de Vue d'un Fournisseur de Services", Thèse de doctorat, 25 septembre 2017.

[^Sokol] Sokol, P., Míšek, J. & Husák, M. "Honeypots and honeynets: issues of privacy". EURASIP J. on Info. Security 2017, 4 (2017). https://doi.org/10.1186/s13635-017-0057-4

[^Zhuang] "Digital twin-based smart production management and control framework for the complex product assembly shop–floor." International Journal of Advanced Manufacturing Technology, 96(1–4), 1149–1163.

[^Eckhart] Eckhart, Matthias & Ekelhart, Andreas. (2019). "Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook." 10.1007/978-3-030-25312-7_14.

[ˆGrieves] Grieves, Michael & Vickers, John. (2017). “Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems”. 10.1007/978-3-319-38756-7_4.

[ˆKnowles] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P. & Jones, K. (2015), “A surveyof cyber security management in industrial control systems”,International Journalof Critical Infrastructure Protection9, 52 – 80.

[ˆDragos] Dragos, Inc., “Industrial Control Vulnerabilities: 2017 in Review”, Hanover, MD, 1 March 2018

[ˆBecue] Becue, Adrien & Maia, Eva & Feeken, Linda & Borchers, Philipp & Praça, Isabel. (2020). “A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future”, Applied Sciences. 10. 4482. 10.3390/app10134482.

[ˆRubio] Rubio, J. E., Alcaraz, C., Roman, R. & Lopez, J. (2017), “Analysis of intrusion detection systems in industrial ecosystems”,in‘14th International Conference

[ˆNist] NIST “Special Publication 800-88 Revision 1 Guidelines for Media Sanitization” Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine, Computer Security Division, Information Technology Laboratory

[ˆKshetri] N. Kshetri and J. Voas, “Hacking Power Grids: A Current Problem,” in Computer, vol. 50, no. 12, pp. 91-95, December 2017, doi: 10.1109/MC.2017.4451203.

Figures

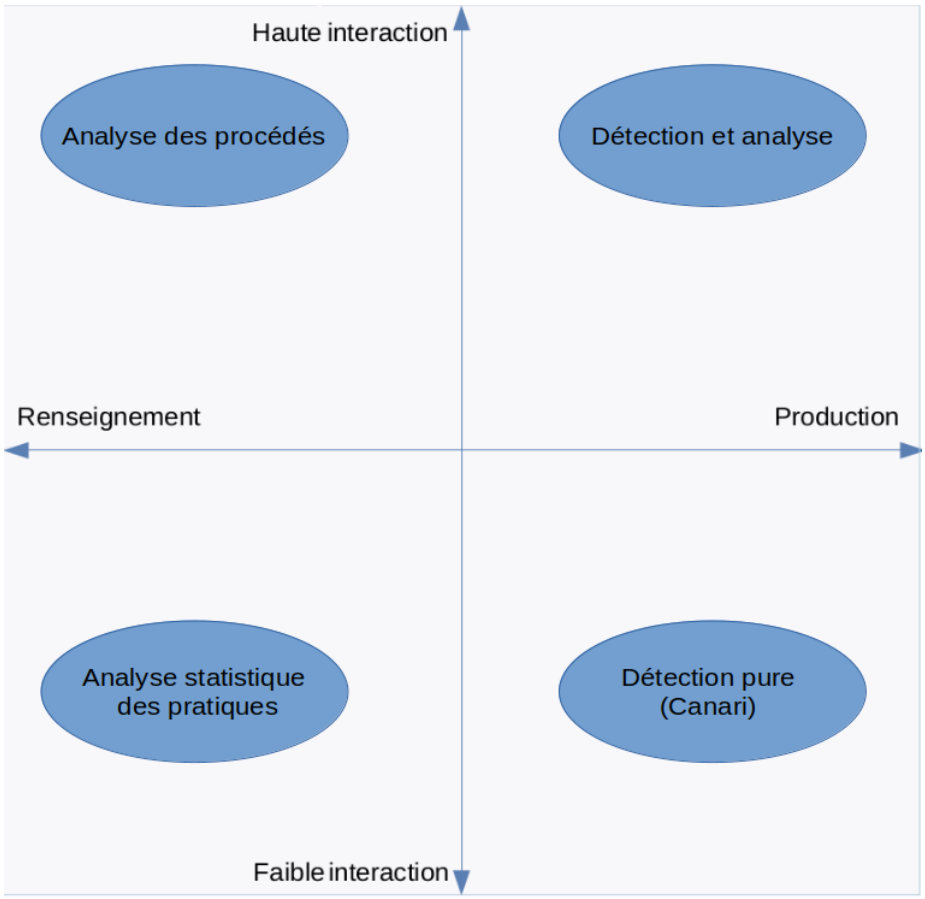

Figure 1: Positionnement des systèmes de leurre

Enjeu	Problématiques	Mise en Œuvre et commentaires
Réalisme	Aspect réel du leurre	Le leurre ne doit pas apparaître comme tel, mais comme un élément vulnérable réel.
		Un soin particulier doit être apporté lors de la construction du leurre, pour que l'inspection n'éveille pas les soupçons de l'attaquant. [Fan]
	Intégration dans architecture et le réseau	Intégration fonctionnelle : Le leurre doit s'intégrer sans altérer négativement l'architecture du réseau ni ses performances.
		Intégration réaliste : Le leurre doit s'intégrer harmonieusement dans son environnement pour ne pas paraître suspicieux (age de la version, type d'équipement, etc.)
	Crédibilité des vulnérabilités dans le contexte	Les vulnérabilités placées dans les leurres doivent être judicieusement choisies pour ne pas sembler artificielles.
	Camouflage de la virtualisation	Les méthodes de virtualisation peuvent dans certains cas être cachées pour améliorer le camouflage du leurre en élément réel. [Dornseif]
	Prise en compte des méthodes d'évasion	Les techniques d'évasion doivent être prises en compte pour qu'un leurre compromis n'affecte pas la sécurité du reste du réseau.
Mise en œuvre	Intégration au réseau réel	Le leurre doit pouvoir faire partie intégrante du réseau sans altérer son fonctionnement et en utilisant ses fonctionnalités (DNS, DHCP) [Artail]
		Le leurre doit être accessible pour les attaquants mais son accès doit être régulé au sein du réseau pour limiter les accès aux administrateurs et attaquants internes.
	Connectivité	Les leurres publics doivent être accessibles depuis l'extérieur du réseau.
		Les leurres au sein d'un réseau privé ne doivent pas être accessibles de l'extérieur et on doit limiter l'accès que des utilisateurs internes pourraient y avoir par mégarde.
	Accès légitime aux infrastructures	Le leurre doit pouvoir accéder aux ressources privées du réseau (DNS, DHCP, etc.) mais aussi aux ressources publiques en cas de nécessité.
	Déploiement et configuration	Le leurre doit être déployable de façon dynamique et simple. Depuis une interface fonctionnelle, on doit pouvoir paramétrer celui-ci sans être un expert.
	Protection et durcissement	Les équipements intégrant les systèmes de leurre doivent être durcis pour remplir les critères de sécurité adaptés (CC, CSPN, etc.)
	Collecte et traitement des données	Au delà des alertes, le leurre doit collecter des données concernant les outils, le timing et les procédés mis en œuvre par l'attaquant. [Nicomette]
		Le système de leurrage doit pouvoir traiter ces données de façon à en extraire des retours plus intéressants pour l'étude des procédés et des attaques que des logs bruts. [Zhan]
	Considérations légales	Les systèmes de leurre sont encadrés légalement. Il ne doivent pas être une incitation à l'attaque ou une plateforme de rebond pour les pirates. Il faut s'adapter aux différentes juridictions. [Mokube]
Coût	Coûts de mise en place	La solution a un coût de mise en place en terme d'ajout de matériel, de licences ou de formation/apprentissage pour les équipes. Il faut limiter ce coût.[Tian]
	Coûts d'entretien	L'entretien est celui des équipements, des licences ainsi que le temps supplémentaire des équipes. Il faut aussi prendre en compte les coûts de surveillance et la charge supplémentaire sur le réseau. [Tian]
	Effets de bord	Des effets de bord existent, notamment sur les plages d'adressage ou le trafic réseau généré. Ils doivent être pris en compte [Artail]
Efficacité	Détection des attaques	Les attaques doivent être détectées au plus vite. Les activités suspectes doivent lever une alerte immédiatement. [Zuzcak]
		Les faux-positifs doivent être le plus rares possible et les faux négatifs impossibles pour que l'outil soit le plus fiable possible. [Agnaou]
	Remontée des alertes	Les alertes doivent être efficaces. Pour cela, elles doivent être rares et précises, une alerte ne doit pas être un cas à examiner mais une attaque en cours. [Agnaou]
	Création de règles de détection	Il faut pouvoir automatiser l'analyse des procédés d'attaque pour permettre la création de règles de détection. Une nouvelle attaque effectuée sur un leurre doit devenir détectable par les IDS. [Matheus]
	Possibilités de contre	Le déploiement de fausses informations, telles que des comptes-leurre ou des identifiants-leurres peut permettre aux leurres d'adopter un rôle de contre attaque. [Mokube]
		Les leurres peuvent permettre l'envoi de fichiers piégés dans le cadre d'une politique de « hack-back » ou d'attribution des attaques. [Djanali]

Figure 2: Enjeux de développement des leurres

Sources	Dornseif	Dornseif, Maximillian & Holz, Thorsten & Müller, Sven. (2005). Honeypots and Limitations of Deception.. 235-252.
	Zhan	Z. Zhan, M. Xu and S. Xu, "Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1775-1789, Nov. 2013, doi: 10.1109/TIFS.2013.2279800.
	Zuzcak	Zuzcak, Matej & Sochor, Tomas & Sokol, Pavol. (2015). Definition of Attack in Context of High Level Interaction Honeypots. Software Engineering in Intelligent Systems. 349. 155-164. 10.1007/978-3-319-18473-9_16.
	Nicomette	Vincent Nicomette, Mohamed Kaâniche, Eric Alata, Matthieu Herrb. Set-up and deployment of a high-interaction honeypot: experiment and lessons learned. Journal in Computer Virology, Springer Verlag, 2011, 7 (2), pp.143-157 10.1007/s11416-010-0144-2 hal-00762596
	Mokube	Mokube, I., & Adams, M. (2007, March). Honeypots: concepts, approaches, and challenges. In Proceedings of the 45th annual southeast regional conference (pp. 321-326). ACM.
	Artail	Hassan Artail, Haidar Safa, Malek Sraj, Iyad Kuwatly, Zaid Al-Masri, A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks, Computers & Security, Volume 25, Issue 4, 2006, Pages 274-288, ISSN 0167-4048
	Matheus	Matheus, Pedro & De Castro, Leandro. (2014). Extracting IDS Rules from Honeypot Data: A Decision Tree Approach.
	Djanali	Djanali, Supeno & Arunanto, Fx & Pratomo, Baskoro & Baihaqi, Abdurrazak & Studiawan, Hudan & Shiddiqi, Ary. (2014). Aggressive web application honeypot for exposing attacker's identity. 212-216. 10.1109/ICITACEE.2014.7065744.
	Agnaou	Agnaou, Abdeljalil & Abou, Anas & Kalam, Anas & Ouahman, Abdellah & De, Mina. (2016). Automated technique to reduce positive and negative false from attacks collected through the deployment of distributed honeypot network. International Journal of Computer Science and Information Security ISSN:1947-5500. 14.
	Tian	Tian, Wen & Ji, Xiao-Peng & Liu, Weiwei & Liu, Guangjie & Lin, Rong & Zhai, Jiangtao & Dai, Yuewei. (2019). Defense Strategies Against Network Attacks in Cyber-Physical Systems with Analysis Cost Constraint Based on Honeypot Game Model. Computers, Materials & Continua. 58. 193-211. 10.32604/cmc.2019.05290.
	Fan	Fan, Wenjun (2019) HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design. IEEE Journal on Selected Areas in Communications, 37 (3). 683 -697. ISSN 0733-8716

Figure 3: Sources du tableau des leurres

Enjeu	Problématiques	Mise en Œuvre et commentaires
Technique	Communication	Des capteurs adaptés doivent permettre de faire le lien entre l'état du jumeau réel et l'état simulé du JN. Les données peuvent être volatiles (position des opérateurs, capacité des machines, etc) ou non-volatiles (listes de machines, dimensions, etc.)
		Les architectures peuvent varier, ont été proposés des systèmes client-serveur, maître-esclave, RESTful, etc. Les protocoles sont tirés de la pile IP ou des protocoles industriels classiques.
	Acquisition des données	Les communications doivent permettre au JN d'acquérir des données sur son jumeau réel. L'acquisition doit être rapide, fiable et économe.
	Représentation et gestion des données	Les données sont hétérogènes et issues de capteurs variés. Elles sont collectées par des capteurs différents et donc potentiellement, l'interopérabilité est à assurer.
		Les données doivent être stockées dans des structures adaptées. Pour cela, des structures de bases de données ainsi que des langages de représentation et d'ontologie sont envisagés.
	Processing	Les données hétérogènes doivent être normalisées et traitées pour servir les simulations et permettre un suivi du jumeau réel. Pour cela, des outils de machine learning et de gestion de données sont utilisables.
Ingénierie	Gestion du cycle de vie	Le JN peut permettre de suivre le produit pendant tout son cycle de vie. Des fonctionnalités sont envisageables dans les phases de conception, de production, de distribution, d'utilisation et pour la fin de vie.
		Pendant toute la phase d'utilisation, le JN peut permettre d'évaluer le fonctionnement et de reconfigurer le produit pour l'optimiser à partir des données collectées et des simulations
	Production du produit	Le JN peut être construit avec une approche modulaire, ce qui facilite la création de nouveaux produits et réduit les coûts de conception.
		Le JN des outils de production permet d'optimiser leur utilisation pour améliorer leur efficacité et les procédés de fabrication
	Interaction jumeau-original	Conceptuellement, les informations et les données disponibles autour du système réel doivent être prises en compte par le JN. Le JN est une première étape vers un Système-Cyber-Physique complet.
Business	Stratégie	L'usage de technologies de JN permet d'allouer efficacement des ressources et d'améliorer la prise de décision. Ceci permet d'obtenir des avantages stratégiques à plusieurs niveaux dans la plupart des secteurs industriels.
	Marché	Le JN permet d'explorer à moindre coût des modifications des produits existants pour satisfaire au mieux les besoins des clients grâce à des services plus adaptés
		Facilite la vente de lots « produit-service » où une valeur est ajoutée par le vendeur tout au long de la durée de vie du produit
	Valeur ajoutée et Potentiel	Le JN permet la création de valeur ajoutée grâce à de meilleurs produits et à l'amélioration des processus internes.
		Il s'inscrit totalement dans la perspective de « smart manufactoring ». Le concept est applicable à des milieux émergents tels que la réalité virtuelle ou plus classiques dans l'éducation ou la santé.

Figure 4: Enjeux de développement du JN