Evaluating Zero Trust Vulnerabilities in Identity and Access Management:

Strengthening Security Posture in Dynamic Environments.

Kuruparan Sivalingam
MS22904850

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY (CYBERSECURITY)

SLIIT
December 2024

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Dr. Harinda Fernando

Approved for MSc. Research Project:

MSc. Programme Co-ordinator, SLIIT.

Approved for MSc:

Head of Graduate Studies, FoC, SLIIT

DECLARATION

Declaration I declare that this is my own research thesis, and this thesis does not incorporate without acknowledgement any material previously published submitted for a degree or Diploma in Sri Lanka Institute of Information Technology or any other university or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Sign: -

Date: - 18th of October 2024

ABSTRACT

S. Kuruparan
MSc in Information Technology (Cyber Security)
Supervisor: - Dr. Harinda Fernando

In the era of widespread digital transformation, cybersecurity frameworks play a crucial role in protecting essential assets. The Zero Trust model has become prominent, advocating a “always verify, never trust” approach to secure network access and control. This study examines vulnerabilities within Zero Trust-based Identity and Access Management (IAM) systems, focusing on the challenges that arise in dynamic digital environments where technological advancements and shifting user behaviors impact security.

Using a mixed-methods approach, the research combines quantitative survey data from cybersecurity professionals with qualitative insights from case studies and expert interviews. Findings indicate that while Zero Trust models strengthen organizational security posture, they introduce operational complexities. High resource demands, integration difficulties, and the need for continuous monitoring pose challenges for organizations, potentially hindering efficient operations. These hurdles underscore the difficulty of balancing Zero Trust’s security benefits with streamlined processes. Additionally, the study reveals that Zero Trust IAM vulnerabilities become especially evident in fast-paced digital settings, where rapidly changing technology and varied user interactions demand an adaptive security approach.

To address these vulnerabilities, the study proposes a structured Zero Trust implementation framework, comprising seven key stages: preparation and assessment, identity verification and access control, network and device security, continuous monitoring via User Behavior Analytics (UBA), data security protocols, incident response, and compliance integration. Each stage targets specific challenges, aiming to enhance security without compromising operational efficiency. For example, identity verification and access control help ensure strict authentication, while network segmentation and endpoint security protect critical assets. Regular monitoring with UBA aids in detecting insider threats, and data security protocols like encryption and Data Loss Prevention (DLP) safeguard sensitive information.

This research contributes to cybersecurity in several ways. Academically, it advances understanding of the vulnerabilities within Zero Trust IAM systems, particularly in dynamic environments where these weaknesses are accentuated. Methodologically, it presents a replicable framework that integrates quantitative and qualitative approaches, providing a comprehensive lens for future cybersecurity research. Practically, the study offers actionable recommendations for organizations across industries, enabling them to bolster their security postures against emerging threats. These insights are invaluable for policymakers and industry leaders seeking to establish resilient cybersecurity standards and guidelines in a rapidly evolving digital landscape.

Ultimately, this research provides a detailed look at Zero Trust IAM vulnerabilities and emphasizes the need for adaptive security strategies to navigate the challenges of a complex digital environment. By addressing key operational hurdles and proposing targeted solutions, this study makes a significant contribution to advancing cybersecurity practices. Its findings underscore the importance of flexible security measures that enable organizations to protect digital assets effectively, supporting organizational resilience within an interconnected and increasingly volatile digital space.

Keywords: *Zero Trust, Identity and Access Management (IAM), Cybersecurity frameworks, Data security protocols, Incident response, Data Loss Prevention (DLP) Vulnerability assessment, Cyber threat resilience, Organizational security, Digital asset protection.*

ACKNOWLEDGEMENT

Even though the research development is an individually assigned academic achievement, I was well supported by my surrounding professionals and loved ones whom I like to be acknowledged with a grateful heart.

First, I like to thank my supervisor **Dr. Harinda Fernando**. His guidance was highly supportive to achieve my academic expectations.

In addition, I would like to take this opportunity to extend my appreciation to **Dr. Prasanna Sumathipala**, who holds the position of Head of Graduate Studies at the Faculty of Computing and Computer Systems Engineering at the Sri Lanka Institute of Information Technology.

Further, I like to thank all my academic lecturers of my master's program who supported and educated me by effectively addressing my knowledge gaps and further developed me to have much-maligned competencies. I like to thank the non-academic staff of the Sri Lanka Institute of Information Technology for their support in addressing all the administrative activities relating to the course.

Lastly, I like to deliver my thank to my loving family members. Your love, support, and kind encouragement always uplift my personal life, professional life, and academic life.

TABLE OF CONTENTS

List of Figures