International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 02, February 2026)

Empowering Cybersecurity Learning Through Zero Trust

Prof. Rahul C. Pawar[1], Prof. Rutuja P. Kadgi[2], Prof. Amol M. Gaikwad[3], Prof. Ankita B. Suryavanshi[4], Prof. Ashwini S. Yadav[5]

Lecturer, Department: - [1,2]Electronics and Telecommunication Engineering, [3,4,5]Computer Engineering, College Name: KJEI' s Trinity Polytechnic Pune (TPP), India

***Abstract--* Zero Trust (ZT) is used by cybersecurity teams as a conceptual and architectural framework to design networks into secure micro-perimeters and to strengthen data security with dynamic and context-aware policies through the systematic integration of state-of-the-art technology, risk management, and threat intelligence. It has been shown by both theoretical analysis and industrial practice that ZT can ensure that organizations avoid becoming victims of known attacks or of failing to discover a breach for a prolonged period of time. Recently, momentum has been gained in the industry by ZT as it helps to defend against the lateral movement of malicious actors within today's borderless networks. Security best practices are required to be adopted by the federal government through the United States 2021 President Executive Order, advancing toward a Zero Trust Architecture (ZTA). However, it has been proved that implementing a ZTA is a complex and non-trivial task due to its novelty. An understanding of what ZT or ZTA is needed to be developed in order to take full advantage of its benefits. Therefore, the fundamental concepts, principles, and architectures of ZT need to be introduced in cybersecurity courses at colleges to better prepare our new cybersecurity professionals for successful careers.**

In the last few years, a module has been actively developed by us and has been effectively used to introduce ZT in cybersecurity courses at senior undergraduate and graduate levels. This module consists of a comprehensive lecture to introduce ZT, a thoughtful homework assignment, and well-structured test questions. The lecture encompasses an insightful introduction to ZT and its principles, design issues in the traditional model of perimeter-based network security are addressed, zero trust architectures are explored, the security benefits of ZT are outlined, the technical challenges to implement a ZTA are discussed, and the main threats to ZT networks are identified. A thorough overview of this module is delivered in this article, with emphasis placed on the contents of the lecture. Valuable experiences and lessons learned in our teaching practice will also be shared by us. A useful reference for those who teach cybersecurity courses at a college or university or who are diligently developing a cybersecurity curriculum will be provided by our collaborative work. Assistance will also be offered to busy professors in developing or revising a zero-trust module for their cybersecurity courses.

I. Introduction

Zero Trust (ZT) has recently been gained prominence as a new standard in cybersecurity management due to its dynamic and context-aware approach to effectively address the issues that remarkable changes in the cybersecurity landscape have brought. Nowadays, a typical infrastructure of information technology (IT) for an enterprise is comprised of multiple internal networks, branch offices, and subcontractors with their local networks, remote and mobile employees working under the policy of "bring your own device," cloud computing services, and Internet-of-Things (IoT) devices. This IT landscape has significantly challenged the ability of traditional perimeter-based network security models, as the increasing number of data breaches and successful hacking attacks is indicated. The perimeter-based security architecture is relied upon for the separation between internal and external networks along with traditional static and implicit network-based measures. Default trust is received by all users, devices, and services on the internal networks, while untrustworthy status is maintained by those from the external networks. However, this model fails to work in the current cybersecurity landscape because such a perimeter on the IT infrastructure of an enterprise is not existed, as is explained later in Section III, due to the pervasive use of cloud computing services, IoT devices, remote workers, subcontractors, and similar factors.

However, a straightforward path for organizations is not presented by the adoption of ZT due to its novelty and the challenges posed by it for IT professionals and the organization itself. Although commitment to ZT is shown by industry leaders, success in replacing the existing solutions is struggled for by most organizations. It is imperative that this cybersecurity strategy is thoroughly understood by decision-makers before a ZT is implemented by them or the existing solution is replaced with it. A recent survey by the Cloud Security Alliance (CSA) has been found to show that two of the top business barriers to adopting the ZT strategy in organizations are represented by the lack of knowledge and expertise (38% out of 824 responses) and the need for additional staffing (33% out of 824 responses).

Therefore, the concepts and principles of ZT, along with its architectures, benefits, and challenges, need to be introduced by educators in college cybersecurity courses to better prepare our new cybersecurity professionals for their careers. This necessity is especially evident in graduate-level cybersecurity courses. However, it is found by busy educators that implementing this change is not a trivial task due to the limited availability of vendor-agnostic and scientifically critical literature. Although findings on the technical aspects and research gaps of ZT as well as ZTA have been published by a few surveys, little work on ZT security from the perspective of cybersecurity education has been reported by researchers.

The concept of zero trust was created by John Kindervag. This innovative framework for cybersecurity management is founded on the philosophy of "never trust, always verify." Organizations are helped by it to prevent security breaches by having implicit trust replaced with explicitly evaluated, real-time adaptive trust levels, along with just enough access to enterprise computing resources and data being provided. As a cybersecurity management strategy, widespread adoption has recently been gained by ZT across various industries. Federal agencies have been ordered by the federal government of the United States to adopt zero trust in their cybersecurity management to enhance the nation's security. Recently, several frameworks have been emerged to implement the principles of zero trust. Notable examples are included, such as Google's Beyond, the Agate zero trust access, Palo Alto's zero trust network access, and VMware secure access. A comprehensive evaluation of 15 ZT products was recently conducted by Forrester Research. Robust functionalities have been developed by most of the evaluated frameworks. More recently, a comprehensive framework has been proposed by experts to assist industries in migrating to ZT. Accordingly, a Zero Trust Architecture (ZTA) has been proposed by the National Institute of Standards and Technology (NIST) of the United States to guide the federal government in advancing toward ZT in its cybersecurity infrastructure.

In the last few years, we have developed a comprehensive module to introduce zero trust in cybersecurity courses at senior undergraduate and graduate levels. This module contains three essential elements:

1. A lecture that presents the principles, architectures, and challenges of zero trust.
2. An open-end homework assignment that encourages students to develop an in-depth understanding of zero trust through self-study. The essay emerges as a collaborative teamwork effort.
3. Test questions, which include multiple choice questions and short answer questions, that help evaluate the students' learning outcomes.

In this paper, the introduction of the development of this lecture is emphasized. The following components are presented:

1. The basic concepts of ZT and the principles that guide the implementation of a ZTA are explained. The questions of what ZT is and what its principles entail are answered in this section. A brief historical evolution and the current state of ZT, alongside recent survey data, are also introduced.
2. Security issues related to the design of a traditional perimeter-based security model are explored. The problems associated with perimeter-based network security are examined to answer the question, "why do we need zero trust?"
3. Zero trust architectures are addressed. An understanding of how the design issues in the traditional network security model can be tackled is gained through the introduction of several approaches. Zero trust architectures are developed by proposed experts with an emphasis on the NIST zero trust architecture.
4. The main security benefits from the ZT strategy are summarized. Several other benefits of ZT from the literature are highlighted, in addition to addressing the existing issues in the design of a perimeter-based network security model.
5. Technical challenges to migrate to a ZTA are identified by experts. Technical and non-technical challenges are recognized, with an emphasis placed on the technical challenges that arise in ZTA implementation.
6. Potential cyber threats to a ZTA are discussed. As a new cybersecurity framework, it is acknowledged that ZT cannot address every security issue and may introduce new problems that need to be considered by organizations when a ZTA is adopted. Potential vulnerabilities of the ZTA that require addressing will be discussed in this component.

The rest of this paper is organized as follows: After the basic concepts and principles, along with a brief historical evolution of ZT, are introduced in the next section, the design limitations present in the traditional perimeter-based model of network security will be discussed in Section III. In Section IV, zero trust architecture is introduced.

Following that, the security benefits of implementing a ZTA in Section V are discussed to explain how these issues can be effectively mitigated or removed through the implementation of a ZTA. Additionally, the technical challenges of practicing ZT in an organization and the potential threats to a ZTA will be addressed in this section. Finally, our work is concluded, and the experiences and lessons that have been gained from the teaching practice are shared. Additionally, learning activities and future work will be described in this section.

II. Zero Trust And Its Principles

In the last one and a half decades, it has been observed by experts that zero trust has evolved from a term, which simply conveys the idea that nothing can be trusted without appropriate verification on the network, to a well-developed strategy for cybersecurity management with a complete set of principles to practice ZT. This short history and the current understanding of zero trust are worth being introduced.

A. Zero Trust and Its Evolution

Zero trust was created by John Kindervag in 2010 to recommend that trust should not be extended by organizations to anything inside or outside of their network perimeters. Various discussions and implementations have been engaged in by experts in the industry and academia since then. However, the concept of ZT was formalized and extended by the National Institute of Standard and Technology (NIST) in 2020 in the NIST Special Publication 800-207. A timeline of zero trust evolution is provided by Zscaler. Although there is no single agreed-upon definition yet, ZT is widely recognized by industry professionals as a security model or a framework with a collection of concepts and principles devised to minimize uncertainty in enforcing least privilege access decisions in information systems, services, and workloads in the face of a network viewed as compromised. This framework requires that all users, devices, services, and workloads, whether inside or outside the organization's network, have their security policy and posture authenticated, authorized, and dynamically validated before access to applications and data is secured or maintained. The principle of least privilege is aimed to be more effectively enforced.

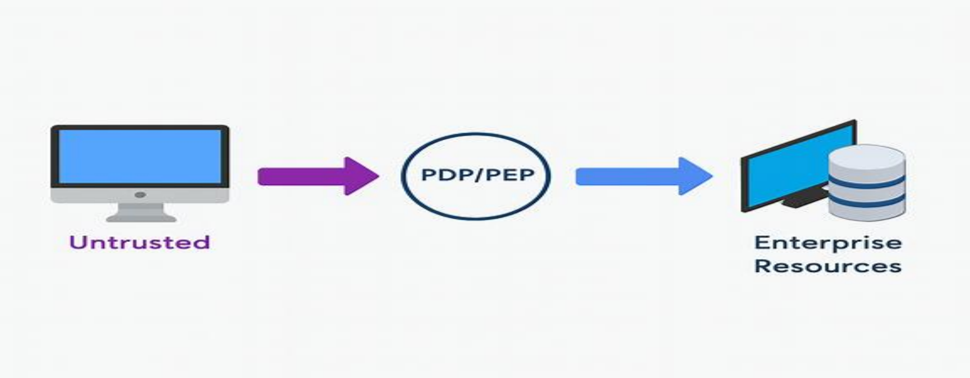

Fig. 1 ZT serves as an access control method in a diagram.

B. Zero Trust Principles

ZT security strategy consists of guiding principles for workflow, system design, and operation that improve a system's security posture. These principles are summarized by NIST as seven tenets shown in Figure 2. More recently, a similar list of principles has been provided by Forrester Research.

These ZT principles are summarized by us below, as shown in Figure 2.

- The principle of least privilege must be implemented by you. Having authentication and authorization for one resource will not automatically allow access to a different resource.
- The integrity and security posture of all owned and associated assets are continuously monitored and diagnosed by the organization, using all collected data to implement contextual access control.

- Access to resources is determined by the system based on the context at the time the user requests access. The context is evaluated by analysts by examining the observable state of client identity, service, requested resource, and other behavioral and environmental attributes. Examples of these attributes include the network status and the result of malware detection.
- All network communication must be secured by all organizations, regardless of the network location. No difference is experienced by users between the communication that occurs on either enterprise-owned networks or external networks.
- All network communication must be secured regardless of location; enterprise-owned and external networks are treated the same.
- All data sources and computing services, such as data on its internal networks and in clouds, are included in an organization's resources. Computing services may also be resided on its internal networks or come from cloud computing providers.
- Authentication and authorization to access a resource are dynamically and strictly enforced by the system before access is allowed**.**

The guidelines for implementing the approach are not specified to include any particular method. For example, the use of multi-factor authentication is recommended by experts. However, it is noted by them that it is not required for every situation. Different authentication methods can be selected by organizations to effectively meet their specific needs..

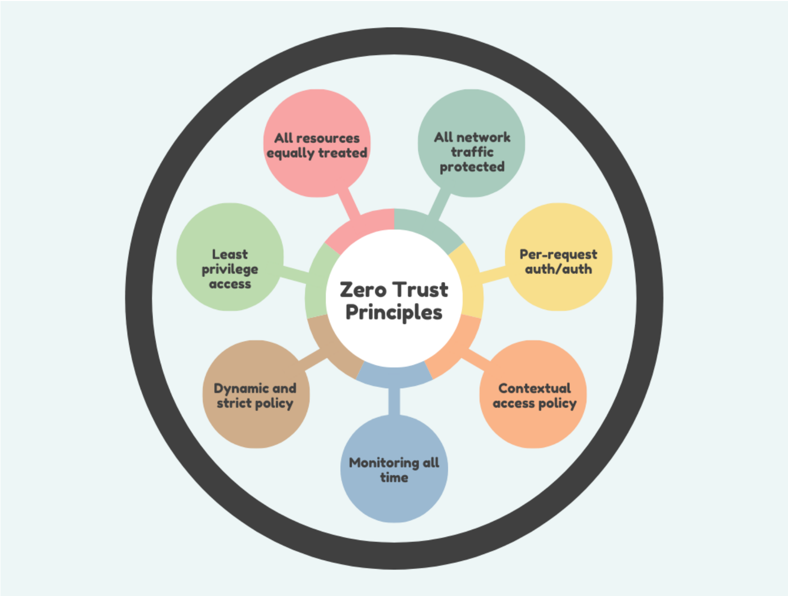

Fig 2. Tenets of zero trust derive from NIST

III. Design Problems In The Traditional Perimeter-Based Network Security Model

It is helpful to have the main problems of the traditional perimeter-based security approach in a modern enterprise environment examined in order to understand the issues that the ZT framework aims to resolve before delving into it. A simplified conceptual diagram of a traditional perimeter-based network security model is illustrated by Figure 3, which is typically implemented by enterprises on their infrastructures. Their own internal networks are maintained by organizations, which connect servers, workstations, laptop computers, and various other devices.

A firewall is utilized by these networked devices to establish protection at the “edge” between internal and external networks. The devices and network traffic that operate on the internal network are implicitly trusted by organizations. Typically, remote or home workers, as well as subcontractors, are allowed by organizations to use their own devices to gain access to the internal network. Their own servers or networks can be operated by subcontractors. A crucial role is played by commercial cloud computing providers in this environment.

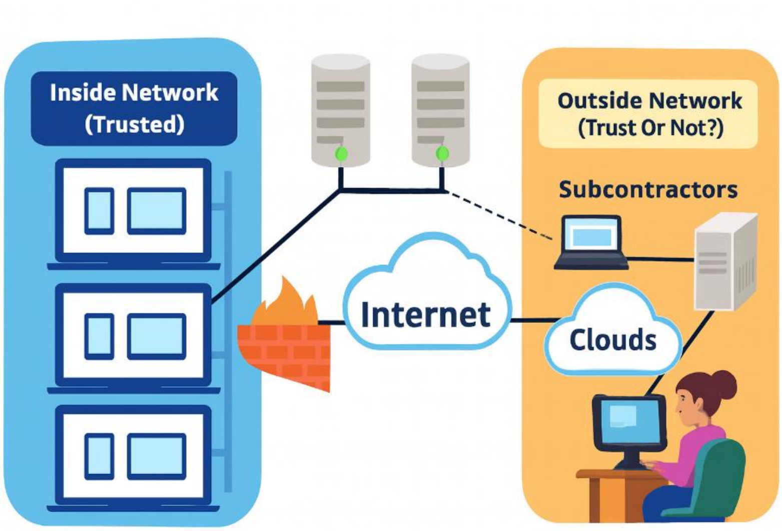

Fig 3. A perimeter-based security model diagram.

A company was contracted by them to provide certain services such as processing and storing sensitive data. The clouds can be accessed by remote workers and subcontractors. The internal network can also be accessed by them through a VPN server, where strong authentication methods can be enforced. It should be noted that a simplified diagram for the purpose of demonstration is represented by Figure 3. In reality, complications can be introduced to the network significantly by a demilitarized zone (DMZ) and other devices, such as IoT devices and edge computing platforms. This design was deemed appropriate when cloud computing had not yet been widely adopted. However, the main problem with the above network configuration is identified as the lack of a boundary that separates the internal network from external networks. Although the internal network can be accessed by remote workers and subcontractors through a VPN proxy server, access to the internal network is also needed by applications running in the clouds that provide services to the organization. Public cloud computing providers are considered to remain external to the organization. Furthermore, three basic threat vectors are identified to exist in the network settings shown in Figure 3.

- A device may be compromised by an attacker through the installation of a malware program originating from a successful phishing email that was sent to the internal network, the subcontractor's network, or a remote worker. Attacks can then be actively launched by that compromised device on other devices connected to the internal network.
- A user's credentials may have been compromised by a malicious actor and used in an attack to gain access to the inside network or the subcontractor's networks. This technique was employed by attackers during the Operation Aurora attacks, which ultimately resulted in Google being prompted to launch they're Beyond Corp project a decade ago.
- A software system – such as an application programming interface (API) or a specific application – can be made to fall prey to compromise, which can lead to negative impacts or even infections of data on the internal network, the subcontractor's network, or the computers that are used by remote workers.

If we think about the number of devices that are present on the networks, including those from remote workers, alongside the total number of users and the variety of vendors, the exponential increase in risk to the organization and its partners can be clearly seen. The above three threat vectors are generally recognized by experts as "lateral movement", which means that adversaries who manage to successfully compromise a user's device can then proceed to compromise other devices on the same network due to the nature of implicit trust that is inherent within those systems.

IV. Zero Trust Architectures

While the term zero trust is commonly recognized by experts as a cybersecurity framework that provides a collection of concepts and principles designed to minimize uncertainty by enforcing more accurate least privilege on a basis of per-request access; zero trust architecture is widely referred to by cybersecurity professionals as a solution to address the cybersecurity needs of an organization. Depending on the specific needs of an organization, different zero trust architectures can be designed. In general, ZT concepts are utilized by a ZTA, ZT principles are followed, and the relationships of components, workflow planning, as well as access policies that need to be integrated and strategically implemented by security teams in order to better secure the assets of an enterprise are encompassed. Several surveys on ZTA have been published by researchers. In this section, the NIST ZTA and Forrester Research Zero Trust extended (ZTX) ecosystem are introduced.

The architecture of the zero-trust network is served as the foundation for the NIST ZTA, where the network is divided into two distinct planes: the data plane and the control plane by designers. As depicted in Figure 4, two main components are included by this framework. In the data plane, a Policy Enforcement Point (PEP) can be found. Meanwhile, in the control plane, a Policy Decision Point (PDP) is located.

- The PEP is served as a communication portal that connects two parties: an untrusted subject and enterprise assets. When a resource like a data item or a computing server within the trusted domain is wished to be accessed by an entity, such as a user, a computer, or a process acting on behalf of a user in the untrusted zone, a request must first be submitted by the subject to the PEP, which then has this request forwarded to the PDP along with the subject's credentials. When a decision is made by the PDP, responsibility is taken by the PEP for dynamically enabling, monitoring, and ultimately terminating connections that exist between the subject and the enterprise asset.

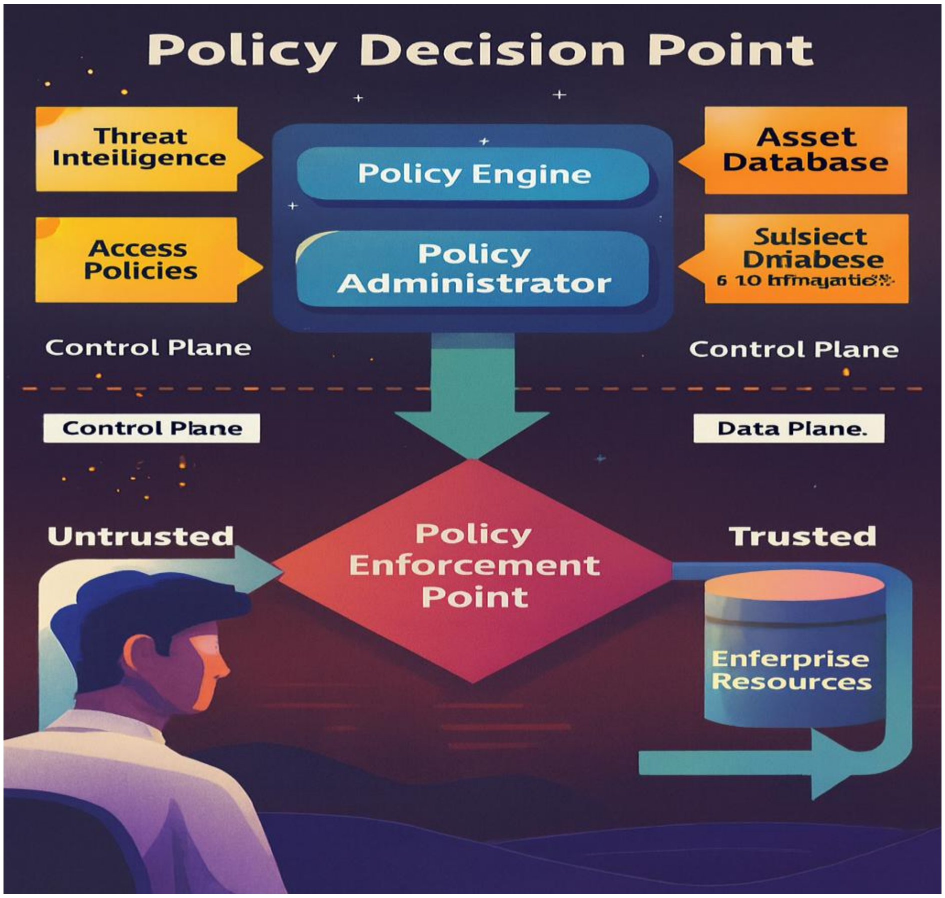

Fig 4. NIST implements Zero Trust Architecture.

- The PDP includes both a Policy Engine (PE) and a Policy Administrator (PA). ZT algorithms are run by the PE to determine whether access to the asset that the subject is seeking should be granted, denied, or restricted. Inputs to this engine are comprised of enterprise policies, monitoring data, and external sources. These input data are actively collected and maintained by integrated subsystems. Examples of such subsystems include an ID management system, a continuous diagnostics and mitigation system, a Security Information and Event Management System (SIEM), as well as industry compliance checks, threat intelligence, and activity logs. The decisions made by the PE are coordinated by the PA, and the responsibility for establishing or shutting down the communication path between the subject and the enterprise asset is held by the PA when appropriate commands are sent to the PEP within the data pane.

In this NIST architecture, the PEP is effectively functioning as an access login portal, as illustrated in Figure 1. The dynamic, context-aware, and real-time policy features are implemented by the ZT team at the policy decision point that operates at the back end. PEP is separated from PDP by designers to ensure a minimum exposure of the system. Here is an example provided to demonstrate how the NIST solution operates. When a data item in the trusted domain is sought to be accessed by a user in the untrusted domain, a request must be submitted to PEP first by the user, which then forwards this request to PDP along with the user's credentials (user ID and login information). At the PE stage, multiple checks are performed by the system before a decision is made. The authentication of the identity is verified by the first check. The level of authentication may vary depending on the specific environment. The next step is for the system to determine whether the necessary requirements to gain access are met by the user's security posture. This is evaluated by the PE using risk-based policies, which can be adjusted at any time to reflect the latest situation. Once a decision is reached, the result is conveyed to PA by PE, which then either establishes or terminates the communication path between this user and the requested data through appropriate commands to the PEP. If access is permitted, a session-specific authentication token is generated by the PEP that will be utilized by the user to access the requested data. When access to the requested data has been gained by a user, the user's activities are continuously monitored and evaluated by the system. Based on the monitoring outcomes and the security posture of this user, either the access is continued or terminated by the system.

V. Discussion On Zero Trust

The various benefits of ZTA will be actively discussed by us in terms of enhancing information security protection, exploring the technical challenges that an organization faces when adopting and implementing a ZTA, and examining the potential cyber threats associated with implementing a ZTA.

A. Security Benefits from Zero Trust Architecture

When the security benefits of ZTA are compared with those of a traditional perimeter-based security architecture outlined in Section III, the security benefits of ZTA can be summarized as follows:

1. *Quicker detection of compromised devices and data breaches:* On a traditional perimeter-based network, a data breach can take weeks or months to be detected by security teams. Network visibility is regarded as one of the main factors that prolong such data breaches. With ZTA, the environment is actively monitored by systems, and continuous analysis of the system status occurs with SIEM, continuous diagnostics and mitigation subsystems, along with system and security logging systems and a threat intelligence system (see in Section IV for details). This ability to inspect all network traffic and packets through the application layer actively provides security operation teams with enhanced visibility. Experimental results have shown that the more visibility regarding the network across the business ecosystem is possessed by security teams, the better chance there is to quickly detect the tell-tale signs of a breach in progress and effectively stop it.
2. *Effective mitigation of lateral movement:* In a fully-featured implementation of ZTA, a strong challenge is faced by adversaries or malware programs in spreading through a network that starts from a compromised endpoint device. This effectiveness is derived from the comprehensive, end-to-end protection that is provided by ZTA. Any access request, regardless of its initiation point, requires authentication of the subject identity through an identity management system. Subsequently, the posture of the subject, along with the device or application from which the request is submitted, is evaluated by the system, and it is assessed against a threat intelligence subsystem. Authorization is led by authentication based on dynamic and contextual policies that can be changed at any moment, guided by real-time data and the results of risk analysis.

This approach is expected to significantly reduce the potential damage that can be inflicted on an enterprise network by any single compromised device, irrespective of how that device becomes compromised (e.g., through compromised user credentials, malware installation, or a vulnerable API; further details can be found in Section III). Effective mitigation of lateral movement in a cloud computing environment that implements ZTA is demonstrated by the preliminary experimental results provided by DeCusatis et al. The effectiveness of mitigating lateral movement on internal networks has also been noted by the industry.

3. *Removal of physical perimeter:* As shown in Figures 1 and 4, a perimeter is effectively removed from a ZTA. All access requests are authenticated and authorized by the system based on the identity of a subject at the PDP, and these requests are enforced by PEP. This process allows an enterprise's security architecture to be actively adapted in order to support new user populations, including remote employees, partners, customers, rapid cloud adoption, and new IoT devices and sensors.

In conclusion, the security issues that arise in a traditional perimeter-based security model will be effectively mitigated by the implementation and operation of a fully-featured ZTA at an enterprise.

B. Technical Challenges to Practice Zero Trust

While problems in traditional perimeter-based networks are promised to be resolved by ZTA, challenges for the implementation and operation of a ZTA are presented by it. In this subsection, the technical challenges that arise are summarized by us.

1. *Lack of standardization:* Due to its novelty and complexity, an evolving stage remains for ZTA. It is believed by experts that standardization is unlikely to be achieved in any way in a short time. Various ways are actively designed and developed for products by different vendors. Recent evaluation results provided by Forrester Research show that the main requirements of ZTA are met by most products from different vendors. However, these products are created by designers for specific purposes. When any of them is selected by a user, a lock into it typically has to be made by the user because of interoperability issues. If changes are made to the infrastructure, challenges to switch to another ZT product without incurring extra costs and time can be presented by it.
2. *Effective integration of various systems is essential:* As explained in Subsection IV, effective integration and proper management must be ensured for many components and systems—including the CDM system, threat intelligence, security and system logging, and SIEM—to facilitate the authentication and authorization decisions made by the PDP. Even deploying and operating such systems individually is not straightforward for administrators. Significant challenges that need to be addressed by organizations are presented by achieving effective integration of these systems.
3. *A huge number of complicated policies exist:* To mitigate the lateral movement of adversaries, micro-segmentation and fine-grained security controls are enforced by ZTA. During the operation of a ZTA infrastructure, a huge number of policies must be specified, implemented, deployed, and managed by organizations. These policies will be attribute-based, meaning they are relied upon by protected resources, subjects, and contexts. While new semantics for security policy specification and testing can be created by developers, challenges that are not trivial are involved in the specification, development, and management of these policies. In addition, when some attributes cannot be trusted, some risk-based criteria for control-related decisions must be applied by organizations. Such criteria are often proved difficult to formalize and automate because they are dependent on specific applications. Together, these factors complicate and render policy management error-prone.

C. Potential Cyber Threats Associated with Zero Trust Architecture

A list of potential cyber threats associated with ZTA is presented by NIST in their SP 800-207. Below, they are summarized:

1. *Denial-of-service attack:* As shown in Figure 4, connections between enterprise resources cannot be established without the permission of PE and the configured action at PA. If access to the PEP or PDP (PE/PA) is disrupted or denied by an adversary using denial-of-service attacks or route hijacking, the operation of the entire enterprise infrastructure can be adversely impacted by such actions.
2. *Stolen credential and insider threat:* While the lateral movement of adversaries can be effectively mitigated by ZTA, a compromised endpoint's already authenticated and authorized session (due to stolen credentials or an insider) can be leveraged in order to carry out malicious activities.

3. *Use of non-person entities in ZTA administration:* Identity-based authentication is employed in a zero-trust architecture. This includes both human users and devices. It remains an open question how authentication is conducted by these non-human entities, including devices, applications, and workloads, in an enterprise that implements a zero-trust architecture.
4. *Subversion of ZTA decision process:* As presented in Section IV, the key components of the entire enterprise in a ZT environment are served by the policy engine and policy administrator. The single points of failure in the NIST ZTA are acted upon by PEP and PDP. No communication between enterprise resources and subjects will occur unless approval and configuration are undertaken at PE and PA. This implies that PE and PA must be properly configured and maintained by administrators. Unapproved changes or mistakes that can disrupt enterprise operations may be made by any enterprise administrator with the privilege to configure and maintain the rules in PE and PA. On the other hand, illegal access to protected resources could be enabled by a compromised PE or PA.
5. *Monitoring techniques and tools:* To support dynamic and contextual policies, various monitoring techniques and tools from different vendors are employed by enterprises to monitor the network and collect data, which can become a target for adversaries. When proprietary data formats and vendor-specific solutions are relied upon by companies, they effectively lock themselves into a limited subset of providers due to interoperability issues. If a security issue or disruption is experienced by one of the providers, excessive costs and significant amounts of time will be involved in migrating to another provider.

Although existing technologies can help mitigate these cyber threats, more attention should be paid to them by developers and architects while creating a zero-trust product and implementing a robust zero trust architecture.

VI. Conclusion, Discussion, And Future Works

Zero trust is a novel and promising cybersecurity management framework with the philosophy of “never trust, always verify.” Due to its prominence across industries and the demands made by the federal government of the United States, ZT must be taught by educators in cybersecurity courses to better prepare our new cybersecurity professionals.

To help a busy professor prepare and introduce ZT effectively, an overview of an educational module that has been used by us to teach zero trust in our cybersecurity course has been provided. This module includes a class lecture, an essay homework assignment, and test questions. The lecture features an introduction to the basic concepts and principles of ZT along with its short evolution history. To understand why ZT has become a new trend in cybersecurity strategy, the design issues that arise in the traditional perimeter-based network security model were discussed by us and ZT architectures, which are referred to as solutions that meet the cybersecurity requirements of an organization, were described. Then, it was talked about by us how the problems in a traditional perimeter-based model can be effectively mitigated through the implementation of a zero-trust architecture. However, nothing is perfect.

This module was used by us to introduce ZT in cybersecurity courses at senior undergraduate and graduate levels. Positive feedback is generally provided by students. However, using it for lower-level courses is not recommended by us because the necessary background knowledge is lacking in the audience. For example, in the NIST zero trust architecture, many subsystems, including PKI (Public Key Infrastructure), SIEM (Security Information and Event Management), and threat intelligence, are integrated. This background knowledge may be lacking in junior students. In such cases, the concept of zero trust may be briefly introduced at a higher level, and its usefulness may be explained by us. Learning activities include a class lecture (about one hour and 15 minutes) and a homework assignment. Test questions are comprised of multiple choice and short answer questions to evaluate the outcomes of the class lecture. The classic papers by John Kindervag and NIST SP800-207 are encouraged to be read by students as part of the homework assignment, after which an essay explaining why zero trust is helpful must be written by them. Their own stories and observations from the real world must be integrated by students. When time permits, group discussions can effectively engage students with real-world examples.

Cybersecurity educators will be enabled by our work to introduce ZT basics in security courses, thereby better preparing future professionals. More engaging activities, such as hands-on tasks, games, or presentations, are aimed to be created by us.

REFERENCES

[1] Gaurav, “The future of network security: Why zero trust is becoming the new standard,” Insights2Techinfo, Online, August 2024, available online at: https://insights2techinfo.com/the-future-of-network-security-why-zero-trust-is-becoming-the-new-standard/. Retrieved on August 7, 2024.

[2] Appgate, “Zero Trust Platform,” Web site, 2025, https://www.appgate.com/zero-trust-network-access/zero-trust-platform. Last accessed on March 18, 2025.

[3] Google, “BeyondCorp: A new approach to enterprise security,” Website, 2022, https://cloud.google.com/beyondcorp. Last accessed on May 16, 2022.

[4] M. Compastié, R. Badonnel, O. Festor, R. He, and M. Kassi-Lahlou, “A software-defined security strategy for supporting autonomic security enforcement in distributed cloud,” in 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). New York City, NY, USA: IEEE, 2016, pp. 464–467.

[5] A. Moubayed, A. Refaey, and A. Shami, “Software-defined perimeter (sdp): State of the art secure solution for modern networks,” IEEE Network, vol. 33, no. 5, pp. 226–233, 2019.

[6] Y. Chen, H.-c. Hu, and G.-z. Cheng, “Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties,” Frontiers of Information Technology & Electronic Engineering, vol. 20, no. 2, pp. 238–252, 2019.

[7] A. Bride and J. Garofalo, “Network security approaches and the case for zero trust: On behalf of Zscaler,” Survey Report, IDG Communications, Inc., Online, June 2022, available online at: https://www.zscaler.com/resources/industry-reports/idg-network-security-for-zero-trust.pdf. Retrieved on September 12, 2024.

[8] Paloalto, “Zero trust with zero exceptions: Secure the future of hybrid work with ZTNA,” Web site, 2022, https://www.paloaltonetworks.com/. Last accessed on May 16, 2022.

[9] S. Turner, D. Holmes, C. Cunningham, J. Budge, P. McKay, A. Cser, H. Shey, and M. Maxim, “A practical guide to a zero-trust implementation,” Forrester Research, Online, March 2021, available online at: https://4719eaee91034be722d8c86a406a93c55de2464febd03debd4f0.ssl.cf1.rackcdn.com/A_Practical_Guide_To_A_Zero_Trust_Implementation.pdf. Retrieved on March 18, 2025.

[10] C. Cunningham, S. Balaouras, R. Perdoni, and P. Dostie, “The Forrester waveTM: Zero Trust eXtended (ZTX) ecosystem providers, q4 2018: Tools and technology: The security architecture and operations playbook,” Forrester Research, Online, November 2018, available online at: https://docs.broadcom.com/doc/the-forrester-wave-zero-trust-extended-ecosystem-providers-q4-2018-en. Retrieved on June 23, 2022.

[11] E. Bertino, “Zero trust architecture: Does it help?” IEEE Security & Privacy, vol. 19, no. 05, pp. 95–96, sep 2021.

[12] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, “Zero trust architecture (ZTA): A comprehensive survey,” IEEE Access, vol. X.2021, pp. 1–36, 2022.