Génération de données pour l'analyse et la détection d'anomalies dans les systèmes cybernétiques navals

Type de contenu : Texte

Type de médiation : b

Type de support : Ressource dématérialisée

Titre(s) : Génération de données pour l'analyse et la détection d'anomalies dans les systèmes cybernétiques navals / Clet Boudehenn ; sous la direction de Abdel-Ouahab Boudraa et de Yvon Kermarrec

Auteur(s) : Boudehenn, Clet (1995-....)

Autre(s) auteur(s) : Boudraa, Abdel-Ouahab (19..-....)
Kermarrec, Yvon (1962-....)
Chonavel, Thierry
Snoussi, Hichem (19..-....)
Tabbane, Nabil Ammar (1967-....)
Francq, Julien
Salamatian, Kavé (19..-....)
Cexus, Jean-Christophe (1977-....)
École nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire 2017-....
École doctorale Mathématiques et sciences et technologies de l'information et de la communication Rennes
Laboratoire en sciences et techniques de l'information, de la communication et de la connaissance

Production : 2022

Titre traduit ajouté par le catalogueur : Data generation for anomaly detection in naval cybernetics systems eng

Autres classifications : 004

Classification décimale Dewey : 004

Note sur le titre et les responsabilités : Titre provenant de l'écran-titre

Note sur la responsabilité : Ecole(s) Doctorale(s) : École doctorale Mathématiques et sciences et technologies de l'information et de la communication (Rennes)
Partenaire(s) de recherche : Equipe Communication System Design (Laboratoire), Département Mathematical and Electrical Engineering (Laboratoire), Laboratoire en sciences et techniques de l'information, de la communication et de la connaissance (Laboratoire)

Autre(s) contribution(s) : Thierry Chonavel (Président du jury) ; Abdel-Ouahab Boudraa, Yvon Kermarrec, Hichem Snoussi, Nabil Ammar Tabbane, Julien Francq, Kavé Salamatian, Jean-Christophe Cexus (Membre(s) du jury) ; Hichem Snoussi, Nabil Ammar Tabbane (Rapporteur(s))

Note de thèses et écrits académiques : Thèse de doctorat Informatique Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire 2022

Résumé ou extrait : De nos jours plus de 90% du transport de marchandises passent par les voies maritimes. Les systèmes navals représentent une part indéniablement stratégique pour le commerce international et les activités militaires. Les systèmes présents à bord sont de plus en plus informatisés de sorte à optimiser les capacités opérationnelles, la navigation, la gestion des opérations et les performances. Pour atteindre ces objectifs, les systèmes cybernétiques navals ont connu, au cours de la dernière décennie, une transformation numérique globale. De nos jours, les systèmes de l'information et les systèmes opérationnels ont fortement convergé en termes de fonctionnement. Cependant, ces changements majeurs ont rendu ces systèmes vulnérables et ont considérablement augmenté la surface d'attaques et les risques d'incidents. Ces systèmes sont d'ailleurs devenus une cible de choix pour les pirates informatiques au regard des préjudices potentiels. En conséquence, la prise en compte de ces vulnérabilités dans ce secteur mondialisé doit devenir une problématique de premier plan à en croire les enjeux stratégiques, économiques et géopolitiques. Dans cette thèse nous proposons une méthodologie pour la génération de données réalistes dédiées à l'amélioration de la cybersécurité des systèmes cybernétiques navals. Dans ce sens, nous avons pu élaborer un certain nombre de scénarios de cyberattaques propres aux Systèmes de Contrôles Industriels ainsi que des cas de falsification GNSS à travers plusieurs cas d'études pour combler le manque de données dans le secteur. La génération de données réalistes nous a permis de proposer une méthodologie d'extraction de caractéristiques originale adaptée aux méthodes de détection d'anomalie dans le but d'améliorer les systèmes de détection d'intrusion. Au cours de ces recherches, nous nous sommes appuyé sur une plate-forme de simulation numérique représentant toute la partie fonctionnelle et opérationnelle que l'on peut retrouver a bord d'un navire. Par ailleurs, toutes les expériences réalisées et outils développer au cours de cette thèse viennent corroborer cette plate-forme qui propose un degré de réalisme dédié à la formation et à la communauté scientifique.
Nowadays, more than 90% of the goods transportation is made by sea. Naval systems are strategic part of international trade and military activities. Onboard systems are increasingly computerized to optimize operational capabilities, navigation, operations management and performance. To achieve these objectives, naval cyber systems have known a global digital transformation over the past decade. Today, information systems and operational systems have strongly converged in terms of operation. However, these major changes have made these systems vulnerable and have significantly increased the attack surface and risk of incidents. These systems have become a prime target for hackers in terms of potential harm. As a consequence, taking into account these vulnerabilities in this globalized sector must become a major issue considering the strategic, economic and geopolitical stakes. In this thesis we propose a methodology for the generation of realistic data to improve the cybersecurity of naval cybernetics systems. We have been able to develop a number of cyberattack scenarios specific to Industrial Control Systems as well as GNSS tampering cases through several case studies in response to the critical lack of data in the sector. The generation of realistic data allowed us to propose an original feature extraction methodology adapted to anomaly detection methods in order to improve intrusion detection systems capacities. We relied on a numerical simulation platform representing all the functional and operational capacities similar to a real ship. In addition, all the experiments and tools developed during this thesis

support this platform which proposes a degree of realism dedicated to training and research community.

Configuration requise : Configuration requise : un logiciel capable de lire un fichier au format : PDF

Sujet(s) : Détection d’anomalie
Génération de données
Systèmes de contrôles industriels
Systèmes de positionnement par satellites
Système de détection d'intrusion
Cybersécurité maritime

Sujet - Nom commun : Détection des anomalies (informatique)
Modélisation des données (informatique)
Systèmes de détection d'intrusion (informatique)
Cyberdéfense
Transports maritimes

Forme, genre ou caractéristiques physiques : Thèses et écrits académiques

Adresse électronique et mode d'accès : http://www.theses.fr/2022IMTA0336/document||Accès au texte intégral
http://www.theses.fr/2022IMTA0336/abes||
https://tel.archives-ouvertes.fr/tel-04007599||