Zero Trust Maturity Dual Assessment Model: Incorporating Technical and Organizational Insights

Yu-Chih Wei[1], Tak Wai Yu[2] and Wei-Chen Wu[3]

[1] National Taipei University of Technology, (10608) 1, Sec. 3, Zhong-Xiao (Chung-Hsiao) E. Rd., Da'an Dist., Taipei City 106, Taiwan (R.O.C.)
vickrey@mail.ntut.edu.tw
[2] National Taipei University of Technology, (10608) 1, Sec. 3, Zhong-Xiao (Chung-Hsiao) E. Rd., Da'an Dist., Taipei City 106, Taiwan (R.O.C.)
t111ab8407@ntut.edu.tw
[3] National Taipei University of Business, (10051) No.321, Sec. 1, Jinan Rd., Zhongzheng District, Taipei City 100, Taiwan (R.O.C.)
weichen@ntub.edu.tw

Abstract. The emergence of the term Zero Trust in recent years within the information security discipline has revealed a new trend aimed at trimming down static defense perimeters and central security models. As this thesis explicates, the Dual-Perspective Assessment Model is very helpful in assessing Zero Trust Maturity for organizations, offering technical and functional aspects together. The model develops an assessment tool that measures the current infrastructure and includes a plan for migration to a Zero Trust Architecture (ZTA). Based on a comprehensive literature review, the study uses both qualitative and quantitative techniques to determine key factors influencing ZTA implementation, addressing the need to incorporate technology and a firm's strategic objectives for higher security. Through this model, organizations implementing or reinforcing the Zero Trust tendency, as well as companies occupying the field of cybersecurity management work, have a practical tool for strategy and tendency.

Keywords: Zero Trust, Maturity Model, Network Security

1 Introduction

1.1 Research Goal

The increasing sophistication in the cyber environment requires changes in the development of security threats. Zero Trust as an emerging strategy, which has its origins in the ideas propounded by the Jericho Forum in 2004 and then systematically outlined by John Kindervag in 2009 [1], helps to overcome the weaknesses of traditional perimeter security. Its fundamental concept is rooted that Zero Trust does not inherently trust any user, whether internal or external to the network. This research aims to explore Zero Trust in the following perspective: (1) What are the critical components and tools required for developing maturity models specifically for Zero Trust? (2) In what ways

can a maturity model provide a comprehensive assessment of Zero Trust implementations? (3) How do individual perceptions and knowledge levels about Zero Trust affect the implementation and maturity of its frameworks in organizational settings? These questions provide the focus for the Zero Trust research with the intent on developing the knowledge and utilization of maturity models in cybersecurity.

2 Related Work

2.1 Zero Trust Architecture Components

The Zero Trust Architecture developed by the National Institute of Standards and Technology (NIST) in the document SP 1800-35B [2] provides a comprehensive foundation for the complex structure with essential components communicating with each other to necessarily access control and resource protection. Policy Engine (PE) lies at the heart of the mechanism decides who to trust by evaluating trust scores and applying enterprise policy; Policy Administrator (PA) is the prominent unit that carries out these commandments and orders the PEP to deal with communication channels and session-specific keys. The PEP, which is the trust zone security, guards over initializing, monitoring, and disconnecting bridges to enterprise systems. The joint PE and PA feature the Policy Decision Point (PDP). The PDP makes the decisions of who can access the information; PIPs play the role of equipment and paperwork that ensure that the information being relayed is accurate at the command point department.

Research has been conducted on the integration of zero trust security and multi-factor authentication (MFA) [3] where the designed systems are adaptable to complex computing environments. Identity security is established as an essential element [4] of the Zero Trust framework, the implementation of rigorous authentication methods; research on designing a new ZT access control scheme [5] introduces a multifaceted approach that utilize exclusive tools for dynamic access control. The design demonstrates the key role of PDP in evaluating security level and deciding final access confirmation based on a real-time assessment of risks; a recent case study for the complete zero trust implementation in the Indonesian financial sector alongside Kubernetes done by Surantha [6]. It points out firewall routines within the Kubernetes full-stack implementation boundaries, soliciting the complete inspections of all network traffic.

2.2 Organization Insight

Literature review extends to the non-technical aspects of Zero Trust, such as the organizational culture and process that support its implementation. The study focusing on the fundamental understanding of Zero Trust among digital employees [7] examines into how personal experiences and awareness shape an employee's trust in technology. The research suggests that employees with a better grasp of technology are likely to be more vigilant and verify the technology they use, rather than blindly trusting it. Complementing this view, research on improving security policies in distance learning systems [8] emphasizes the responsibility of participants in ensuring information security. It aligns

with the Zero Trust concept by advocating for detailed response policies to incidents, thus integrating Zero Trust principles into the framework of educational systems.

2.3 Zero Trust Maturity Models

The Zero Trust Maturity Model developed by the Cybersecurity and Infrastructure Security Agency (CISA), is tailor-made for federal agencies but is also applicable to other organizations. It categorizes maturity into five areas: Identity, Devices, Networks, Applications and Workloads, and Data, emphasizing cross-cutting capabilities such as Visibility and Analytics, Automation and Orchestration, and Governance[9]. A few theses are found to be focusing on Zero Trust Maturity Assessment. Michel [10] introduces ZeTuMM which advocates for a paradigm shift towards Zero Trust, guiding enterprises in initiating and advancing their Zero Trust maturity. The model emphasizes stringent verification and security within IT infrastructures, reflecting the evolution of cybersecurity through various waves. The research conducted by Jansen and Tokerud [11] extends the research scope a step further, addressing both technological and organizational aspects of cybersecurity, the EZTMM proposed moves beyond network-centric applications to a holistic approach. Developed through design science research, it incorporates literature reviews, expert consultations, and case studies, offering a tool for assessing Zero Trust capabilities.

3 Research Methodology

3.1 Survey Design

A questionnaire is designed to explore the influence of Zero Trust on organizational maturity, targeting IT staff and cyber-security officers to gather diverse perspectives on Zero Trust's application and impact. It assesses the integration of Zero Trust principles both technically and organizationally, aiming to gauge participants' knowledge and attitudes, providing data to validate the maturity model and inform the effectiveness of current methodologies. This survey evaluates organizational maturity and user perspective on project progression, including demographic queries and knowledge assessment of Zero Trust through quizzes and a Likert scale based Zero Trust Attitude assessment. It also examines the importance of different components in assessing Zero Trust maturity, using a holistic approach that blends subjectivity and objectivity.

3.2 Conceptual Maturity Model Development

The design approach for the Dual Dimensions Zero Trust Maturity Model (DuZTMM) is based on the methodology developed by de Bruin et al. [12]. The method utilizes and optimizes proven approaches, designing an organized process for the assessment of ZTA implementation. The DuZTMM model integrates technology and organizational aspects, which represent the integral components of the scheme and progress of the enterprises towards achieving maximum Zero Trust maturity level. The DuZTMM framework is a mapping of maturity stages that starts with the realization that a Zero

Trust architecture is required, then develops an adaptive and resilient stance that leads to the continual enhancement of cybersecurity protection. It highlights the value of basing decisions on the adoption of state-of-the-art technologies in the areas of real-time threat analysis and instantaneous decision-making, as well as the development of an organization-wide culture of security awareness and preparedness.

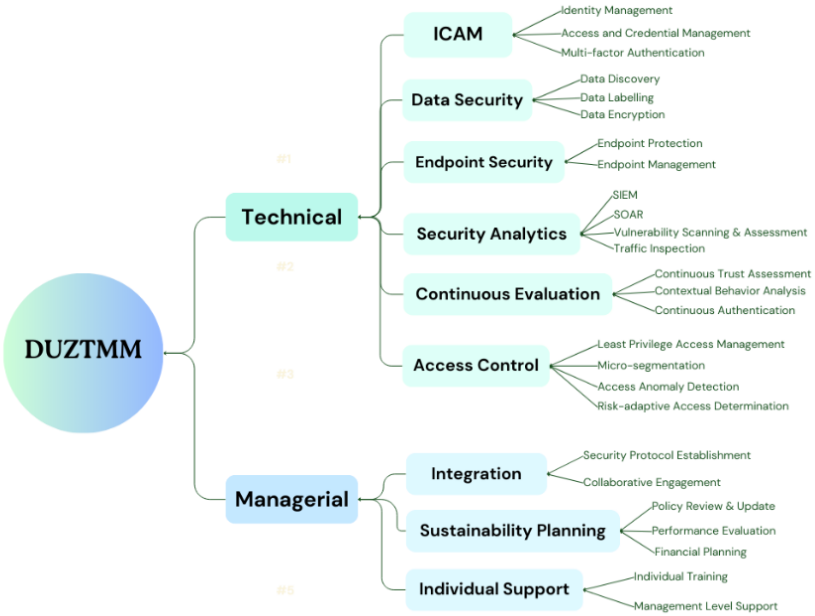

Figure 3.1 DuZTMM Structure Overview

4 Survey Analysis and Result

4.1 Demographic Data and Descriptive Analysis

A total of 36 surveys were returned from participants whose expertise ranges in different areas including financial and insurance, software service, hardware, academic, and government departments. Participants' roles are evenly distributed between management and technician positions.

In section C, a Zero Trust knowledge quiz involving True/False and multiple-choice questions was designed to examine participants' knowledge level of Zero Trust's main concepts; an average score of 8.4/10 was returned, and an SD of 1.5 showed a moderate level of variability among the dataset, suggesting participants could be noticeably more or less familiar with Zero Trust. Overall, respondents possess sufficient knowledge on the research topic to make them suitable candidates for the survey.

Participants' attitudes towards Zero Trust are investigated as well, where a 5-point Likert scale is used to rate an individual's opinion on Zero Trust-related questions. Examples of questions from Section D to E are provided in Table 3.1. For attitude examination, participants reported mean scores of 3.38 or higher for all questions, except for one question asking if participants feel that Zero Trust implementation is an over-complicated process, for which a mean score of 2.63 was returned. The results indicate that participants overall feel positive about Zero Trust as an effective and essential security posture, although they consider that the components and concepts included in Zero Trust could be seen as complicated and might be reasons why organizations hold back on implementing related processes.

In Sections E, participants were asked about their personal views on Zero Trust and the importance of involving different components in assessing Zero Trust maturity within a team or organization. Participants reported a mean score of 4.2/5 for questions relevant to both technical and managerial components, echoing the components considered in the Zero Trust maturity assessment framework

Table 3.1 Survey Sample Questions

Section	Sample Question	Option(s)
C. Zero Trust Knowledge Quiz	"Zero Trust assumes everything inside the internal network is trustable." "What are the" 5 pillars of Zero Trust Model by CISA?	True or False/ Multiple-Choice
D. Attitude Towards Zero Trust	"I believe that the Zero Trust approach is essential for modern cyber-security." "The benefits of Zero Trust outweigh the complexities of its implementation."	1- Strongly Disagree 2 - Disagree 3 - Neutral 4 - Agree 5 - Strongly Agree
E. Maturity Assessment Components Opinion Examination	"A mature Zero Trust implementation should involve the implementation of security analytics practices in a Zero Trust environment, including SIEM, SOAR, and network traffic monitoring." "Success in implementing Zero Trust strategies should take both technical and managerial levels into consideration."	

4.2 Correlation Analysis

Pearson Correlation Analysis was performed to examine if there is any relationship between an individual's attitude and knowledge level on Zero Trust. The value from the Pearson correlation analysis of 0.249 shows there is a weak but positive correlation between the respondents' average attitude towards implementing the Zero Trust concept and their knowledge scores. They were not presented with this p-value correlation in the provided data. Though the association seems to be slightly shifting toward the null, this confirms that the hypothesis is that the higher the degree of knowledge of Zero Trust, the better attitude people tend to develop towards it.

The result leads to the insight that management may contemplate enhancing the training programs further on the topic, and this can sufficiently be the answer as it raises awareness among the employees, thus proactively supporting them to engage with practices linked to the concept.

5 Discussion

By starting with the summary of the analysis in this thesis, the following limitations have been identified, which influence the interpretation and outcomes of the results.

Moreover, the lack of sample diversity leads to the limited applicability of the data's results. This imposed limitation, in this way, sets the tone for questioning how far the findings can be generalized across different organizational settings.

Going on, this research issue should be tackled by taking observations from a multitude of surveys to include different types of people, ensuring the verification and portability of the novel's findings. In addition, it is important to utilize a wider variety of data-gathering methods to include more influencing measures and thus reduce the observed variability problems. This method would aim at exploring further all the dynamics behind this phenomenon, figuring out the interactions between the technical and organizational aspects. This comprehensive understanding of the relationship between technical components and the level of organizational maturity would enrich our knowledge.

References

1. Aiello, S., *Zero Trust: A Governance Perspective.* 2022.
2. *Implementing a Zero Trust Architecture Third Preliminary Draft*. 2023, NIST Special Publication 1800-35B.
3. Varun Varma Sangaraju, K.H., *Zero Trust Security and Multifactor Authentication in Fog Computing Environment*. 2023, University of the Cumberlands.
4. Poller, J., *Identity: The Glue that Ties Zero Trust Together*. 2022, Enterprise Strategy Group.
5. García-Teodoro, P., et al., *A novel zero-trust network access control scheme based on the security profile of devices and users.* Computer Networks, 2022. **212**.
6. Surantha, N., F. Ivan, and R. Chandra, *A case analysis for Kubernetes network security of financial service industry in Indonesia using zero trust model.* Bulletin of Electrical Engineering and Informatics, 2023. **12**(5): p. 3142-3152.
7. Samah, I.H.A., et al., *Fundamental of zero trust among digital employees in migration to industry 4.0: Cyber security and movement to iot in Malaysian perspectives*, in *Advances in Fracture and Damage Mechanics Xx*. 2023.
8. Pavlo Skladannyi, O.T., Viktor Korniiets, Maksym Vorokhob, and Tetiana Opryshko. *Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept*. in *CEUR Workshop Proceedings*. 2023.
9. *Zero Trust Maturity Model Version 2.0*, C.a.I.S. Agency, Editor. 2023.
10. Modderkolk, M., *Zero Trust Maturity Matters*, in *Department of Information and Computer Science*. 2018, Utrecht University: Netherlands.
11. Jarand Nikolai, J., Simen, Tokerud, *Designing the Extended Zero Trust Maturity Model*, in *Department of Information Systems*. 2022, University of Agder.
12. Tonia de Bruin, R.D.F., Uday Kulkarni, Michael Rosemann, *Understanding the Main Phases of Developing a Maturity Assessment Model*, in *16th Australasian Conference on Information Systems* 2005: Sydney.