الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس

Ecole Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbes

Mémoire de Fin d'étude

Pour l'obtention du diplôme de **Master**

Filière : **Informatique**

Spécialité : **Systèmes d'Information et Web (SIW)**

Dans le cadre d'un diplôme - une startup

Thème

Exploration de la Blockchain et de l'Architecture Zéro Confiance : Perspectives, Défis et Solutions

Présenté par **:**

- Mlle Dadoua Hadria Kawthar
- Mr Benhocine Ayyoub

Soutenu le : **09/07/2023**

Devant le jury composé de :

- M.Amar Bensaber Djamel	Président
- M.Amrane Abdelkader	Encadreur
- Mme.Badia Klouche	Examinateur
- M.Kechar Mohamed	Représentant de l'incubateur

Année Universitaire : 2022 / 2023

Remerciement

Nous tenons tout d'abord à exprimer notre profonde gratitude à Dieu tout-puissant, qui nous a accordé le courage, la patience et la prévoyance nécessaires pour mener à bien ce projet.

Nous exprimons nos sincères remerciements à notre encadrant du projet de fin d'études, Monsieur AMRANE Abdelkader pour son suivi attentif, ses conseils précieux, son orientation éclairée, ainsi que pour le temps et les efforts qu'il a consacrés à notre réussite.

Nous souhaitons également adresser nos remerciements les plus chaleureux à Monsieur le président ainsi qu'aux membres du jury pour avoir gracieusement accepté d'évaluer notre travail avec bienveuillance et expertise.

Enfin, nous souhaitons également remercier nos chers parents, nos amis et camarades, ainsi que toutes les personnes qui ont contribué de près ou de loin à la concrétisation de ce projet. Leurs encouragements infaillibles, leur précieuse aide et leur motivation tout au long de notre parcours académique.

Résumé

Cette thèse explore la convergence de l'architecture de confiance zéro (Zero Trust Architecture ou ZTA) et des systèmes de détection et de prévention des intrusions basés sur la blockchain, en mettant l'accent sur l'augmentation de la ZTA au niveau des points d'extrémité. L'objectif est d'améliorer la défense contre les mouvements latéraux dans les réseaux sans frontières et de remédier aux vulnérabilités des points d'extrémité compromis au sein de la ZTA. L'article commence par une vue d'ensemble de la ZTA et de la blockchain, en discutant de leurs définitions, des différents types, des caractéristiques et des applications. Il examine ensuite l'évolution des architectures traditionnelles basées sur les périmètres vers la ZTA, en mettant en évidence les principes fondamentaux et les capacités essentielles de la ZTA, ainsi que les différents modèles de ZTA selon le NIST.

Ensuite, l'article examine les défis et les solutions associés à la ZTA, en mettant l'accent sur le besoin de mécanismes de détection des intrusions. Il explore le concept d'utilisation de la technologie de la blockchain pour la détection des intrusions, en tenant compte de son immuabilité et de son potentiel pour renforcer le processus de détection. L'article présente également des travaux connexes sur les systèmes de détection des intrusions basés sur la blockchain et les mécanismes de consensus.

En conclusion, la convergence de la ZTA et de la blockchain offre des possibilités prometteuses pour améliorer la sécurité des réseaux et la détection des activités malveillantes. En augmentant la ZTA au niveau des points d'extrémité et en exploitant l'immutabilité de la blockchain, il devient possible de renforcer le processus de détection des intrusions. Cependant, plusieurs défis subsistent, tels que garantir la scalabilité, la confidentialité et la gouvernance des systèmes basés sur la blockchain. L'article identifie ces défis ouverts et suggère des orientations futures pour la recherche dans ce domaine.

Abstract

This thesis explores the convergence of Zero Trust Architecture (ZTA) and blockchain-based intrusion detection and prevention systems, with a focus on enhancing ZTA at the endpoint level. The goal is to improve defense against lateral movement in borderless networks and address vulnerabilities of compromised endpoints within ZTA. The paper begins with an overview of ZTA and blockchain, discussing their definitions, different types, characteristics, and applications. It then examines the evolution from traditional perimeter-based architectures to ZTA, highlighting the fundamental principles and essential capabilities of ZTA, as well as various ZTA models according to NIST.

Next, the paper explores the challenges and solutions associated with ZTA, emphasizing the need for intrusion detection mechanisms. It explores the concept of using blockchain technology for intrusion detection, considering its immutability and potential to strengthen the detection process. The paper also presents related work on blockchain-based intrusion detection systems and consensus mechanisms.

In conclusion, the convergence of ZTA and blockchain offers promising opportunities to enhance network security and detect malicious activities. By enhancing ZTA at the endpoint level and leveraging the immutability of blockchain, it becomes possible to strengthen the intrusion detection process. However, several challenges remain, such as ensuring scalability, confidentiality, and governance of blockchain-based systems. The paper identifies these open challenges and suggests future directions for research in this field.

تلخيص

تستكشف هذه الأطروحة تقارب الهندسة المعمارية للثقة الصفر (ZTA) وأنظمة اكتشاف ومنع الاختراقات التي تعتمد على التكنولوجيا البلوكشين، مع التركيز على تعزيز الZTA على مستوى نقاط النهاية. الهدف هو تحسين الدفاع ضد الحركات الجانبية في الشبكات الخالية من الحدود ومعالجة ضعف نقاط النهاية المتعرضة للاختراق ضمن الZTA. تبدأ المقالة بنظرة عامة على ZTA والبلوكشين، وتناقش تعريفاتهما وأنواعهما المختلفة وخصائصهما وتطبيقاتهما. ثم تستعرض تطور الهندسة المعمارية التقليدية المستندة إلى الحواجز نحو ZTA، مبرزة المبادئ الأساسية والقدرات الأساسية للZTA، بالإضافة إلى نماذج مختلفة للZTA وفقًا لمعايير NIST.

بعد ذلك، تناقش المقالة التحديات والحلول المرتبطة بالZTA، مع التركيز على حاجة آليات اكتشاف الاختراق. تستكشف المقالة مفهوم استخدام تكنولوجيا البلوكشين لاكتشاف الاختراق، مع مراعاة صفتها غير القابلة للتغيير وإمكانيتها لتعزيز عملية الاكتشاف. تقدم المقالة أيضًا أعمال ذات صلة حول أنظمة اكتشاف الاختراق التي تعتمد على التكنولوجيا البلوكشين وآليات التوافق.

في الختام، توفر تقارب الZTA والبلوكشين فرصًا واعدة لتعزيز أمان الشبكات وكشف الأنشطة الخبيثة. من خلال تعزيز الZTA على مستوى نقاط النهاية واستغلال صفة غير القابلية للتغيير في التكنولوجيا البلوكشين، يصبح من الممكن تعزيز عملية اكتشاف الاختراق. ومع ذلك، تبقى العديد من التحديات، مثل ضمان قابلية التوسع، والسرية، والحوكمة للأنظمة المعتمدة على التكنولوجيا البلوكشين. يحدد المقال هذه التحديات المفتوحة ويقترح توجهات مستقبلية للبحث في هذا المجال.