Modern Security Needs Modern Infrastructure: A Zero Trust Architecture

Jake Derkowski
Department of Computer Science
Cyber Forensics Intelligence Center
Sam Houston State University
Huntsville, TX, USA
jad084@shsu.edu

Kirk Burns
Department of Computer Science
Cyber Forensics Intelligence Center
Sam Houston State University
Huntsville, TX, USA
lib_kab@shsu.edu

***Abstract*—Zero Trust network model (ZTM) was designed by John Kindervag in 2010 to address a critical flaw that he had identified with the infrastructure and security of traditional networks: trust. A vulnerability that many organizations are only now aware of because of the recent changes in the workplace brought about by the COVID-19 pandemic. Unfortunately, many organizations were not prepared for the change to remote work and attackers saw opportunity and took advantage. This crisis expedited the adoption of various technologies as well as shown the areas in which new technologies were needed. A modern network infrastructure is now needed more than ever with the increase of remote work, the utilization of cloud computing, and other technological innovations has made the Zero Trust Model (ZTM) more relevant, applicable, and desirable than ever before.**

***Index Terms*—architecture, authentication, authorization, network security, zero trust**

I. Introduction

Over the past year, the COVID-19 pandemic has caused drastic changes in nearly every aspect of our life–especially in the workplace. This rapid transition from on-site work to working remotely has been difficult for many unprepared organizations but an easy *hook* malicious actors [1]. In this context, "hook" is defined as "any mechanism used to mislead a victim into falling prey of an attack". According to [1], people are more prone to fall prey to an attack when they are experiencing work pressure, personal change of situation, medical issues, or events that cause deep and traumatic impact in the whole society [1]–like the environment the pandemic caused.

The constant fear and dread that was brought upon during this time, evidence shows that this did not stop attackers from sinking their hook. During April 2020, Google reportedly blocked 18 million malware and phishing emails [2] as well as a significant increase in the frequency of brute-force attacks on Microsoft's Remote Desktop Protocol (RDP); both pandemic-related [3]. This reaffirms that malicious actors know no bounds; if a vulnerability exists then there also exists attackers interested in exploiting it.

Traditional enterprise networks are constructed with a perimeter-based security model, meaning there is emphasis on fortifying it's boundaries to keep intruders out of the local *trusted* network [4]. In this model, also referred to as the Implicit Trust model, the authenticated subjects are given authorized access to a variety of resources and assets provided by the network allowing for the unauthorized lateral movement around the internal network [5]. Furthermore, this perimeter defense is ineffective when it comes to detecting and blocking attacks from within the network, leaving a comfortable spot for the malicious insiders. A perimeter defense can only effectively protect subjects within these bounds–cloud and remote employees do not receive any protection [6]. Such a model is inadequate for the constantly evolving network landscape that is significantly more complicated and distributed than it was in the 1990's when it was originally designed [7]. A modern and flexible model that is scalable to technological innovations and provides protection of all assets regardless of location is now needed more than ever [8].

Unfortunately, it has taken disaster to get the world's attention and support for this change. Back in February 2013, a United States Presidential Executive Order on Cybersecurity was issued which outlined a clear and present danger form cyber attacks and made Cyber Defense a national priorities for a number of government agencies [9]. More specifically, this Executive Order included a call of action which tasked the National Institute of Standards and Technology (NIST) with creating a set of voluntary policies and guidelines to help develop the U.S. a fundamentally different approach to cybersecurity–NIST proposed the *Zero Trust Model (ZTM)* [9].

The aim of this paper is to provide organizations with the knowledge and confidence to begin the implementation of Zero Trust (ZT) concepts into their own network. This will include a simplified and amended version of the currently accepted Zero Trust migration guidelines that will provide insight for each step. The goal is to show that the Zero Trust Model is not something to be feared, but desired. The benefits and potential that ZTM offers us unlike anything before seen with the traditional architecture. As these details are described throughout this paper, it will be shown that the Zero Trust Model is to be desired.

Following the introduction, section II presents a literature review of the Zero Trust concepts, section III illustrates Zero Trust Architecture, section IV elaborates on the proposed

proposed model; section V discusses the findings of the research which is followed by conclusion and further work.

II. Literature Review

Despite how relatively new the Zero Trust Model (ZTM) is, it has seen a lot of attention in recent years due the enterprise trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary [10]; this trend saw exponential growth in the past year with due to the COVID-19 pandemic [1]. IBM claims "Zero Trust has the potential to substantially change and improve an organization's ability to protect their systems and data" [11].

This section will review some of the contributed work regarding the architecture and implementation of Zero Trust (ZT) concepts. We will begin with analyzing articles written by John Kindervag of Forrester Research–the creator of ZT.

In Kindervag's first described the Zero Trust Model (ZTM) in his 2010 paper entitled *Build Security Into Your Network's DNA: The Zero Trust Architecture*. In this paper, he says that these concepts were developed out of a necessity for an updated trust model with modern security [5]. Kindervag has completed a several more papers intended to promote and education others of this new model. One of these papers titled *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*, Kindervag uses an real life example to illustrate the issues traditional architecture problems and the ways in which the ZTM resolves them.

This story is about Phillip Cummings, a help desk employee for a company called TelData Communications, Inc. (TCI) in 1999 and 2000. At work, Cummings had access to all client passwords and subscription codes because he supported software used by the major credit bureaus [12]. Cummings was contacted and offered money by a Nigerian crime syndicate for each credit report that he gave them, and he accepted. Cummings programmed a computer to automatically send these reports to the criminals beginning in 2001, after he was no longer employed, and continued for 2 solid years. Eventually, the reports of identity theft led to an investigation which found Cummings to be guilty. However, this was after 30,000 identities and $2.7 million dollars were stolen [12].

This real world example is intended to get organizations to ask the question: *Do we have a Phillip Cummings?*. The reality is that no organization can say with full confidence that they do not have a *Cummings* working for them. This kind of trust, as well as the trust of users, devices, packets, and interfaces is the pitfall of the traditional architecture [12]. These pitfalls serve as the foundation from which Kindervag's main concepts of Zero Trust were formed [12]:

A. Ensure That All Resources Are Accessed Securely Regardless Of Location

Phillip Cummings, and the laptop he used to steal the credit reports, were automatically given privilege to sensitive data because it was part of TCI's internal network–this is an example of the trust that ZTM eliminates.

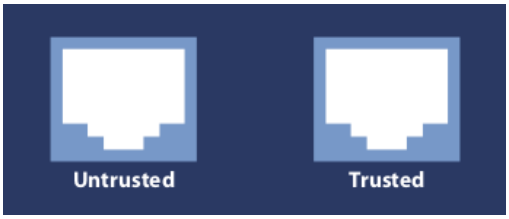

Fig. 1. The ports in TCI's network

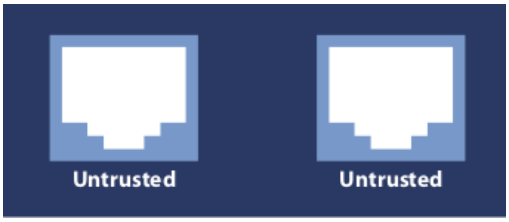

Fig. 2. Port view in Zero Trust Architecture

In the Zero Trust Model, security professionals must assume that all traffic is threat traffic until it is verified that the traffic is authorized, inspected, and secured [12]. If this was the model that was used at TCI, it is very unlikely that credit reports would be successfully sent in the first place because all users can only access the resources in a secure manner(i.e. after their identity has been verified).

B. Adopt A Least Privilege Strategy And Strictly Enforce Access Control

Cummings should only have access to the credit records when it is absolutely necessary–access controls should be always be minimum and dynamic due to the required per-transaction request [13]. The method in which identity is verified is not necessarily so long as it is strong and secure [9]. The following cases are examples of "strong and secure" user authentication.

There has been a variety user authentication and authorization methods that have been researched, some far more complicated than others. In the ZTA that Google has been experimenting with, called *Beyond Corp*, user are authenticated by using their company's credentials and the *BeyronCorp Google Chrome extension* [14].

IBM describes another method known as *Root of Trust* (RoT). The RoT method establishes cryptographic identities for RoT components (e.g. CPU, IO controllers, memory, network interface, sensor/actuator), one or more of which could contain a hardware root of trust [11].

C. Inspect And Log All Traffic

If all network traffic was visible and logged, it would have been obvious when there was data being sent to an external address by looking at the network logs–even in the traditional architecture.

Inspecting and logging all traffic is the "verify" part of the "never trust, always verify" of the philosophy of ZT because there does not exist any trust in the network as well as we must

verify the ones that we decide to trust [5]. The architecture of Zero Trust allows for the visibility that is necessary to accurately view all the traffic, but Forrester also recommends the deployment of network analysis and visibility (NAV) tools in conjunction with the system information event management (SIEM) that should already be implemented [7]. These tools help map network flow which can aid in the engineering of future more efficient zero trust architectures.

This "never trust, always verify" philosophy is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Application Layer threat prevention, and simplifying granular user-access control. [5]–thus addressing all of the issues we have seen in traditional networks.

Education and implementation of Zero Trust Architecture has received a lot of attention in light of recent events and technological innovations–33% of enterprises are targeting zero trust adoption by early 2021 however, 43% of IT security teams to lack confidence in their ability to provide zero trust architecture [4]. The proposed migration procedure found in this paper has been designed to increase both of these numbers by providing a better understanding of Zero Trust's underlying philosophy and to minimize the anxiety that the work *migrate* stirs up within management.

III. Zero Trust Architecture

Throughout this paper we have discussed the benefits of the Zero Trust Architecture, in this section we will discuss the logical components as well as define some on the imperative components. However foreign this terminology may seem, this model is actually quite simple, but it does require willingness to set aside preconceived notions about what the network should be and think about what the network could be [12].

ZTA uses an *explicit trust* model, which has been referred to as the "never trust, always verify" approach which is a layered, defense-in-depth approach, which avoids kill chains and thus prevents single points of failure from compromising the entire security defense system [15]. Unlike traditional networks, such a system is meant to be designed from the inside out [7]. We are now focused on the actual data that needs security; not securing an edge. The Zero Trust approach improves network analysis and visibility, especially when combined with exhaustive logging and analysis of management plane data. Other potential benefits include simpler, vendor agnostic architectures, better scalability, and improved application portability [15].

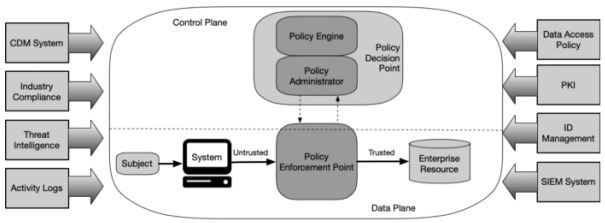

Fig. 3. Zero Trust Architecture Logical Components [6]

A. The Protect Surface

Commonly referred to as the DAAS (Data, Applications, Assets, and Services), this is where all the business critical assets are found and where access control is the strongest.

- **Data–**Customer payment card information (PCI), personally identifiable information (PPI), protected health information PHI, intellectual property (IP)
- **Applications–**out-of-box and custom software
- **Assets–**SCADA controls, point-of-sale terminals, medical equipment, manufacturing assets, and Internet of Things (IoT) devices
- **Services–**Active Directory, DNS, DHCP, FTP

B. Logical Components

These components is what enable and define the Zero Trust Architecture. There does exist variations within each technology–we will provide a summary of each.

- **Policy, or Trust Engine–**to evaluate the trustworthiness of any user, device, or application that joins the network. The arrangement of data is questioned on demand in real-time to afford situational context to make the best authorization decisions possible [15]
- **Policy enforcement point (PEP)–** enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource [6].
- **Microperimeters–**
- **Segmentation Gateways–** monitor traffic, stop threats and enforce granular access across all possible environments (on-premise, cloud, etc.)
- **MCAPs–**utilizes a new type of network called a data acquisition network (DAN) which the main function is to funnel all network data (logs and packets) to one place that can be easily monitored

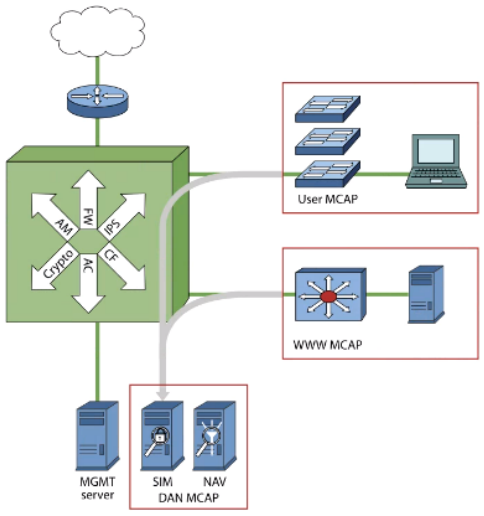

Fig. 4. Enables clear visibility of the network and easy logging

C. Zero Trust Technology

The following technologies is what makes these logical components possible.

- **Next-Generation-Firewalls (NGFWs)–**can act as the PEP, devices dynamically grant access to individual requests from a client, asset or service.
- **Software Defined Networks (SDNs)–**makes networks more flexible and easier to manage through centralized control from the data forwarding function in the discrete networking devices; making it possible for dynamic configurability, actionable threat intelligence in real-time [15]

D. Policy

- **Kipling Method–**defines Zero Trust policies based on the "who, what, when, where, why and how"
- **Compliance and Industry Policy–**ZTA have the ability to ensure the compliance of nearly all policies by only allows certain behaviors–which is most likely already present within an organization.
- **Data Access–**determines the privileges the users are granted. A crucial component in ZTA-its design is generally based off of roles and what is required for each one.

IV. Guidelines for Zero Trust Migration

The process is meant to be an iterative process which allows for the transition a full ZTA to be as slow or fast as desired. We recommend that organizations ease into this process because there will be organization-specific requirements or differences that will have to hashed out. Before jumping straight into the migration it is important to identify a general plan.

When migrating existing network assets or resource to fit this architecture, especially if this task is experimental, we recommend selecting a resource that will eventually be part of the DAAS, if possible, something that has to abide by strict policies (PCI, PHI, etc.).

The objective of the ZTA is to promote security and restrict access. As with all things unfamiliar, it will take time to adjust to the new best practices. During this time, if resources permit, develop initial builds within a secure test environment with sample data to prevent possible breaches.

Suggested ZTA Migration Procedure

Now that some of the common components and technologies have been identified, let us begin describing how to implement these using our proposed guidelines. Note, this framework is an adaption of the Palo Alto Network's *Simplify Zero Trust Implementation with A Five-Step Methodology* [5] but with more specific steps that can help organizations ease into the migration with confidence.

A. Define the protect surface

The "protect surface" refers to the DAAS (Data, Assets, Applications, Services) that we looked at in the last section. Zero Trust has been characterized as "resource protection" vs. the traditional "perimeter protection", therefore the *network* with a ZTA is the cumulation of an organization's resources–where ever they may be.

This step is likely have already been completed for most organization which have an up-to-date business continuity and disaster recovery plan because these policies require the identification of the critical business functions (CBFs) as well as their supporting technologies. If these plans do not exist, it may be in the organization best interest to develop these before introducing new technology.

B. Map the Transaction Flows

To "map the transaction flows" is essentially just identify where and how traffic is moving throughout your network. This will definitely include how all of the components within the DAAS communicate with one another and those outside of the DAAS. This is a very important step in designing an effective ZTA which is the most difficult when initially beginning this process, but becomes easier with familiarity and experience.

This is one of the aspects that will strengthen over time and with the number of iterations through this procedure. Traffic within a ZTA is inherently much more visible than it is within traditional models, therefore on the first iteration the most important thing is that you move onto the next step. There exists tools that make identify assets and network flow easier to identify, such as *Cortex XDR*, but we recommend drawing a physical diagram of your current network, including off-site resources, to see the interdependencies–dependencies show network flow.

C. Build a Zero Trust Architecture

To build a ZTA, privileges need to be granted using the principle of least privilege as noted by [13]. This principle states that only the required access should be granted, access to resources that do not pertain to a given task should never be granted. This principle supports the "never trust" aspect of ZTA because if extra privileges are granted this implies that the organization *trusts* not to abuse it with malicious intent. This would render a network something other than ZTA. From the security viewpoint, it is always preferable for employees have to ask for permission rather than beg for forgiveness later.

The success of ZTA implementation rests on the accuracy of the roles and groups that are created for the employees. These roles will determine the level of access granted to each type of position. This step, as crucial as it is, can be completed by nearly anyone–all that is required to to analyze job descriptions and make a diagram of the shared requirements of certain positions and those that are not shared. From this, someone in IT can easily determine the rights that each will require.

In this step, the authorization and authentication method should be agree upon. There are many different options here, but there already exists tools that will make this decision relatively easy. We recommend that use some variant of a NGFW because of their power to act as a PEP plus the ease of which it can be implemented. Specifically, Palo Alto's Next-Generation Firewall because has built-in identity verification

that utilize the ZT concepts. These include "User-ID", "App-ID", and "Content-ID" as filtering agents.

D. Create Policy

It is highly recommended to use the *Kipling Method* when creating ZTA policy because it enables the Application Layer security that must be present within a ZTA. This method uses the policy creation outline: "Who? What? When? Where? How? and Why?".

The more specific the rules are in the policy the more strict and secure the ZTA will be. This step, as the rest, will improve as iterations continue. These policies discussed below are arguably the most important to achieve Zero Trust.

- *Access Control Policy*–Once the roles have been define, this is where the IT department with draft the corresponding access controls.
  In the spirit of ZTA–do not trust the IT department. Verify that you can fulfill your job requirements, report when you cannot. May this begin an organization-wide collaboration where not trust is likely to lead to strengthening department bonds and an organization [16].
- *Zero Trust Policy*–this is the policy which will allow the various network resources to communicate to one another and will specify the way in which it does. However intimidating this seem, creation of this policy can be viewed as nothing other than "connecting the dots"–dots is the work completed in the previous steps.

E. Monitor and Maintenance

The use of Next-Generation firewalls make all traffic visible, enabling for the monitoring and maintenance that is required for ZTA. Next-Generation firewall illuminate network traffic through, another built-in function, enabling micro-segmentation of perimeters. This will increase the logging potential and allow for dynamic policies to be be made and distributed throughout the network. This is crucial, as well as one of the most desirable, aspects of the ZTA because it enables an organization's security to constantly improve and adapt to the ever changing workplace environment and IT landscape.

V. Discussion

We hope that these guidelines and explanation of the Zero Trust Architecture has made this technology easier to understand. Hopefully this will reach organizations and allow them to set aside their preconceived notions on networks as well as desire one that is more secure than what they are currently using. The goal of this paper is to propose framework which all kinds organizations can follow to begin seeing how the resources and data that their critical business functions require relate to this architecture. If this has been achieved, then it must be known that the first step of migration has already been completed. Confusion and the feelings of being overwhelmed are common when faced with something foreign, but this can be simplified.

Adopting this concepts must be a cooperative task where various departments are able to communicate and troubleshoot issues together [16]. But the security benefits, the cost-efficacy, and the scalability of this technology certainly outweigh the risks that are associatied with legacy networks. We urge organization to begin educating and preparing themselves so that they can avoid failure in time of crisis as so many organizations experienced during this year's pandemic.

VI. Conclusion

The Zero Trust Model (ZTM) has been said to no longer be only a theory, but it is has nearly already become the standard [17], thus knowledge of these concepts and how to begin migrating towards using them is believed to only become more necessary in the future. We hope that this paper presented Zero Trust in a clear manner that was able to be understood. Adopting a network philosophy is a difficult feat and there are expected to be growing pains throughout a migration.

This is way we have illustrated the general ZTA migration road map, and have emphasized that the length of this process shall reflect the size of the organization as well as the complexity of their private network. Hybrid architectures serve as a great initial goal, especially while employees are receiving education and the authentication method is decided upon. The Zero Trust Model (ZTM) is a solution the problems that we have faced during this time of crisis as well as those concerning modern technologies (cloud computing).

VII. Future Work

There will be much more literature and use cases in the near future due to the high demand of Zero-Trust and similar security models due to the evolving technology industry as well as the workplace environment. We hope that this paper is able to serve as a guideline to begin the necessary migration to more modern technologies so that serious breaches can be prevented if possible. In the future, we hope that we may work with some organizations that now understand the importance of maintaining up to date systems is to their success and aid in their migration. This will bring very important insight as to developing a more specific road map for a given industry as well as size of an organization.

VIII. Acknowledgment

This work was inspired and support by the works of Forrester Research and Palo Alto Networks.

References

[1] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *arXiv preprint arXiv:2006.11929*, 2020.

[2] f. Shi, "Protecting against cyber threats during covid-19 and beyond — google cloud blog."

[3] D. G. on April 29, D. Galov, and N. *, "Remote spring: the rise of rdp bruteforce attacks."

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

[5] P. Alto, "What is zero trust?."

[6] V. Stafford, "Zero trust architecture," *NIST Special Publication*, vol. 800, p. 207, 2020.

[7] J. Kindervag, "Build security into your network's dna: The zero trust network architecture," *Forrester Research Inc*, pp. 1–26, 2010.

[8] J. Flanigan, "Zero trust network model," 2018.

[9] 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)*, pp. 5–10, 2016.

[10] P. G. T. P. G. is a web editor for FedTech and h. i. a. a. a. l. o. t. N. Y. Y. StateTech. Besides keeping up with the latest in technology trends, "What is a zero-trust model in cybersecurity, and what does it mean for federal it?," Jul 2020.

[11] D. Sabella, A. Alleman, E. Liao, M. Filippou, Z. Ding, L. G. Baltar, S. Srikanteswara, K. Bhuyan, O. Oyman, G. Schatzberg, *et al.*, "Edge computing: from standard to actual infrastructure deployment and software development," *ETSI White Paper*, 2019.

[12] J. Kindervag, "No more chewy centers: Introducing the zero trust model of information security," *Forrester Research*, 2010.

[13] I. Ahmed, T. Nahar, S. S. Urmi, and K. A. Taher, "Protection of sensitive data in zero trust model," in *Proceedings of the International Conference on Computing Advancements*, ICCA 2020, (New York, NY, USA), Association for Computing Machinery, 2020.

[14] V. M. Escobedo, F. Zyzniewski, M. Saltonstall, *et al.*, "Beyondcorp: The user experience," 2017.

[15] S. Mehraj and M. T. Banday, "Establishing a zero trust strategy in cloud computing environment," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–6, 2020.

[16] B. Zimmer, "LISA: A practical zero trust architecture," in *Enigma 2018 (Enigma 2018)*, (Santa Clara, CA), USENIX Association, Jan. 2018.

[17] N. Papakonstantinou, D. L. Van Bossuyt, J. Linnosmaa, B. Hale, and B. O'Halloran, "Towards a zero trust hybrid security and safety risk analysis method," in *ASME 2020 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers Digital Collection, 2020.