AVIS DE SOUTENANCE DE THESE

Le Doyen de la Faculté des Sciences Dhar El Mahraz –Fès – annonce que

Mr **TOUIL Hamza**
Soutiendra : **le Mardi 31/12/2024** à **10H00**
Lieu : ***FSDM – Centre Visioconférence***

Une thèse intitulée :

« Innovative Cybersecurity Approaches and Advanced Strategies for Data Protection and Authentication »

En vue d'obtenir le ***Doctorat***

FD : ***Sciences et Technologies de l'Information et de la Communication***
Spécialité : ***Informatique***

Devant le jury composé comme suit :

Nom et prénom	Etablissement	Grade	Qualité
AZROUL Elhoussine	Faculté des Sciences Dhar El Mahraz, Fès, USMBA	PES	Président
SBAI El Hassan	Ecole Supérieure de Technologie, Meknès, UMI	PES	Rapporteur
AKSASSE Brahim	Faculté des Sciences, Meknès, UMI	PES	Rapporteur
SATORI Hassan	Faculté des Sciences Dhar El Mahraz, Fès, USMBA	PES	Rapporteur
HADDOUCH Khalid	Ecole Nationale des Sciences Appliquées, Fès, USMBA	MCH	Examinateur
LOQMAN Chakir	Faculté des Sciences Dhar El Mahraz, Fès, USMBA	PES	Examinateur
EL AKKAD Nabil	Ecole Nationale des Sciences Appliquées, Fès, USMBA	MCH	Co-directeur
SATORI Khalid	Faculté des Sciences Dhar El Mahraz, Fès, USMBA	PES	Directeur de thèse

Résumé :

La sécurité des données est un enjeu hyper important dans un cyberespace en perpétuelle mutation où les menaces se multiplient et où la protection des informations sensibles devient une priorité absolue. Dans le contexte de cybersécurité, notre étude se concentre sur le développement de solutions cryptographiques avancées, répondant aux besoins actuels tout en anticipant les vulnérabilités futures. Nous avons conçu des méthodes de sécurité personnels basés sur des techniques cryptographiques éprouvés, telles que le cryptage symétrique et asymétrique, garantissant ainsi la confidentialité et l'intégrité des données. Ces solutions améliorent la sécurité des échanges dans des protocoles essentiels comme TLS et SSH, en optimisant ces derniers par l'utilisation de clés AES à longueurs variables, augmentant ainsi leur résistance aux attaques tout en maintenant la compatibilité avec les systèmes existants. Cela permet une transition en douceur vers des systèmes plus sécurisés, sans compromettre les performances opérationnelles. Cependant, l'avènement de l'informatique quantique présente une menace sérieuse pour les méthodes de cryptage traditionnelles, qui risquent de devenir obsolètes face à la puissance de calcul quantique. Pour contrer cette menace, notre recherche propose l'intégration d'algorithmes post-quantiques, capables de sécuriser les connexions et le stockage des données, garantissant ainsi que les systèmes cryptographiques demeurent robustes face aux défis futurs. De plus, dans la gestion des mots de passe et les processus d'authentification, nous avons proposé des méthodes innovantes qui s'appuient sur des techniques issues d'autres domaines afin de complexifier l'analyse des systèmes par des acteurs malveillants, rendant plus difficile la conception de méthodes de piratage. L'une de ces techniques est la transformation Braille, qui consiste à crypter les mots de passe en utilisant un format Braille à six points. Cette approche unique renforce la sécurité en ajoutant une couche supplémentaire de protection difficile à contourner. Par ailleurs, nous avons également introduit la technique H-Rotation, appliquée à l'algorithme SHA-3, qui permet de transformer les phrases de passe en valeurs de hachage complexes. Cette méthode renforce considérablement la résistance aux attaques en rendant la récupération des phrases de passe initiales extrêmement difficile. Nos méthodes ont été testées et évaluées avec des résultats très favorables, notamment en ce qui concerne la sécurité des données mobiles.

Mots clés : Cryptographie moderne, authentification, qualité de service, fonction de Hachage, stockage, reconstruction SHA-3, Quantique.

Abstract :

In an ever-evolving cyberspace, data security has become a paramount concern as threats proliferate and the protection of sensitive information emerges as a critical priority. In the context of cybersecurity, our study focuses on developing advanced cryptographic solutions that address current needs while anticipating future vulnerabilities. We have devised personalized security tools grounded in well-established cryptographic techniques, including both symmetric and asymmetric encryption, thereby ensuring the confidentiality and integrity of data. These solutions enhance the security of communications within key protocols such as TLS and SSH by optimizing the use of variable-length AES keys, significantly bolstering their resistance to attacks while maintaining compatibility with existing systems. This approach facilitates a seamless transition to more secure infrastructures without compromising operational performance. However, the advent of quantum computing poses a substantial threat to traditional cryptographic methods, which are at risk of becoming obsolete in the face of quantum computational power. To mitigate this risk, our research proposes the integration of post-quantum algorithms capable of securing both connections and data storage, ensuring that cryptographic systems remain resilient in the face of emerging technological challenges. Moreover, in the realm of password management and authentication protocols, we have introduced innovative methods that draw upon techniques from other fields to complicate system analysis by malicious actors, thereby making it significantly harder to devise hacking strategies. One such technique is the Braille transformation, wherein passwords are encrypted using a six-point Braille format, adding an extra layer of security that is exceedingly difficult to circumvent. Additionally, we introduced the H-Rotation technique, applied to the SHA-3 algorithm, which converts passphrases into complex hash values, greatly enhancing resistance to attacks by making the recovery of original passphrases exceedingly difficult. We rigorously tested and evaluated our methods, yielding highly favorable results, particularly in the realm of mobile data security.

Key-words: Modern cryptography, authentication, quality of service, hash function, storage, SHA-3 reconstruction, Quantum.