Détection contextuelle de cyberattaques par gestion de confiance à bord d'un navire

Type de contenu : Texte

Titre(s) : Détection contextuelle de cyberattaques par gestion de confiance à bord d'un navire [texte imprimé] / sous la direction de Gouenou Coatrieux et de Cyril Ray

Auteur(s) : Coste, Benjamin

Autre(s) responsabilité(s) : Coatrieux, Gouenou (Directeur de thèse)
Jousselme, Anne-Laure (958)
Nana Tchamnda, Laurent (956)
Napoli, Aldo (958)
Ray, Cyril (Directeur de thèse)
Institut de recherche de l'École navale - 981
Laboratoire de traitement de l'information médicale (Brest, Finistère) - 981
École doctorale Mathématiques et sciences et technologies de l'information et de la communication (Rennes) École doctorale associée à la thèse - 996
École nationale supérieure Mines-Télécom Atlantique Bretagne Pays de Loire Organisme de soutenance - Organisme de soutenance

Description matérielle : 1 vol (V-154 p.) ; 30 cm

Note de thèses et écrits académiques : Thèse Thèse de doctorat 2018 École nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire

Résumé ou extrait : Dans le domaine maritime, la maîtrise de la navigation et de la conduite d'un navire sont deux aspects essentiels pour la bonne marche et la sécurité du navire, des personnels et la préservation de l'environnement maritime. Or, les navires modernes embarquent de plus en plus de technologies informatisées, connectées et automatisées pour gérer ces fonctions primordiales. Ces technologies (capteurs, actionneurs, automates, logiciels) qui constituent le système d'information (SI) d'un navire peuvent cependant être leurrées ou corrompues par un tiers, remettant ainsi en cause la confiance qui leur est accordée. Dans ce contexte, une nouvelle approche de détection des falsifications des informations fondée sur l'évaluation de la confiance dans les composants du SI est proposée. Du fait de leur complexité, les systèmes d'information des navires peuvent être considérés comme des ensembles de blocs fonctionnels inter-reliés qui produisent, traitent et reçoivent des informations. La confiance d'un bloc fonctionnel producteur d'information est évaluée au travers de sa capacité, divisée en deux composantes (compétence et sincérité), à rendre compte de la situation réelle du navire. Elle se propage ensuite, à l'instar de l'information, aux autres entités du système, quelle que soit leur complexité. Différents scénarios ont été expérimentés grâce à l'élaboration d'un simulateur. La variabilité de la confiance face à des altérations volontaires d'informations numériques permet de déduire la survenue d'une attaque ainsi que sa cible sous certaines conditions. Sans se restreindre aux systèmes navals, l'approche proposée permet de s'adapter à une grande variété de situations incluant le facteur humain. Les travaux de cette thèse ont été soutenus et co-financés par la région Bretagne ainsi que la Chaire de Cyber

Défense des Systèmes Navals impliquant l'École navale, IMT Atlantique, Naval Groups et Thales

Sujet(s) : Confiance
Thèses et écrits académiques
Gestion des données (systèmes d'information)
Cyberdéfense