Open Access License Notice

A Zero Trust Module for Cybersecurity Education

Xinli Wang
College of Computing
Grand Valley State University
wangx@gvsu.edu
0009-0007-0939-237X

Vijay Bhuse
College of Computing
Grand Valley State University
bhusevij@gvsu.edu
0009-0009-6460-6048

Yuan Cheng
University of Nottingham
Ningbo China
yuan@ycheng.org
0000-0001-7176-3951

Abstract—Zero Trust (ZT) is a conceptual and architectural framework for cybersecurity teams to design networks into secure micro-perimeters and strengthen data security with dynamic and context-aware policies by systematically integrating state-of-the-art technology, risk management, and threat intelligence. Both theoretical analysis and industrial practice have shown that ZT can ensure that organizations are not victims of known attacks or fail to discover a breach for a long time. ZT has recently gained momentum in industry to defend against lateral movement of malicious actors in today's borderless networks. The United States 2021 President Executive Order requires the federal government must adopt security best practice and advance toward a Zero Trust Architecture (ZTA). However, it is not a trivial task to implement a ZTA due to its novelty and complexity. We need to understand what ZT or ZTA is to take full advantage of it. Therefore, there is a need to introduce the fundamental concepts, principles, and architectures of ZT in cybersecurity courses at a college to better prepare our new cybersecurity professionals for their careers.

In the last few years, we have developed a module and used it to introduce ZT in cybersecurity courses at senior undergraduate and graduate levels. This module consists of a lecture to introduce ZT, a homework assignment, and test questions. The lecture includes an introduction to ZT and its principles, design issues in the traditional model of perimeter-based network security, zero trust architectures, security benefits of ZT, technical challenges to implement a ZTA, and the main threats to ZT networks. This article provides an overview of this module with the emphasis on the contents of the lecture. We will also share the experience and lessons we have learned in our teaching practice. Our work will provide a good reference for those who teach cybersecurity courses at a college or university or are developing a cybersecurity curriculum. It will also help busy professors develop or revise a zero-trust module for their cybersecurity courses.

Keywords—*Zero Trust; Education; Cybersecurity; Zero Trust Architecture*

I. INTRODUCTION

Zero Trust (ZT) has recently gained prominence as a new standard in cybersecurity management due to its dynamic and context-aware approach to address the issues brought by the remarkable changes in the cybersecurity landscape [1]. Nowadays, a typical infrastructure of information technology (IT) for an enterprise consists of multiple internal networks, branch offices and subcontractors with their local networks, remote and mobile employees with the policy of "bring your own device", cloud computing services, and Internet-of-Things (IoT) devices [2]–[5]. This IT landscape has formidably challenged the ability of a traditional perimeter-based network security model, as indicated by the increasing number of data breaches and successful hacking attacks [3], [6]–[10]. The perimeter-based security architecture is based on the separation between internal and external networks along with traditional static and implicit network-based measures [1], [11]. All users, devices, and services on the internal networks are trusted by default, while those from the external networks are untrustworthy. However, this model does not work in the current cybersecurity landscape because such a perimeter on the IT infrastructure of an enterprise does not exist as explained later in Section III, due to the pervasive use of cloud computing services, IoT devices, remote workers, subcontractors, and so on.

The concept of zero trust was created by John Kindervag [11]–[14]. It is a novel framework for cybersecurity management founded on the philosophy of "never trust, always verify." It helps in preventing security breaches by replacing implicit trust with explicitly evaluated, real-time adaptive trust levels, and just enough access to enterprise computing resources and data [2]. As a cybersecurity management strategy, ZT has recently been widely adopted across industries [14], [15]. The federal government of the United States has ordered the adoption of zero trust in their cybersecurity management to improve the nation's security [16], [17]. Several frameworks have been developed recently to implement the principles of zero trust. Examples include Google's BeyondCorp [18], [19], the Appgate zero trust access [20], [21], Palo Alto zero trust network access [22], and VMware secure access [23]. A recent comprehensive evaluation of 15 ZT products has been conducted by Forrester Research [24]. Most of the evaluated frameworks have been well developed. More recently, a comprehensive framework has been proposed to guide industries for migrating to ZT [25]. Accordingly, the National Institute of Standards and Technology (NIST) of the United States has proposed a Zero Trust Architecture (ZTA) [26] to guide the federal government to advance toward ZT in cybersecurity infrastructure.

However, the adoption of ZT is not straightforward due to its novelty and the challenges it brings to the organization and IT professionals [26]–[28]. Although industry leaders are committed to ZT, most organizations have not succeeded in replacing the existing solutions [29]. It is imperative to understand this cybersecurity strategy before a decision is made to implement a ZT or replace the existing solution with it [30]. A recent survey conducted by the Cloud Security Alliance (CSA) [15] has noticed that the lack of knowledge and expertise (40% out of 823 responses) and additional staffing needs (34% out of 823 responses) are two of the top business barriers to adopting ZT strategy in their organization. Therefore, there is a need to introduce the concepts and principles of ZT along with its architectures, benefits, and challenges in college cybersecurity courses to better prepare our new cybersecurity professionals for their careers. This is especially true for graduate-level cybersecurity courses. However, it is not a trivial task for a busy educator to do so due to the limited availability of vendor-agnostic and scientific critical literature [31]. Although a few surveys have been published on the technical aspects [32], [33] and research gaps [30] of ZT as well as ZTA [34], little work has been reported on ZT security in the perspective of cybersecurity education.

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

1. A lecture to introduce the principles, architectures, and challenges of zero trust.
2. An open-end homework assignment designed for students to develop an in-depth understanding of zero trust through self-study. The essay is a collaborative teamwork effort.
3. Test questions including multiple choice questions and short answer questions to evaluate the students learning outcomes.

In this paper, we emphasize introducing the development of this lecture in this paper. It includes the following components:

1. The basic concepts of ZT and the principles it follows to implement a ZTA. This is to answer what ZT is and what the principles are. A short evolution history and current state of ZT are also introduced along with recent survey data.
2. Security issues in the design of a traditional perimeter-based security model. We discuss the problems with perimeter-based network security to answer the question “why would we need zero trust?”
3. Zero trust architectures. To understand how the design issues in the traditional network security model can be addressed, we introduce several proposed zero trust architectures with an emphasis on the NIST [26] zero trust architecture.
4. Main security benefits from the ZT strategy. In addition to addressing the existing issues in the design of a perimeter-based network security model, we summarize several other benefits of ZT from the literature.
5. Technical challenges to migrate to a ZTA. There are technical and non-technical challenges. We emphasize on technical challenges in ZTA implementation.
6. Potential cyber threats to a ZTA. As a new cybersecurity framework, ZT cannot address every security issue and may bring new problems that need to be considered when a ZTA is adopted. This component is to discuss potential vulnerabilities of ZTA that need to be addressed.

Each of these components will be presented in the following sections. Experience and lessons we learned will also be shared.

The rest of this paper is organized as follows: After introducing the basic concepts and principles as well as a short evolution history of ZT in the next section, the design limitations in the traditional perimeter-based model of network security is discussed in Section III. We introduce zero trust architecture in Section IV. Then we discuss the security benefits of implementing a ZTA in Section V to explain how these issues can be effectively mitigated or removed by the implementation of a ZTA. Technical challenges to practice ZT in an organization and potential threats to a ZTA will also be discussed in this section. Finally, we conclude our work and share the experience and lessons that we have gained from our teaching practice. Learning activities and future work will also be described in this section.

II. ZERO TRUST AND ITS PRINCIPLES

In the last one and half decades, zero trust has evolved from a term, which simply conveys the idea that nothing can be trusted without appropriate verification on the network [12], to a well-developed strategy for cybersecurity management with a complete set of principles to practice ZT [26], [35]. It is worth introducing this short history and the current understanding of zero trust.

A. Zero Trust and Its Evolution

Zero trust was created by John Kindervag in 2010 to recommend that organizations should not extend trust to anything inside or outside of their network perimeters [12], [14]. There had been various discussions and implementations in the industry and academia since then [18], [36]–[39]. 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 [26]. A timeline of zero trust evolution is given by Zscaler [40].

Although there is no single agreed-on definition yet [41], ZT is widely recognized as a security model or a framework with a collection of concepts and principles devised to minimize uncertainty in enforcing least privilege access decision in information systems, services, and workloads in the face of a network viewed as compromised [26], [42]. This framework requires all users, devices, services, and workloads, whether inside or outside the organization network, to be authenticated, authorized, and dynamically validated for security policy and posture before being granted or keeping access to applications and data [11], [26], [34], [42], [43]. The goal is to more effectively enforce the principle of least privilege.

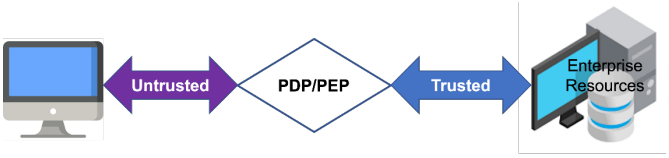

Fig. 1. A diagram of ZT as an access control method

A high-level look at ZT is that it can be considered as a kind of access control model [42], as shown in Figure 1, with which any request to access a network, workload, or data item is granted utilizing policies informed by continuous, contextual, and risk-based verification across users and their associated devices. Compared with the traditional perimeter-based security model, as described in Section III, the "perimeter" in a ZT framework can be considered as a software-defined perimeter consisting of policy decision point and policy enforcement point [21], [26]. Details will be discussed in Section IV.

B. *Principles of Zero Trust*

ZT security strategy is a collection of guiding principles for workflow, system design, and operation that can be employed to improve the security posture of a system. NIST [26] summarizes these principles as seven tenets as depicted in Figure 2. More recently, Forrester Research [42] gives a similar list of principles.

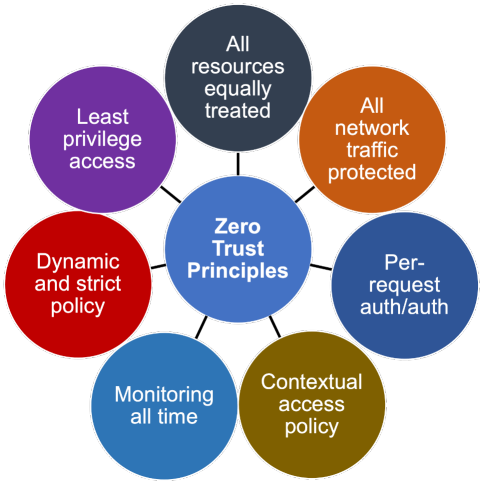

Fig. 2. Tenets of zero trust (derived from NIST [26])

As depicted in Figure 2, we summarize these ZT principles below:

- Resources of an organization comprise all data sources and computing services. These include data on its internal networks and stored in clouds. Computing services can also be on its internal networks and provided by cloud computing providers.
- All network communication must be secured regardless of network location. There is no difference between the communication from either enterprise-owned networks or external networks.
- Access to individual organization's resources must be authenticated and granted on a per-session basis.
- Access to resources is determined by the context at the time the access is requested [42]. The context is evaluated from the observable state of client identity, service, requested resource, and other behavioral and environmental attributes. Examples include the network status and malware detection result.
- Continuous monitoring is implemented. The organization monitors and diagnoses the integrity and security posture of all owned and associated assets. All the collected data will be used to implement contextual access control.
- Authentication and authorization to access a resource are dynamically and strictly enforced before the access is allowed.
- The principle of least privilege must be implemented. Authentication and authorization to one resource will not automatically grant access to a different resource.

The approach for implementation is not specified. For example, multi-factor authentication is recommended [26]. However, it is not required for every case. An organization can choose different authentication methods to meet their needs.

III. DESIGN PROBLEMS IN THE TRADITIONAL PERIMETER-BASED NETWORK SECURITY MODEL

It is helpful to examine the main problems of the traditional perimeter-based security approach in a modern enterprise environment to understand the issues ZT tries to resolve before delving into it. Figure 3 depicts a simplified conceptual diagram of a traditional perimeter-based network security model that is typically implemented on an enterprise infrastructure. An organization has its own internal network connecting servers, workstations, laptop computers, and other devices. These networked devices are protected with a firewall at the "edge" between the internal and external networks [6], [31], [44]–[46]. Devices and network traffic on the internal network are implicitly trusted. Typically, an organization will allow remote or home workers and subcontractors to use their own devices to access the internal network. Subcontractors can have their own servers or networks. Commercial cloud computing providers are

contracted to provide certain services such as processing and storing sensitive data. Remote workers and subcontractors can access the clouds. They can also access the internal network through a VPN server, where strong authentication methods can be enforced. Note that Figure 3 is only a simplified diagram for the purpose of demonstration. A demilitarized zone (DMZ) and other devices, such as IoT devices and edge computing platforms, may exist in reality [26], [31], which make the network more complicated.

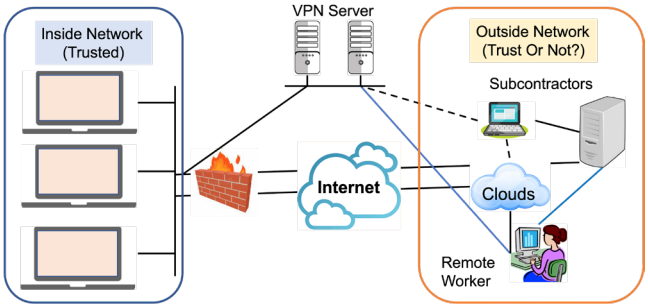

Fig. 3. A diagram of a perimeter-based security model

This was an appropriate design at the time when cloud computing was not yet widely adopted. However, the main problem with the above network configuration is that there is no such a boundary that separates the internal network from the external networks in such an environment. Although the remote workers and subcontractors can access the internal network through a VPN proxy server, the applications running in the clouds providing services to the organization also need to access the internal network. Apparently, the public cloud computing providers are external to the organization.

Furthermore, there are three basic threat vectors to the network settings shown in Figure 3 [33]:

- A user's credentials may have been compromised and used in an attack to gain access to the inside network or the subcontractor's networks. This technique was used in the Operation Aurora attacks [47], which triggered Google to launch their BeyondCorp project [18], [48] a decade ago.
- A device may be compromised by installing a malware program from a successful phishing email on the internal network, or on the subcontractor's network, or from a remote worker. That compromised device can then attack other devices on the internal network.
- A software system – like an application programming interface (API) or application – can be compromised and that can negatively impact or infect data on the internal network, the subcontractor's network, or the remote worker's computers.

If we think about the number of devices we have on the networks and from remote workers, the number of users, and the number of vendors, we can see how the risk to the organization and its partners has increased exponentially. The above three threat vectors are generally recognized as "lateral movement" [31], which means that adversaries, who manage to successfully compromise a user's device, can move on to compromise other devices on the same network due to the nature of implicit trust.

IV. ZERO TRUST ARCHITECTURES

While the term zero trust is commonly known 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 a solution to address the cybersecurity needs of an organization [26], [49], [50]. Depending on the needs, different zero trust architectures can be designed. In general, a ZTA utilizes ZT concepts, follows ZT principles, and encompasses the relationships of components, workflow planning, as well as access policies that need to be properly integrated and strategically implemented to better secure the assets of an enterprise [26], [34]. Several surveys on ZTA have been published [31], [34], [41], [51]. We introduce the NIST ZTA [26] and Forrester Research Zero Trust eXtended (ZTX) ecosystem [52] in this section.

A. *NIST Zero Trust Architecture*

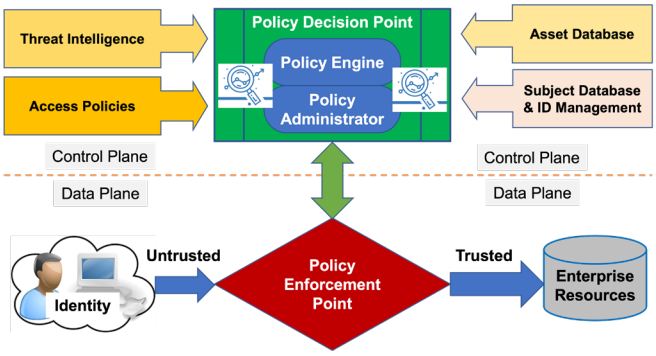

Fig. 4. Zero trust architecture

The NIST ZTA is based on the architecture of zero trust network [53], where a network is divided into two planes: *data plane* and *control plane*. As shown in Figure 4, it consists of two main components [26]. A Policy Enforcement Point (PEP) is located in the data plane. A Policy Decision Point (PDP) is located in the control plane.

- The PEP acts as a communication portal between two sides: an untrusted subject and enterprise assets. When a subject, such as a user, a computer, or a process on the behalf of a user, in the untrusted zone wishes to access a resource, such as a data item or a computing server, in the trusted domain, the subject must submit a request to PEP first, which then forwards this request to the PDP along with the subject's credentials. When a decision is made by PDP, the PEP is responsible for dynamically

enabling, monitoring, and eventually terminating connections between a subject and an enterprise asset.

- The PDP consists of a Policy Engine (PE) and a Policy Administrator (PA). The PE hosts ZT algorithms for making the decision to grant, deny, or restrict access to the asset the subject is seeking for. Inputs to the engine include enterprise policies, monitoring data, and external sources. These input data are collected and maintained dynamically by integrated subsystems. Examples are an ID management system, a continuous diagnostics and mitigation system, a Security Information and Event Management System (SIEM), industry compliance, threat intelligence, and activity logs. The PA coordinates the decision made by PE and is responsible for establishing and/or shutting down the communication path between the subject and the enterprise asset by sending appropriate commands to PEP in the data pane.

In this NIST architecture, the PEP works pretty much as an access login portal as depicted in Figure 1. The ZT features of dynamic, context-aware, and real-time policy are implemented at the policy decision point that runs at the back end. The separation of PEP from PDP is a great design to have a minimum exposure of the system.

Here is an example to show how the NIST solution may work. When a user in the untrusted domain wishes to access a data item in the trusted domain, the user will need to submit a request to PEP first, which then forwards this request to PDP along with the user's credentials (user ID and login information). At PE, there can be multiple checks before a decision is made. The first check is on the authentication of the identity. The level to which authentication is carried out may change depending upon the environment. The next step is to determine whether the security posture of the user satisfies the security need to be allowed access. The PE makes a decision using risk-based policies, which can change at any time to reflect the latest situation. When a decision is made, PE passes the result to PA, which then either establishes or shuts down the communication path between this user and the requested data via appropriate commands to the PEP. If the access is allowed, the PEP would generate a session-specific authentication token used by the user to access the requested data. When a user has been granted access to requested data, its activities of access will be monitored and evaluated continuously. Depending on the monitoring results and the security posture of this user, his/her access can be either continued or terminated.

B. *Forrester Research Zero Trust Extended Ecosystem Framework*

More recently, Forrester Research has evolved the initial ZT concept [12], [13] into a more advanced Zero Trust eXtended (ZTX) ecosystem framework [52], [54], [55] with a modern definition of the ecosystem [42]. As shown in Figure 5, ZTX framework extends data flows across local networks, cloud computing infrastructure, external applications and websites, and a wide range of endpoint devices, including IoT devices. Cunningham *et al*. [52], [54] have provided a good description of the technologies that can be used to support each item in the framework.

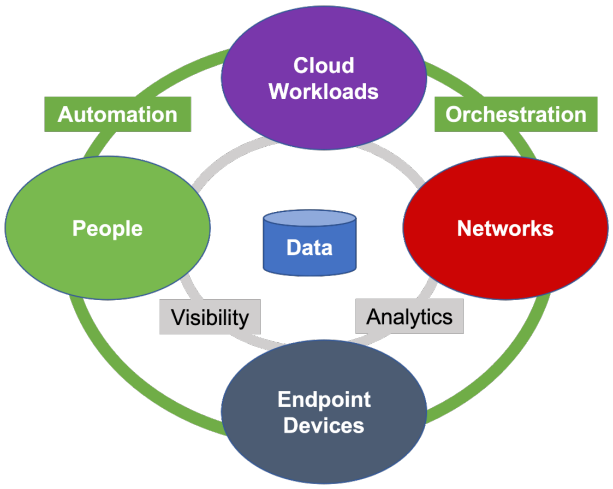

Fig. 5. The Forrester ZTX framework (derived from Forrester Research [52])

While the details included in the NIST architecture (Figure 4) provides a good guideline for the US Federal government to implement, the ZTX provides general guidelines for practicing ZT at an organization. To protect the data of an organization, all the data users, including human beings, cloud workloads, networks, IoT devices, etc., must be considered to provide an automatic and orchestral environment. At the same time, the whole environment and activities must be monitored continuously to make them visible. All monitored data must be analyzed online with appropriate models to make real-time and context-aware decisions.

ZTA is not a single cybersecurity product or a single solution for an enterprise cybersecurity architecture [43]. While numerous guidelines to ZTA deployment exist from different vendors [56]–[58] and research institutes [15], [55], [59], implementation of ZTA is organization-specific. It must be based on an extensive analysis of the organization's security needs, current infrastructure, risk management, and so on, to effectively adopt and implement a ZT security model.

V. DISCUSSION ON ZERO TRUST

We will discuss the benefits of ZTA in terms of information security protection, the technical challenges for an organization to adopt and implement a ZTA, and the potential cyber threats associated with a ZTA.

A. *Security Benefits from Zero Trust Architecture*

Compared with a traditional perimeter-based security architecture briefed in Section III, the security benefits of ZTA can be summarized as follows:

1. Removal of physical perimeter: As shown in Figures 1, 4, and 5, a perimeter is effectively removed from a ZTA. All access requests are authenticated and

authorized based on the identity of a subject at the PDP and enforced by PEP [13], [26], [41], [52], [55]. This allows an enterprise to adapt security architecture to support new user populations such as remote employees, partners, customers, rapid cloud adoption, and new IoT devices and sensors.

2. Effective mitigation of lateral movement: In a fully-featured implementation of ZTA, it is highly unlikely that an adversary or malware program will be able to spread through a network starting from a compromised endpoint device. This is because ZTA provides end-to-end protection. Any access request, no matter where it is initiated, must be first authenticated with the subject identity through an identity management system, then the posture of the subject and the device or the application from where the request is submitted on behalf of the subject is evaluated against a threat intelligence subsystem. The access is authorized based on dynamic and contextual policies that can change at any time based on real-time data and the result of risk analysis [18], [26], [41], [48], [52]. This will significantly reduce the damage a single compromised device can do to an enterprise network no matter how this device is compromised (e.g., compromised user credentials, malware installation, or vulnerable API, see Section III for details). The preliminary experimental results provided by DeCusatis *et al*. [6] have shown an effective mitigation of lateral movement in a cloud computing environment where a ZTA is implemented. The industry [60] has also observed the fact of effective mitigation of lateral movement on internal networks.

3. Quicker detection of compromised devices and data breaches: On a traditional perimeter-based network, it can take weeks or months for security teams to detect a data breach [61], [62]. Network visibility is one of the main factors in such long-lasting data breaches [63], [64]. With ZTA, the systems are watching and the status of the system is analyzed continuously with SIEM, continuous diagnostics and mitigation subsystem, along with system and security logging systems and threat intelligence system (see in Section IV for details). This ability to inspect all network traffic and packets through the application layer provides the security operation teams with visibility. Experimental results [63] have shown that the more visibility a security team has into the network across the business ecosystem, the better chance the security team has to quickly detect the tell-tale signs of a breach in progress and stop it.

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

B. Technical Challenges to Practice Zero Trust

While ZTA is promising to resolve problems in traditional perimeter-based networks; it comes with challenges in implementation and operation of a ZTA. We summarize the technical challenges in this subsection.

1. Huge number of complicated policies: To mitigate the lateral movement of adversaries, ZTA enforces micro-segmentation and fine-grained security controls [26], [55]. In the operation of a ZTA infrastructure, huge numbers of policies are expected to be specified, implemented, deployed, and managed [65]. These policies will be attribute-based [66], [67], that is, based on properties of subjects, protected resources, and contexts [26], [34], [55]. While new semantics can be developed and used for security policy specification and testing [68], the specification, development, and management of these policies are not a trivial task [65]. In addition, when some attributes cannot be trusted, some risk-based criteria must be used for control-related decisions [66]. Such criteria are often difficult to formalize and automate as they are application dependent. These factors together make the policy management complicated and error-prone.

2. Effective integration of various systems: As explained in Subsection IV, many components and systems, such as CDM system, threat intelligence, security and system logging, SIEM, and so forth, must be effectively integrated and properly managed to facilitate the decision of authentication and authorization by PDP. It is not straightforward even to deploy and operate such systems individually [69]–[71]. Effective integration of these systems can be expected to be highly challenging.

3. Lack of standardization: Due to its novelty and complexity, ZTA is still in its evolving stage. It is unlikely to be standardized in any way in a short time. Different vendors design and develop their products in different ways [18]–[23]. Recent evaluation results by Forrester Research [24] show that most products from different vendors meet the main requirements of ZTA. However, they are designed and developed for specific purposes. When a user selects any of them, the user has to lock into it due to interoperability issues. If the infrastructure has changed, it can be challenging to switch to another ZT product without extra cost and time.

C. Potential Cyber Threats Associated with Zero Trust Architecture

NIST [26] presents a list of potential cyber threats associated with ZTA in their SP 800-207. They are summarized below:

1. Subversion of ZTA decision process: As presented in Section IV, the policy engine and policy administrator are the key components of the entire enterprise in a ZT environment. PEP and PDP are the single points of failure in the NIST ZTA. There will be no communication between enterprise resources and subjects unless it is approved and configured at PE and PA. This implies that PE and PA must be properly configured and maintained. Any enterprise administrator with the privilege to configure and maintain the rules in PE and PA may be able to make unapproved changes or mistakes that can disrupt the enterprise operations. On the other hand, a compromised PE or PA could allow illegal access to protected resources.
2. Denial-of-service attack: As shown in Figure 4, enterprise resources cannot be connected to each other without the permission of PE and configured action at PA. If an adversary disrupts or denies access to the PEP or PDP (PE/PA) with denial-of-service attacks or route hijack, it can adversely impact the operation of the entire enterprise infrastructure.
3. Stolen credential and insider threat: While ZTA can effectively mitigate the lateral movement of adversaries, the already authenticated and authorized session of a compromised endpoint (stolen credentials or an insider) can be leveraged to carry out malicious activities.
4. Monitoring techniques and tools: To support dynamic and contextual policies, various monitoring techniques and tools from different vendors are employed to monitor the network and collect data, which can be a target for adversaries. Reliance on proprietary data formats and vendor-specific solutions will make an enterprise locked into a subset of providers due to interoperability issues. If one of the providers has a security issue or disruption, migration to another provider will involve excessive cost and time.
5. Use of non-person entities in ZTA administration: Identity-based authentication is employed in a zero trust architecture. This includes human users and devices. It is still an open question [26] how these non-human entities, including devices, applications, and workloads, authenticate themselves in an enterprise implementing a zero trust architecture.

Although existing technologies can be employed to mitigate these cyber threats [26], [31], more attention should be paid to them while developing a zero trust product and implementing a 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 demands by the federal government of the United States, there is a need to teach ZT in cybersecurity courses to better prepare our new cybersecurity professionals. To help a busy professor prepare and introduce ZT, we have provided an overview of an educational module that we have been using to teach zero trust in a cybersecurity course. This module includes a class lecture, an essay homework assignment, and test questions. The lecture includes 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 a cybersecurity strategy, we discussed the design issues in the traditional perimeter-based network security model and described ZT architectures, which are referred to as solutions to meet cybersecurity requirements of an organization. Then, we discussed how the problems in a traditional perimeter-based model can be effectively mitigated by implementing a zero-trust architecture. However, nothing is perfect. ZT itself has its challenges and limitations as discussed in Section V.

We have used this module to introduce ZT in cybersecurity courses at senior undergraduate and graduate levels. Feedback from the students is generally positive. However, it is not recommended to use it for a course at a lower level because the audience does not have the background knowledge yet. For example, in the NIST zero trust architecture [26], many subsystems, including PKI (Public Key Infrastructure), SIEM (Security Information and Event Management), and threat intelligence, are integrated. Junior students may not have such background knowledge. If this is the case, it may be appropriate to briefly introduce the concept of zero trust at a higher level and explain why it can be helpful.

Learning activities in this module includes a class lecture (about one hour and 15 minutes) and a homework assignment. Test questions include multiple choice questions and short answer questions to evaluate outcomes of the class lecture. The homework assignment encourages students to read the classic papers by John Kindervag [12] and NIST SP800-207 [26]. Then, write an essay to explain why zero trust is helpful. Students are required to integrate their own stories and observations from the real world. When time permits, group discussions can be a good learning activity to engage students with real-world examples.

Our work will help cybersecurity educators to introduce ZT basics in a security course to better prepare our future cybersecurity professionals for their careers.

In the future, we would like to develop more activities, such as hands-on activities, a game, or a presentation, to engage students in an active learning environment.

REFERENCES

[1] A. 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] 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.

[3] 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.

[4] 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.

[5] 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.

[6] C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing zero trust cloud networks with transport access control and first packet authentication," in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*. New York city, NY, USA: IEEE, 2016, pp. 5–10.

[7] M. Shlapentokh-Rothman, E. Hemberg, and U.-M. O'Reilly, "Securing the software defined perimeter with evolutionary co-optimization," in *Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion*, ser. GECCO '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1528–1536. [Online]. Available: https://doi.org/10.1145/3377929.3398085

[8] C. Cimpanu, "SEC filings: SolarWinds says 18,000 customers were impacted by recent hack," ZDNet, online, December 2020, available online at: https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/. Retrieved on May 26, 2022.

[9] Z. A. Collier and J. Sarkis, "The zero trust supply chain: Managing supply chain risk in the absence of trust," *International Journal of Production Research*, vol. 59, no. 11, pp. 3430–3445, 2021.

[10] E. Salam, "Cyber-attack forces shutdown of one of the US's largest pipelines," US News, online, May 2021, available online at: https://www.theguardian.com/technology/2021/may/08/colonial-pipeline-cyber-attack-shutdown. Retrieved on May 26, 2022.

[11] M. Campbell, "Beyond zero trust: Trust is a vulnerability," *Computer*, vol. 53, no. 10, pp. 110–113, 2020.

[12] J. Kindervag, S. Balaouras, and L. Coit, "No more chewy centers: Introducing the zero trust model of information security," Forrester Research, Online, September 2010, available online at https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf. Retrieved on August 19, 2024.

[13] ——, "Build security into your network's DNA: The zero trust network architecture," Forrester Research, Online, November 2010, available online at: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. Retrieved on May 19, 2022.

[14] D. Golden, A. Perinkolam, M. Nicholson, K. Norton, A. Perinkolam, A. Rafla, and W. Rockall, "Zero trust: Never trust, always verify – security in the age of the porous perimeter," Deloitte© Insights, Tech Trends 2021, Online, 2021, available online at: https://www2.deloitte.com/us/en/insights/focus/tech-trends/2021/zero-trust-security-framework.html. Retrieved on August 31, 2024.

[15] H. Baron, J. Yeoh, I. Armstrong, J. Buker, D. Catteddu, S. Heide, A. Kaluza, C. Lehnert, S. Lumpe, and J. Reavis, "CISO perspectives and progress in deploying zero trust," Cloud Security Alliance (CSA), Online, June 2022, available online at: https://cloudsecurityalliance.org/artifacts/ciso-perspectives-and-progress-in-deploying-zero-trust/. Retrieved on June 21, 2022.

[16] The White House, "Executive order on improving the nation's cybersecurity," Briefing Room, The White House, Online, May 2021, available online at: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. Retrieved on March 18, 2025.

[17] The White House, "National cybersecurity strategy," The White House, Online, March 2023, available online at: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Retrieved on March 18, 2025.

[18] R. Ward and B. Beyer, "BeyondCorp: A new approach to enterprise security," *;login:*, vol. Vol. 39, No. 6, pp. 6–11, 2014.

[19] Google, "BeyondCorp: A new approach to enterprise security," Web site, 2022, https://cloud.google.com/beyondcorp. Last accessed on May 16, 2022.

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

[21] Appgate, "Appgate SDP," Web site, 2022, https://www.appgate.com/zero-trust-network-access. Last accessed on June 9, 2022.

[22] 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.

[23] VMware, "VMware secure access," online, 2022, https://www.vmware.com/docs/vmw-sdwan-zero-trust-service-so. Last accessed on March 18, 2022.

[24] D. Holmes, J. Blankenship, C. Provost, and P. Dostie, "The forrester new wave™: Zero trust network access, q3 2021 – the 15 providers that matter most and how they stack up," Forrester Report, Online, August 2021, available online at: https://www.forrester.com/report/the-forrester-new-wave-zero-trust-network-access-q3-2021/RES176124. Retrieved on March 18, 2025.

[25] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," *IEEE Access*, vol. 11, pp. 19 487–19 511, 2023.

[26] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST SP 800-207, August 2020, available online at: https://csrc.nist.gov/publications/detail/sp/800-207/final. Retrieved on May 12, 2022.

[27] C. Cunningham, "Next-generation access and zero trust," Forrester Featured Blogs, Online, March 2018, available online at https://www.forrester.com/blogs/next-generation-access-and-zero-trust/. Retrieved on May 11, 2022.

[28] S. Shackelford, "Zero-trust security: Assume that everyone and everything on the internet is out to get you – and maybe already has," The Conversation, May 2021, available online at: https://theconversation.com/zero-trust-security-assume-that-everyone-and-everything-on-the-internet-is-out-to-get-you-and-maybe-already-has-160969. Retrieved on May 6, 2022.

[29] M. Polacek, "Leaders are now committed to zero trust – zero trust is a digital business enabler for all size firms," Forrester Research, Online, October 2020, available online at: https://info.cloudflare.com/rs/713-XSC-918/images/Forrester_Opportunity_Snapshot_for_Zero_Trust.pdf. Retrieved on March 18, 2025.

[30] C. Buck, C. Olenberger, A. Schweizer, F. Vo¨Ister, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Computers & Security*, vol. 110, pp. 102 436: 1–26, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821002601

[31] L. Alevizos, V. T. Ta, and M. Hashem Eiza, "Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review," *SECURITY AND PRIVACY*, vol. 5, no. 1, p. e191, 2022, e191 SPY-2021-0038.R2. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.191

[32] X. Yan and H. Wang, "Survey on zero-trust network security," in *Artificial Intelligence and Security*, X. Sun, J. Wang, and E. Bertino, Eds. Singapore: Springer Singapore, 2020, pp. 50–60.

[33] B. Embrey, "The top three factors driving zero trust adoption," *Computer Fraud & Security*, vol. 2020, no. 9, pp. 13–15, 2020.

[34] 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.

[35] The Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, "Department of defense (DOD) zero trust reference architecture, version 2.0," Unclassified Document, July 2022, available online at: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf. Retrieved on March 18, 2025.

[36] K. Townsend, "The history and evolution of zero trust," Security Week, Online, July 2022, available online at: https://www.securityweek.com/history-and-evolution-zero-trust/. Retrieved on August 31, 2024.

[37] D. Heath, "The evolution of zero trust and the frameworks that guide it," IBM, Online, April 2023, available online at: https://www.ibm.com/blog/the-evolution-of-zero-trust-and-the-frameworks-that-guide-it/. Retrieved on August 31, 2024.

[38] C. Allen, "The evolution of zero-trust security," CryptoMathic, Online, May 2023, available online at: https://www.cryptomathic.com/news-events/blog/the-evolution-of-zero-trust-security. Retrieved on August 31, 2024.

[39] E. Atwell, "The history, evolution, and controversies of zero trust," Kolide, Online, 2024, available online at: https://www.kolide.com/blog/the-history-evolution-and-controversies-of-zero-trust. Retrieved on August 31, 2024.

[40] Zscaler, "A brief history of zero trust from the whiteboard to the white house," Zscaler, Online, 2022, available online at: https://www.zscaler.com/resources/infographics/brief-history-zero-trust.pdf. Retrieved on August 31, 2024.

[41] M. Shore, S. Zeadally, and A. Keshariya, "Zero trust: The what, how, why, and when," *Computer*, vol. 54, no. 11, pp. 26–35, 2021.

[42] D. Holmes and J. Burn, "The definition of modern zero trust," Forrester Research, Online, January 2022, available online at: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/. Retrieved on May 26, 2022.

[43] S. Turner, "Zero trust is not a security solution; it's a strategy," Forrester Research, Online, February 2021, available online at: https://www.forrester.com/blogs/zero-trust-is-not-a-security-solution-it-is-a-strategy/. Retrieved on May 26, 2022.

[44] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th ed. One Lake Street, Upper Saddle River, New Jersey 07458, USA: Pearson Education, Inc., 2006.

[45] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 4th ed. Upper Saddle River, NJ 07458, USA: Pearson, July 2021.

[46] T. D. Nadeau and K. Gray, SDN: *Software Defined Networks*, 1st ed. 1005 Gravenstein Highway North, Sebastopol, CA: O'Reilly Media, 2013.

[47] McAfee Labs and McAfee Foundstone Professional Services, "Protecting your critical assets: Lessons learned from "operation aurora"," White Paper by McAfee labs, Online, March 2010, available online at: https://web.archive.org/web/20160429214018/http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf. Retrieved on March 18, 2025.

[48] B. Osborn, J. McWilliams, B. Beyer, and M. Saltonstall, "BeyondCorp: Design to development at Google," *;login:*, vol. Vol. 41, No. 1, pp. 28 – 34, 2016.

[49] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of o-ran," *Computer Networks*, vol. 217, p. 109358, 2022.

[50] M. Hussain, S. Pal, Z. Jadidi, E. Foo, and S. Kanhere, "Federated zero trust architecture using artificial intelligence," *IEEE Wireless Communications*, vol. 31, no. 2, pp. 30–35, 2024.

[51] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 6476274, 2022.

[52] C. Cunningham, S. Balaouras, B. Barringham, and P. Dostie, "The zero trust extended (ZTX) ecosystem: Extending zero trust security across your digital business," Forrester Research, Online, January 2018, available online at: https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf. Retrieved on June 19, 2022.

[53] E. Gilman and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*, 1st ed. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Inc., June 2017.

[54] J. Blankenship, S. Balaouras, B. Barringham, and P. Harrison, "The forrester wave™: Security analytics platforms, Q1 2017: Tools and technology: The security architecture and operations playbook," Forrester White Paper, Online, March 2017, available online at: https://www.midlandinfosys.com/pdf/siem-security-product-comparison-reviews.pdf. Retrieved on June 24, 2022.

[55] 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://4719eaee91034be722d8-c86a406a93c55de2464febd03debd4f0.ssl.cf1.rackcdn.com/A_Practical_Guide_To_A_Zero_Trust_Implementation.pdf. Retrieved on March 18, 2025.

[56] J. Turner, "Zero trust architecture explained: The ultimate guide to zero trust security – never trust, always verify," Strongdm Blog, Online, February 2022, available online at: https://www.strongdm.com/zero-trust. Retrieved on May 16, 2022.

[57] J. Watts and N. MacDonald, "What are practical projects for implementing zero trust?" Gartner Document, Online, February 2022, available online at: https://www.gartner.com/en/documents/3999439. Retrieved on May 16, 2022.

[58] Microsoft, "Zero trust guidance center," Microsoft Documents, Online, May 2022, available online at: https://docs.microsoft.com/en-us/security/zero-trust/. Last visited on June 23, 2022.

[59] J. Koilpillai, J. Wadhwa, A. Harper, S. Parikh, P. Deakin, V. Tero, G. Bateman, A. Merchant-Dest, J. Kelley, P. Thomas, U. Rajagopal, and R. Choynowski, "Toward a zero trust architecture: A guided approach for a complex and hybrid world," Cloud Security Alliance (CSA), Online, October 2021, available online at: https://cloudsecurityalliance.org/artifacts/towards-a-zero-trust-architecture/. Retrieved on June 21, 2022.

[60] M. Loftus, A. Vezina, R. Doten, and A. Mashatan, "The arrival of zero trust: What does it mean?" *Communications of the ACM*, vol. 66, no. 2, pp. 56–62, 2023.

[61] T. S. Bernard, T. Hsu, N. Perlroth, and R. Lieber, "Equifax says cyberattack may have affected 143 million in the U.S." The New York Times, Online, Sept. 2017, Available online at: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html, Last visited on June 24, 2022.

[62] O. BEAVERS and A. BRELAND, "Equifax suffered hack months earlier than the date it disclosed," The Hill TV, Online, September 2017, Available online at: https://thehill.com/policy/cybersecurity/351253-equifax-suffered-a-hack-months-earlier-than-the-date-it-disclosed-report/, Last visited on June 24, 2022.

[63] C. Cunningham, S. Balaouras, R. Perdoni, and P. Dostie, "The Forrester wave™: 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.

[64] C. Cunningham, D. Holmes, J. Pollard, J. Blankenship, M. Cyr, and P. Dostie, "The eight business and security benefits of zero trust: Business case: The zero trust security playbook," Forrester White Paper, Online, September 2019, available online at: https://www.kennisportal.com/wp-content/uploads/2022/06/Akamai-the-eight-business-and-security-benefits-of-zero-trust-report.pdf. Retrieved on June 24, 2022.

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

[66] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2013.

[67] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[68] C. Katsis, F. Cicala, D. Thomsen, N. Ringo, and E. Bertino, "Can i reach you? do i need to? new semantics in security policy specification and testing," in *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 165–174. [Online]. Available: https://doi.org/10.1145/3450569.3463558

[69] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 35–41, 2014.

[70] I. Anastasov and D. Davcev, "Siem implementation for global and distributed environments," in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*. New York, NY, USA: IEEE, 2014, pp. 1–6.

[71] S. S. Sekharan and K. Kandasamy, "Profiling siem tools and correlation engines for security analytics," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSP-NET)*. New York, NY, USA: IEEE, 2017, pp. 717–721.