Centre d'Etudes Doctorales : Sciences et Techniques et Sciences Médicales

Avis de Soutenance

THESE DE DOCTORAT

Présentée par

Madame ASMAE ZNITI

Discipline : Génie Electrique
Spécialité : Télécommunications

Sujet de la thèse

Hardware Implementation of an Authentication-based Prototype of Secure Automotive Embedded CAN Systems

Formation Doctorale " Sciences de l'Ingénieur, Sciences Physiques, Mathématiques et Informatique"

Thèse présentée et soutenue **le samedi 23 septembre 2023 à 10h** au centre de Conférence à la Faculté des Sciences et Techniques de Fès, devant le jury composé de :

Nom et Prénom	Titre	Etablissement	
Mohamed EL HAMMOUMI	PES	Faculté des Sciences et Techniques de Fès	Président
Jalal SABOR	PES	Ecole Nationale Supérieure d'Arts et Métiers de Meknès	Rapporteur
Anass MANSOURI	PES	Ecole Nationale des Sciences Appliquées de Fès	Rapporteur
Hassane EL MARKHI	PES	Faculté des Sciences et Techniques de Fès	Rapporteur
Abdelhamid BENALI	PES	Ecole Nationale des Sciences Appliquées Oujda	Examinateur
Hicham GHENNIOUI	PES	Faculté des Sciences et Techniques de Fès	Examinateur
Driss TAHRI	PES	Faculté des Sciences et Techniques de Fès	Examinateur
Nabih EL OUAZZANI	PES	Faculté des Sciences et Techniques de Fès	Directeur de Thèse

Laboratoire de recherche : Signaux, Systèmes et Composants
Etablissement : Faculté des Sciences et Techniques de Fès

Résumé de la thèse

Cette étude présente une nouvelle méthode de sécurité visant à améliorer la fiabilité et la sécurité de la communication entre les différents nœuds du bus de données (CAN) automobile. Cette approche repose sur l'utilisation d'un code d'authentification robuste, fondé sur un algorithme de hachage, intégré à une architecture adaptative incluant un nœud de surveillance. Ce dernier a pour fonction d'authentifier chaque calculateur et de vérifier le code d'authentification de message (MAC) associé à chaque trame circulant sur le bus. Afin de déterminer l'algorithme optimal pour la technique proposée, une étude comparative a été menée, impliquant les finalistes de la troisième ronde de SHA-3 compétition ainsi que les versions les plus récentes des algorithmes de hachage. Cette analyse a été réalisée à l'aide d'un microcontrôleur PIC32 et d'un circuit FPGA ZYNQ afin de simuler des scénarios automobiles réalistes, en mettant particulièrement l'accent sur la vitesse d'authentification. En conséquence, un classement des algorithmes a été généré en fonction de leurs métriques spécifiées, permettant ainsi la sélection de l'algorithme de hachage Blake3 comme étant le plus approprié. Par ailleurs, dans le but de souligner les enjeux de sécurité des systèmes CAN intégrés dans l'industrie automobile, un prototype concret est élaboré et mis en œuvre, mettant en évidence les vulnérabilités inhérentes à ces réseaux. Cette conception expérimentale sert également à évaluer l'efficacité du modèle proposé en exposant le système à diverses attaques. L'évaluation confirme la capacité de la plateforme développée à détecter les événements malveillants, tout en respectant les exigences de l'industrie automobile en termes de temps de traitement. Par conséquent, la transmission de données peut s'effectuer via un bus CAN amélioré, conformément au protocole standard, sans avoir le risque de subir d'interception ni d'altération de la part d'entités non autorisées. Il est à noter que ce prototype ne nécessite aucun changement majeur au niveau matériel ni de modification du protocole CAN existant, ce qui le rend fortement réalisable et performant.

Mots clés : Bus CAN, Cyber attaques, Véhicules, Cyber sécurité, Authentification, Algorithme de Hachage, MAC, Nœud de Surveillance