Zero Trust Network Architecture

by

Priyadharsini Srinivasan
B.E., Anna University, 2020

A Project Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Computer Science

Zero Trust Network Architecture

by

Priyadharsini Srinivasan
B.E., Anna University, 2020

Supervisory Committee

Dr. Kui Wu, Supervisor
(Department of Computer Science)

Dr. Sudhakar Ganti, Departmental Member
(Department of Computer Science)

ABSTRACT

In light of the rapid advancement of digital technology and the increasing popularity of cloud-based services, it has become necessary to revisit traditional approaches to cybersecurity. Businesses are facing ever-more sophisticated cyberthreats, both from within and outside their networks, which have exposed the limitations of perimeter-based security solutions. The zero-trust architecture (ZTA) has emerged as a promising model for cybersecurity, focusing on resource security instead of network perimeter protection. This project provides a comprehensive overview of ZTA, including its fundamental principles and the Zero Trust Network Access (ZTNA) architecture.

The project focuses on an in-depth analysis of Cisco Duo's Multi-Factor Authentication (MFA) system using Wireshark to capture network traffic on a local PC. This analysis provides a comprehensive understanding of the user identity verification process using multiple authentication factors. Additionally, the project discusses the driving forces behind the adoption of ZTA, as well as the challenges and opportunities that it presents. The project explores real-world ZTA implementations, including Google's BeyondCorp and Microsoft's Zero Trust Network Architecture. The application of ZTA in various fields, including big data, cloud computing, and the Internet of Things (IoT), is also investigated.

The project concludes by discussing potential future research directions in ZTA, emphasizing the need for more complex trust algorithms, continuous verification and authentication techniques, and standardized frameworks for applying ZTA in various sectors and use cases. Overall, this project provides a comprehensive and detailed examination of the zero-trust architecture, its applications, and its potential for improving cybersecurity in an increasingly digitized world.

Contents

List of Figures

ACKNOWLEDGMENTS

I express my sincere gratitude to Dr. Kui Wu for his consistent guidance, valuable insights, and continuous support, which have been very crucial in the successful completion of this project. Additionally, I would like to express my gratitude to the University of Victoria for providing an excellent academic environment and resources that have been very useful for the significant development of this project. Furthermore, a special thanks to my friends Sai Chandra Madduri and Neha Koulecar for their unwavering encouragement and support throughout this journey of my Master's degree.

DEDICATION

I dedicate this project to my loving family, to my dad, Srinivasan, and my mom, Geetha Srinivasan, who have always believed in me, supported, and encouraged me throughout my academic journey. Their guidance and wisdom have shaped me into who I am today, and I also would like to offer my heartfelt thanks to my sister, Subiksha. I am eternally grateful for them.

Chapter One

Introduction

The frequency and severity of network-based cybersecurity attacks have increased in the past years. Over 100,000 security events per day can be experienced in a moderately-sized commercial data center [1]. These attacks may be caused by various categories of hostile actors from individual hackers to cyber-gangs. These attacks may have various objectives including compromising critical network resources such as Software Defined Controller(SDN) or a Domain Name Server [1].

With the emergence of various trends such as telecommuting and improvement in digital transformation, the digital boundaries of various businesses have disappeared. With the instant disappearance of these boundaries, traditional perimeter security solutions are no longer able to address the increased demand for remote access. The idea of zero-trust goes beyond protecting the IT perimeter, which has long dominated traditional security, and recognizes that trust is a vulnerability when it comes to security [2].

Traditional network security has emphasized the importance of perimeter defences, with users having broad access to a variety of corporate resources once inside the network perimeter. As a result of which, even malicious actors can therefore originate from both inside and outside the network. Furthermore, because there are more points of entrance, departure, and data access than ever before, the difficulty of securing an organization's digital resources has increased due to the expansion of cloud computing and the number of remote workers[3].

The idea of traditional network security has been forced to be reconsidered by various industries. A zero-trust architecture (ZTA) tackles this trend by focusing on securing resources rather than network perimeters. In this approach, the network location is no longer seen as the primary component of the resource's security posture [3].

Zero-trust is a set of cybersecurity principles that are based on the idea of "never trust, always verify." The idea is to develop a strategy that focuses on narrowing network defences from broad, static network perimeters to users, systems, and single or small groupings of resources [2][3].

The zero-trust security model does not automatically trust the users, data, devices, applications, and services within the security limit of an organization. Rather before granting access, the system must verify every individual entity that requests a connection, the verification must also be done every time the user attempts to make a connection with the system, affirming the fact that the network traffic must be considered as untrusted [4].

Zero-trust helps to safeguard cloud resources by removing unknown users and unmanaged devices, as well as limiting lateral movement. Furthermore, all components inside and outside the network must be tested and proven trustworthy before this model can be implemented[3].

1.1 Motivation

In the era of digital transformation, due to the development of IoT technologies and the proliferation of various cloud platforms, institutions have to rely upon the identities of the users. The main targets for hackers are these identifiers. Security incidents and various data breaches occur mainly due to identity theft and corruption of credentials. After the COVID-19 pandemic, and with an increase in the usage of cloud platforms, the need for efficient authentication was essential, and an on-demand least privileged access was granted in specific settings only based on adaptive and dynamic decisions.

1.2 Structure of the Report

The rest of the project report is organized as follows:

Chapter two summarizes the background and the related work, discussing the existing zero-trust architectures and real-world implementations of ZTA briefly.

Chapter three discusses the Supporting techniques, Models and the Architecture of ZTNA.

Chapter four presents the Analysis of the working of Cisco Duo Multi-factor Authentication.

Chapter five discusses the Applications of Zero-Trust in various fields like Big-Data, Cloud Computing, and the Internet of Things.

Chapter six presents examples of Real-World Zero-Trust Architecture Implementations, such as Google's BeyondCorp and Microsoft's ZTA, in detail.

Chapter seven concludes the project and talks about future research.

Chapter Two

Background and Related Work

2.1 Background

Forrester Analyst John Kindervag coined the term 'Zero Trust' and introduced the concept in the paper "No More Chewy Centers: Introducing the Zero Trust Model of Information Security" in 2010 [5].

The paper emphasized the importance of enforcing security within the network and not just on the perimeters of the network. Kindervag also suggests that the idea of soft chewy centers must be eliminated so that security is made ubiquitous throughout the network and no insider can easily manipulate the protected resources. With this, the new model called "Zero Trust" had been developed for Information Security by Forrester [5][6].

Forrester also released a series of reports describing the Concept, Architecture and Case-studies of the Zero-Trust Model. Later, Zero-Trust Extended(ZTX) Framework was developed, which included Data, Workloads and Identity as the core components of Zero-Trust [5][6].

Due to the growing number of cybersecurity threats, a United States Presidential Executive Order was issued on Cybersecurity in February 2013. The order clearly outlined the various cybersecurity threats and has made Cyber Defense a national priority for organizations such as the National Science Foundation. The National Institute of Standard and

Technology (NIST), a division of the U.S. Department of Commerce, was given the responsibility by this executive order to draught a set of voluntary policies as well as guidelines to aid in the development of the American cybersecurity framework [1].

In 2015, the NIST had drafted the first two drafts of NIST Special Publication (SP) 800-207, Zero Trust Architecture(ZTA). These publications discussed core logical components that construct a zero-trust architecture (ZTA) network strategy. The second draft publication has a new section discussing multiple zero trusts approaches and updates [2].

The foundational concepts of zero trust are:

- Zero Trust
- Trust/Risk Assessment
- Integrity Check
- Least Privilege

1. **Zero Trust**: Regardless of their location on the network, all assets of the network including devices, various computing resources, and services, are treated as untrustworthy. Therefore, all communications must meet the same security standards as the other third-party interactions [2].

2. **Trust/Risk Assessment**: Every single access request is thoroughly assessed for trust and risk. This assessment is done for the entire duration of the access and is dynamic in nature [2].

3. **Integrity Check**: All network resources and requestors have their security status monitored continually in real-time. In accordance with security policy guideline standards, an automated system evaluates the security posture of devices, users and network assets [2].

4. **Least Privilege**: Any kind of access that is given to a device/user must be with the minimum available rights. Also, access that has been granted to one resource is not

transferable to any other resource [2].

For organizations having a good IT heritage, a full conversion to a zero-trust model seems implausible because it would necessitate the reconstruction of the entire information system. Also, many organizations are considering switching to the Zero Trust Architecture model, but there are certain challenges while implementing a ZTA [3]:

- There are security issues such as the ability to recognize attacks.
- Compromise of the zero-trust control pane.

An entity may not be willing to switch to ZTA because of the following reasons [3]:

- Heavy investment in other technologies
- Inability to create a transition plan due to a lack of various resources

Commitment to Zero-trust cybersecurity requires a continuous commitment to ongoing administration. The foundation of zero-trust models is based on an extensive network of firmly defined permissions. Employees keep switching to new roles and changing locations. Therefore, to have access to specific information, access controls must be updated each time to ensure correct people have their access controls. It requires continuous effort to keep updating permissions and maintain them accurately. Not updating the access permissions then and there could lead to serious problems such as unauthorized people getting access to sensitive information [3].

2.2 Related Work

In the recent few years, with the onset of COVID-19 and the proliferating work-from-home culture, the organizations adopted a remote workforce that did not support the use of firewalls, which led to multiple unauthorized intrusions and security attacks. Users and the devices within the network are both given full access to the protected resources and are categorized as trusted users. This could result in major issues, such as the ability of any outside invader to get access to the organization's internal network and the right to change or harm the resources that are safeguarded. This calls for a perimeter-less security solution. Zero-Trust Network architecture is one such solution whose basic principle is to "Never Trust, Always Verify"[2]. Various Zero-Trust network topologies and models put forth by various researchers will be discussed in this section.

DeCusatis et al.[1] discussed a unique network architecture enabling an explicit zero-trust network. This paper has also discussed various principles of Zero trust using a transport access control system. The access control system is based on a steganographic overlay, in which explicit trust is established based on the authentication of identity tokens on the first packet of a TCP Connection. A Transport access control (TAC) gateway appliance connection is established between the user and the rest of the network. The gateway before the protected resources receives the connection request and applies the security policy based on the received identity after authentication. In the cases where the identity has not been resolved, the connection request is rejected, and no further responses are offered to the requestor, thus preventing fingerprinting of protected resources [1].

Hosney et al.[2] have introduced a conceptual model that could be used for configuration and better tuning of security policies in order to allow or block access to the assets of the network. An AI-based Zero trust Policy Engine was developed and responsible for making the decision to grant access to the resources. The policy engine is comprised of 3 main components: Static Policies, Security Feed, and ML policies. Static policies contain the

policies configured by the security admins, which in turn can be used to train the machine learning algorithm for validation of the network flows. The Policy Engine will utilize the security feeds of different sources in order to maintain the same security posture as older security controls. ML policies would treat the allow/block queries as a classification problem, and it uses the same features in the Kipling method for the validation [2].

With the increase in the usage of cloud services, and the constant risk of exposure to security threats such as data breaches, identity theft and reputation attacks, it is crucial to establish trust management within a cloud computing environment. Saima Mehraj and M. Tariq Banday[7] have proposed a conceptual zero-trust strategy for the cloud computing environment. The proposed model aids both cloud service providers and customers in choosing trustworthy entities in the cloud computing environment. The zero-trust strategy starts with the basic principle of identification of the sensitive data by the CSP and observing the flow of the sensitive data across the cloud environment. End-User Authorization and Device Authorization are performed to validate the user and device trustworthiness. Security controls such as implementing Zero-Trust micro-perimeters and multi-factor authentication (MFA) were considered [7].

Rizwana Shaikh and Dr. M. Sasikumar[8] proposed a trust model that measures the security strength and computes the trust value based on various parameters that helps in measuring the security of the cloud computing environment. Some of the parameters used were: Identity Management, Authentication, Authorization, Data Protection etc. Maliha Sulthana and the other co-authors[9] worked together to suggest a conceptual model for the secure transfer of medical information between the medical technologist and the patient based on zero-trust principles. Following three stages of security - Sender authentication, Health Parameter Check (device authentication phase), and Data Encryption with a public key-sensitive data is transferred to the recipient. Only after three layers of protection, including receiver authentication, two-factor device authentication, and data decryption using the private key, will the receiver be able to view the data [8].

A version of Zero-Trust was implemented in the BeyondCorp initiative by Google[10]. This model discards the need for a privileged corporate network. It relies on device and user authentication for granting access and establishing trust. Inventory databases are maintained for tracking and maintenance of the devices that request access to the network. Group databases are maintained for tracking and maintenance of users. Access to the enterprise resources is granted upon authentication, authorization and encryption based on the credentials of the user and the device [10].

Chapter Three

Architecture of ZTNA

3.1 Architecture of ZTNA

In a zero-trust architecture environment, irrespective of the location, there is no implicit trust placed on the subjects/entities. Authentication and authorization of the subjects are required to be proven trustworthy in a zero-trust environment. Hence the same can be enforced on every request to access a resource in the network [2][11]. In any zero-trust architecture, there are 5 significant logical components as shown in the figure 3.1 [5][12]:

- Subject
- Resource
- Policy Decision Point (PDP) [Made up of 2 components: Policy Engine (PE) and Policy Administrator (PA)]
- Policy Enforcement Point (PEP)

3.1.1 Core Components of Zero-Trust Logical Model

Subject refers to any system, user or application requesting access to a resource in the network. The resource can be classified as the network component that is requested for [5][12].

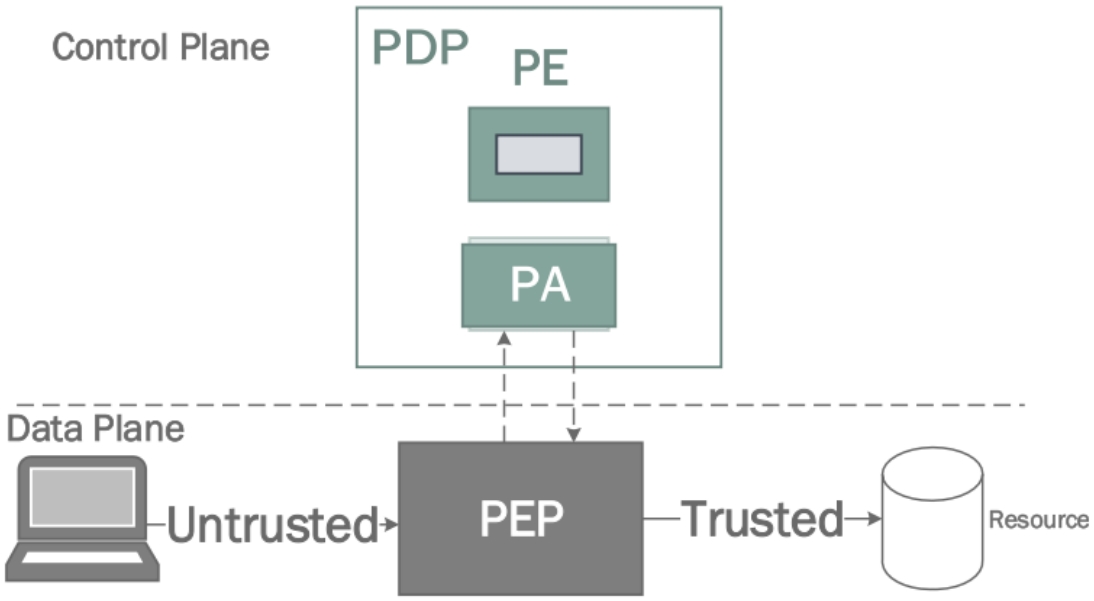

Figure 3.1 Core components of zero-trust logical model [13]

Descriptions of the components in detail:

Policy Decision Point (PDP):

Policy decision points can be further broken down into two components:

1. Policy Engine (PE)
2. Policy Administrator (PA)

Policy decision point as a whole is responsible for making decisions to grant or deny access to a resource and establishing/terminating communication with the same [5][12].

Policy Engine:

Ultimately, the Policy engine takes up the responsibility to decide if a subject will be granted access to a particular resource or not. During this decision-making process, the policy engine makes use of the various enterprise policies and input from external sources and sends it as input to a trust algorithm in order to decide if access should be granted or denied or revoked if given already. This decision is logged [5][12].

Policy administrator:

The policy administrator is responsible for establishing or terminating the communication between the subject and the resource. PA closely works with PE and allows or denies a session establishment based on the decision of the PE. Session-specific authentication tokens are generated in order to access the enterprise resource. If the session has been authenticated and the request is authorized, then PA issues a command to the PEP to let the session start or else the connection is asked to be shut down [5][12].

Policy Enforcement Point:

PEP acts as a gateway between the subject and the resources. PEP is responsible for enabling, monitoring and terminating the connection between the resource and the subject. The part of the network beyond PEP is the trust zone. There are also several other data sources that get involved in making access decisions by providing useful information such as input and policy rules to the PE. Some of these data sources include [5][12]:

- Data access policies
- Threat intelligence feeds
- Continuous diagnostic and mitigation (CDM) system
- Network and system activity logs.

3.1.2 Trust Algorithm

In a ZTA, the policy engine is the brain and the trust algorithm is the primary thought process. It is a pivotal process used by the PE in order to decide whether to grant access or not to a resource. There are several factors involved while making this decision like asset database, network traffic, access request, subject information, threat intelligence sources, security and network traffic logs etc. The above factors are fed as input to the policy engine. There are weights of importance assigned to each data source and these weights determine the significance of the data source [11][13].

3.2 Supporting Techniques

An enterprise can implement a ZTA based on several techniques. The variations in the several techniques used are based on the logical components used and the set of policy rules established. The various implementation techniques are based on [12][13]:

- Identity Governance
- Logical Micro-Segmentation
- Software-Defined Perimeter-based Segmentation

The policy rules established for the policy engine are derived from a number of data sources:

- Access Control
- Identity Management
- Network and Application logs
- Continuous Diagnostics and Mitigation
- Threat Intelligence

3.2.1 Zero-Trust Architecture Using Identity Governance

In this approach of implementing a ZTA driven by Identity, the identities of users and devices are considered primarily when creating policies for the Policy Engine. The access policies of the various resources in the enterprise are devised based on the attributes and the identity of the users/devices. Resource access is granted to the subject based on the access privileges. To a certain extent, access is also granted considering other factors such as the device used to gain access, the status of the asset/resource etc. [12][13]

3.2.2 Zero-Trust Architecture Using Micro-Segmentation

In this approach, the resources individually or collectively are placed with a network segment which is guarded by a gateway security component. The gateway security components basically guard the resources from unauthorized access and act as the PEP. The gateway devices are responsible for granting access to requests from a client/service. The gateway could be a single PEP component or a part of multiple other PEP components/devices. Next-Generation Firewalls or Routers, for instance, could potentially be used as a gateway security PEP component [12][13].

3.2.3 Zero-Trust Architecture Using Network Infrastructure and Software-Defined Perimeters

This approach involves creating a software-defined perimeter (SDP) by establishing an overlay network which controls access to the various resources. In this approach, the idea is to create a black box so that the resources are hidden from the view of the public. Connection to the requested resource is established only after the verification process. This results in dynamic network segmentation and helps enforce secure communication and access control.

In order to implement the zero-trust architecture in an efficient way, it is important to identify the relevant zero-trust tenets and understand which approaches are most suitable for the various tenets [12][13].

3.3 Models

3.3.1 Resource-Based Deployment Model

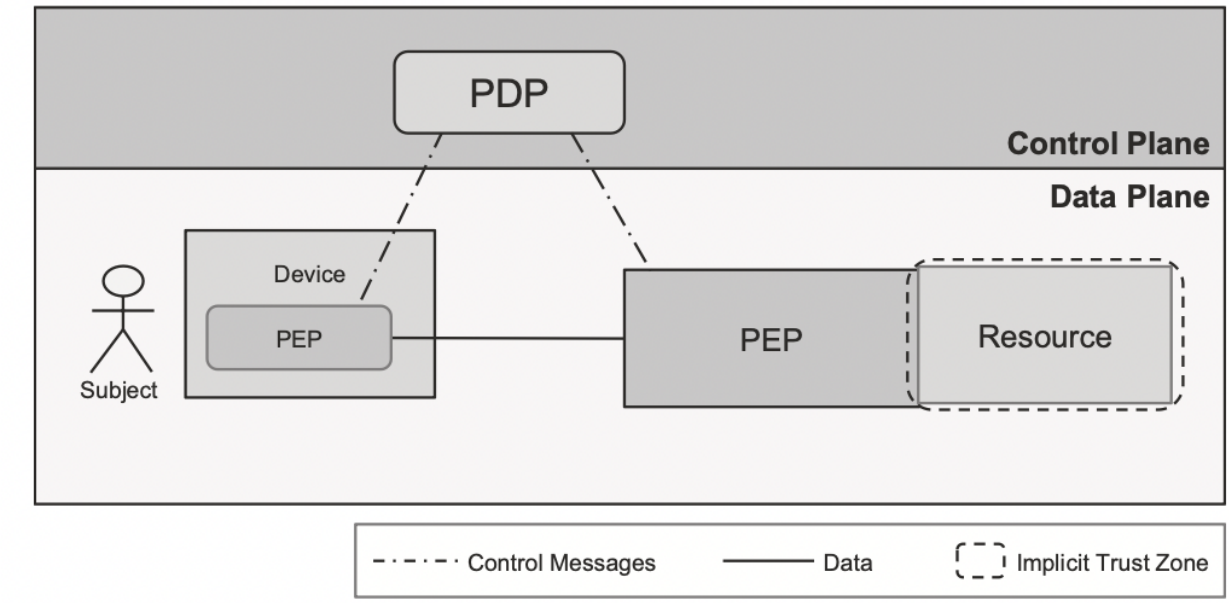

Figure 3.2 Figure depicting resource-based deployment model [5]

In this deployment model (figure 3.2), there are two PEP components involved: One is the user-agent PEP component and the other is the inline PEP component. The user-agent PEP is deployed on the subject's system itself, whereas the inline PEP is deployed on/beside the resource. In this model, the resources are present within an implicit trust zone, all the resources that are part of this trust zone are trusted to the same degree. The network communications that occur between the target resources and the user device are completely encrypted. PEP is completely responsible for enforcing the network communications with the resources in the implicit trust zone [5].

3.3.2 Enclave-Based Deployment Model

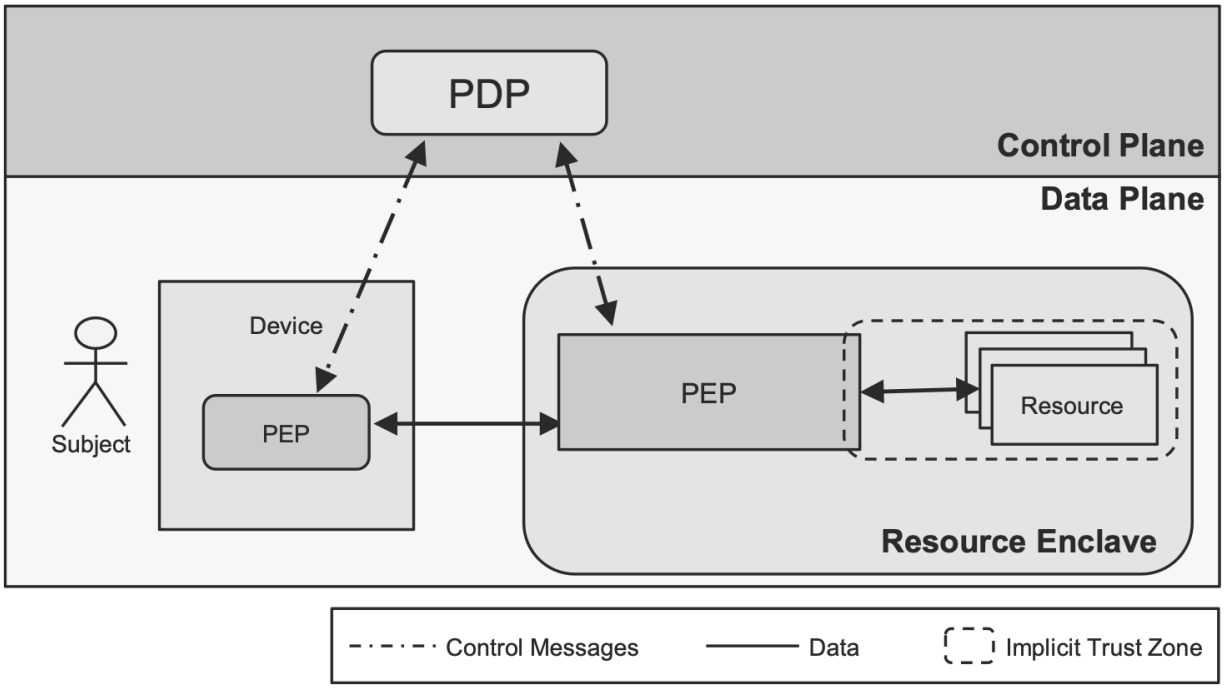

Figure 3.3 Figure depicting enclave-based deployment model [5]

This deployment model (figure 3.3) also has two PEP components, one deployed near the subject and the other deployed near the boundary of the resource enclave which is a collection of multiple resources. User-agent PEP in this model is optional. The collection of various resources in the resource enclave may be logically related or located together physically. The resources within the enclave/the implicit trust zone communicate with each other independently of the PEP whereas the communication from resources outside the trust zone is established only via the PEP [5].

3.3.3 Micro-segmentation Deployment Model

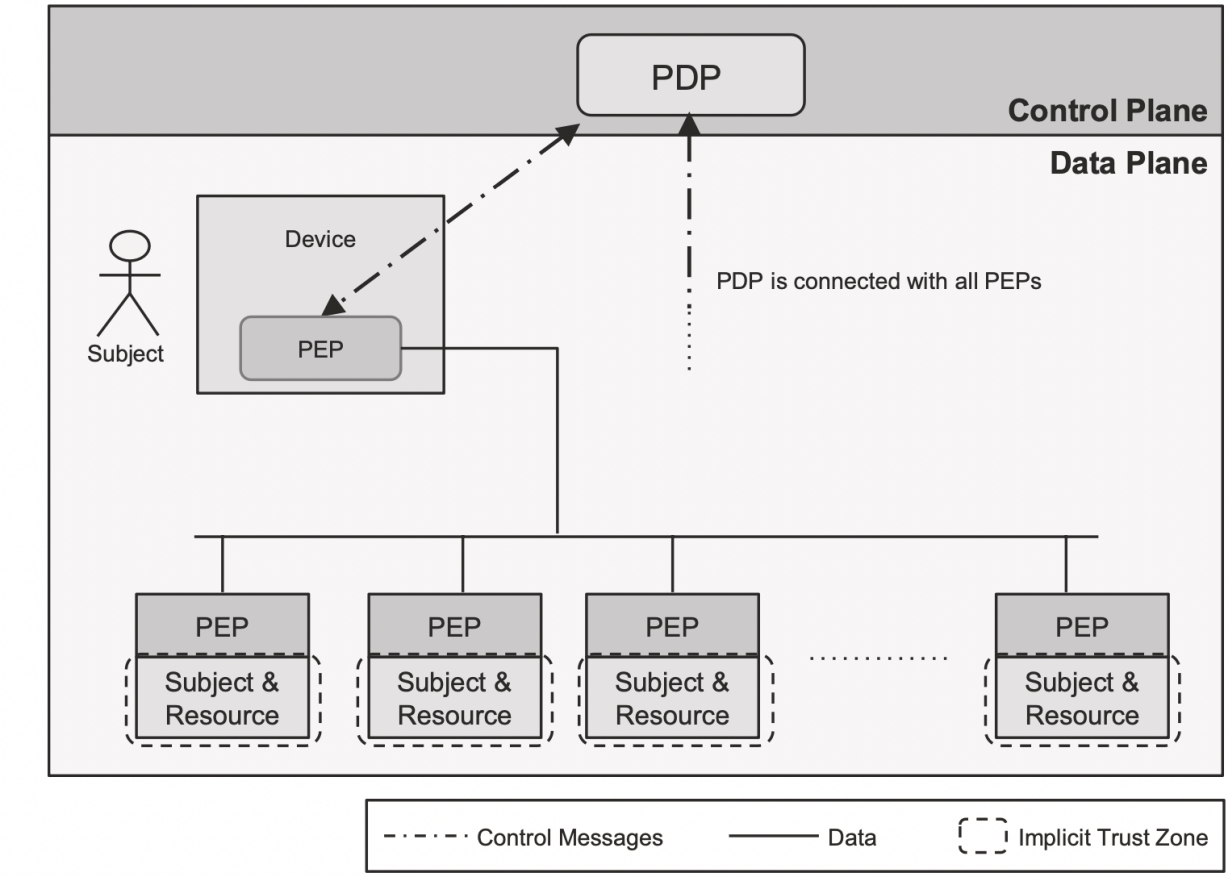

Figure 3.4 Figure depicting Micro-segmentation deployment model [5]

In this deployment model (figure 3.4), the resources are the primary subjects. Various policies are created and enforced around these resources. There is also a human subject depicted. The resources are the non-person entities/NPEs. The resources which are the primary subjects are the authenticated identities. The identities of these NPE subjects are weaker than that of the human subjects. Mostly, these NPE subjects have a single authentication factor. This model also has a small implicit trust zone which is confined to the resource. A fine-grained control of the resource access is established [5].

Chapter Four

Analysis of Cisco Duo Multi-factor Authentication

4.1 Introduction

Multi-factor authentication involves a series of steps for account login, intended to bolster access security by mandating at least two authentication factors. These factors may encompass something the user knows, such as a username and password, in addition to something they possess, such as a smartphone app that approves authentication requests. As an illustration, a user may be required to input a code sent to their email or answer a secret question in addition to their password, or even scan a fingerprint. Employing a second authentication form can serve as a preventive measure against unauthorized access in the event of a system password compromise [14].

4.2 Types

To authenticate a user's identity, there exist various options for a second authentication factor. One such option is **SMS-based two-factor authentication**, which involves sending a security code to the user's mobile device, which they then input into the website or

application they're accessing. Another form of 2FA is **TOTP (Time-based, One-Time Password)**, which generates a randomly generated code as an additional authentication token. Typically, these codes are produced via a smartphone app such as Google Authenticator, and hence, TOTP can be classified as "something you have." [15].

Push notification MFA utilizes a pop-up message on a user's smartphone, enabling them to authorize or deny access through a single button press. Additionally, push MFA notifies the user of the time and source of the access request, thereby immediately alerting them if an unauthorized party is attempting to breach their account [15].

4.3 Why is MFA important?

The foundational aspect of a zero-trust security model is multi-factor authentication (MFA), which verifies the identity of users attempting to access sensitive data. 2FA is a specific type of multi-factor authentication (MFA). MFA is an effective measure against a wide range of security threats, including phishing, brute-force attacks, and credential exploitation, among others, that target user accounts and passwords [15].

After authenticating with a username and password, it's vital to use a different out-of-band channel for the second factor to protect against remote attacks. Approving a push notification sent over your mobile network is an example of out-of-band authentication [15]. By incorporating two-factor authentication with your applications, remote attackers are unable to access your accounts without possessing the physical device that's required to complete the second factor [15].

4.4 The Experiment

In this study, network data was captured on a local PC using the popular network protocol analyzer Wireshark to examine how the Cisco-Duo multi-factor authentication system functions. To understand the inner workings of the system,analysis was done on the detailed network traffic that was collected from the capture. Examples of the captured network traffic were also included as part of the analysis such as the capture shown in figure 4.1.

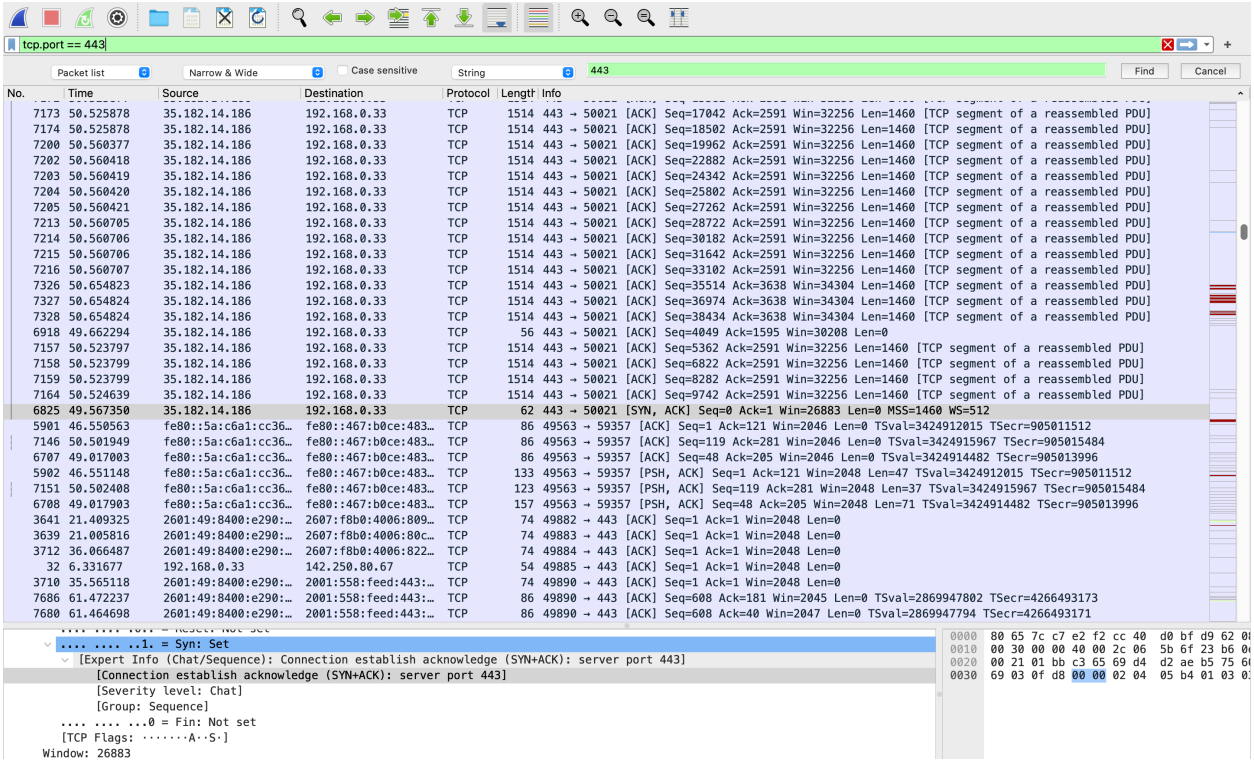

Figure 4.1 Screenshot illustrating network traffic captured using Wireshark

A flowchart (figure 4.3) and a network diagram (figure 4.2) were created to demonstrate the observed patterns of network traffic and system behaviour using the insights gained from the aforementioned investigation. The resulting visual representations help to offer an accurate and succinct overview of the underlying procedures and mechanisms at work within the Cisco-Duo multi-factor authentication system.

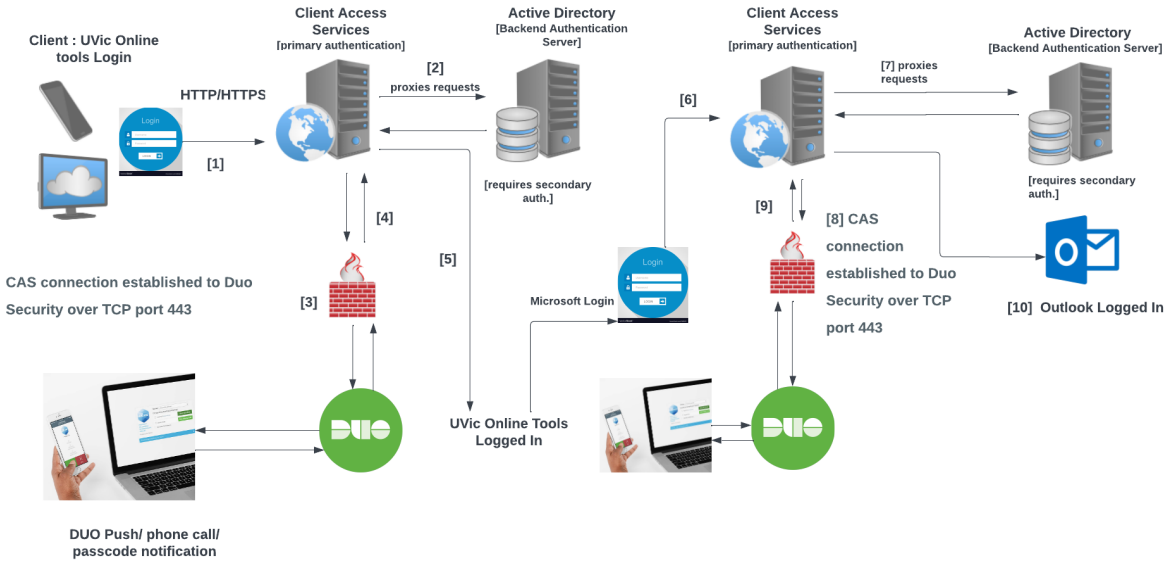

Figure 4.2 Network Diagram illustrating the working of Cisco Duo MFA

The network diagram (figure 4.2) illustrates the work behind one login session of Microsoft OWA, the connection is initiated via UVic's Online tools portal. The steps involved are diagrammatically represented one by one as follows:

1. UVic Online tools connection initiated via HTTP/HTTPS.

2. The Client Access Server receives the client connection, authenticates this connection and will proxy a request to the Mailbox Server, which has the active copy of the database that contains the user's mailbox [16].

3. Active Directory (AD) is Microsoft's implementation of a directory service, It stores information about a broad range of resources residing on a network, including users, groups, computers, printers, applications, services, and any type of user-defined objects. As such it provides a means of centrally organizing, managing, and controlling access to these resources [17].

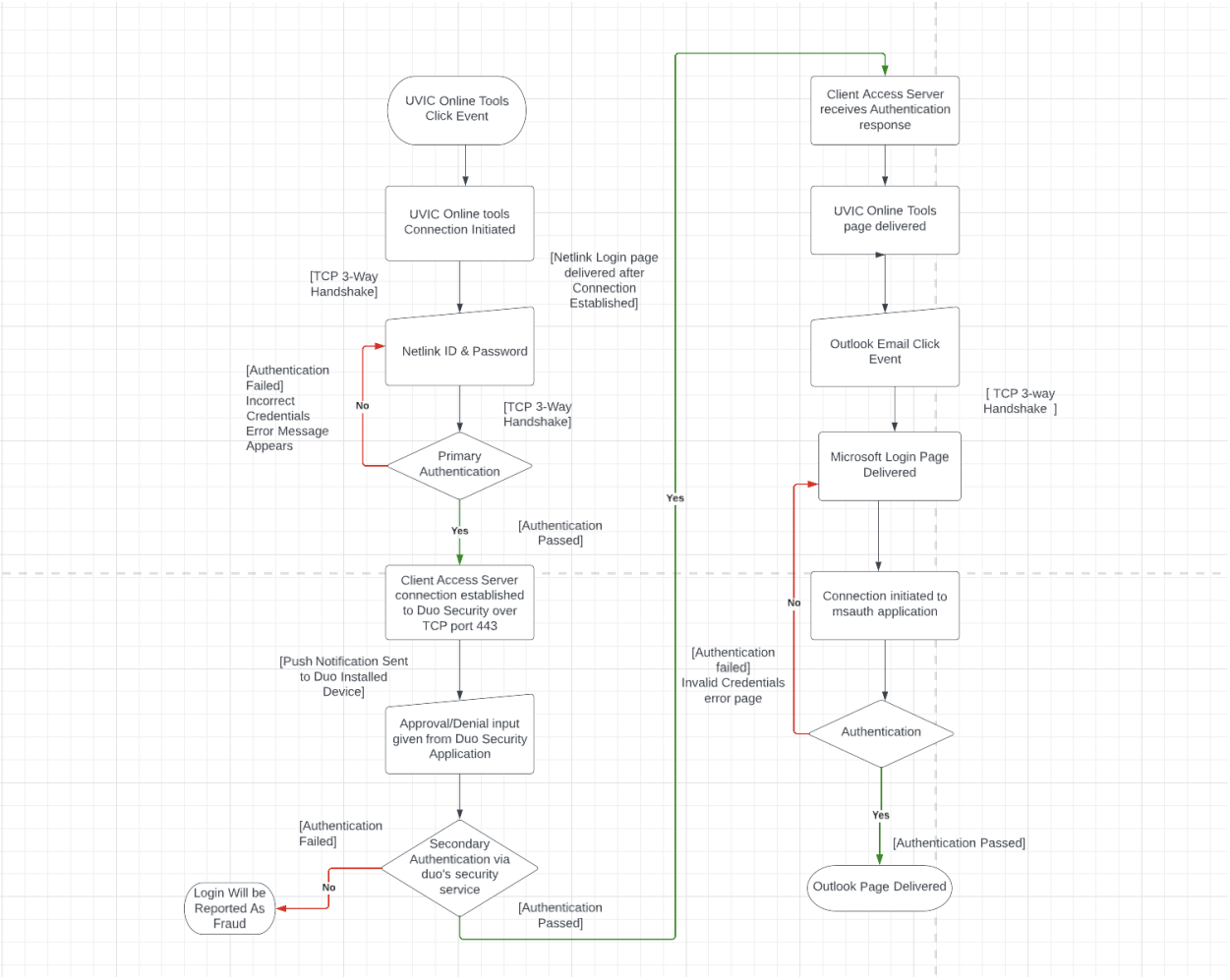

Figure 4.3 Flowchart illustrating working of Cisco Duo MFA

4. Active Directory acts as a backend authentication server and requires one more form of authentication besides verifying username and password (Primary Authentication). Secondary authentication could be anything varying from a push notification from a trusted device like a phone or a smartwatch, to biometrics like a fingerprint [18].

5. In this experiment, we use Cisco's Duo Authentication Application, to perform the secondary authentication. CAS connection is established to Duo Security Application over TCP port 443. Based on the settings configured already, a push notification or a phone call or passcode notification is sent to the Duo app, once the user approves

the notification confirming that he or she is the intended user, then authentication response is sent back to CAS and Online tools is logged in.

6. In case of denial, saying that he or she is not the intended person trying to login, the login session is cancelled, and a fraudulent report is generated and sent to the user's email ID.

7. When OWA login is initiated, Microsoft requests the login credentials, CAS authenticates the client connection, and proxies the request to AD.

8. AD requires secondary authentication and notification is sent to the Duo Security service by CAS over TCP port 443.

9. OWA is logged in once the user acknowledges the notification that he or she is the one attempting to log in. Otherwise, permission for the requested access is refused.

4.4.1 Key Packets Involved in the Cisco Duo MFA

Information about the key packets involved in the Online tools login, Microsoft account login and Duo secondary authentication processes are discussed below as part of the network analysis. The main protocols involved were: IP, UDP, TCP, DNS. TCP is responsible for establishing reliable connections between different applications running on different hosts in the network, and they provide valuable information about the flow of data between hosts, the types of applications and protocols being used. Hence, TCP packets were identified as the key packets to analyze the network connections. Network traffic received or sent by the client device is alone captured, the traffic that is passing through the intermediate devices or hops in the network are/can not be captured as part of this analysis.

UVic Online tools Login :

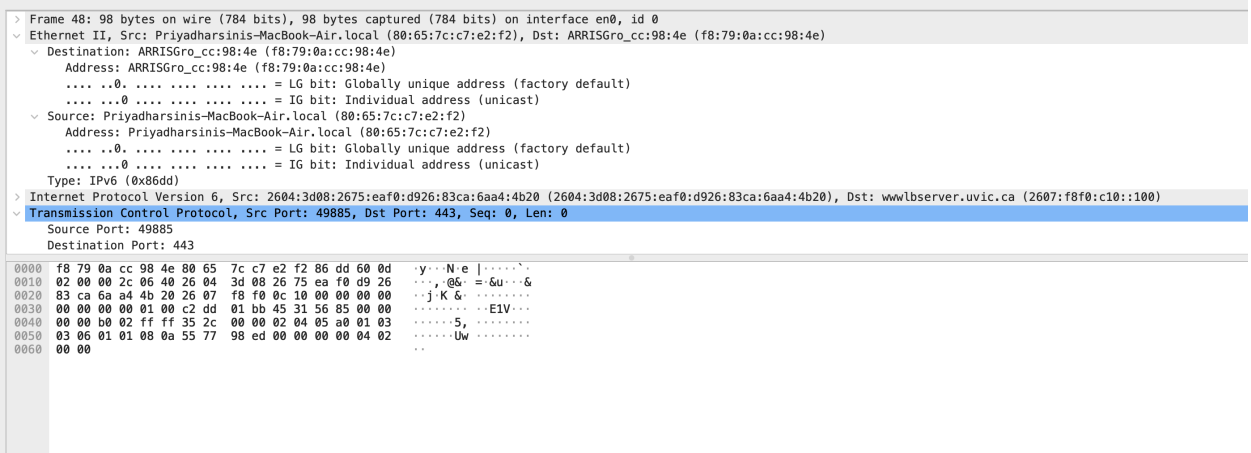

Figure 4.4 Frame 48 responsible for initiating the connection between the client browser and the UVic server

The network packet (frame 48) shown in the figure 4.4 is responsible for initiating the connection between the client and the server in the UVic Online tools login procedure.

- The client browser's IPv6 address is included as the source IP address(Src).
- The IP address of the UVic server is the destination address(Dst).
- The transport protocol involved is Transmission Control Protocol, TCP is responsible for establishing a connection between the two hosts involved.
- Since this packet is initiating the connection, it contains an SYN flag and a sequence number of 0.
- Source port 49885 and Destination port 443 indicate a communication/TCP connection between the client and the server using the HTTPS protocol.

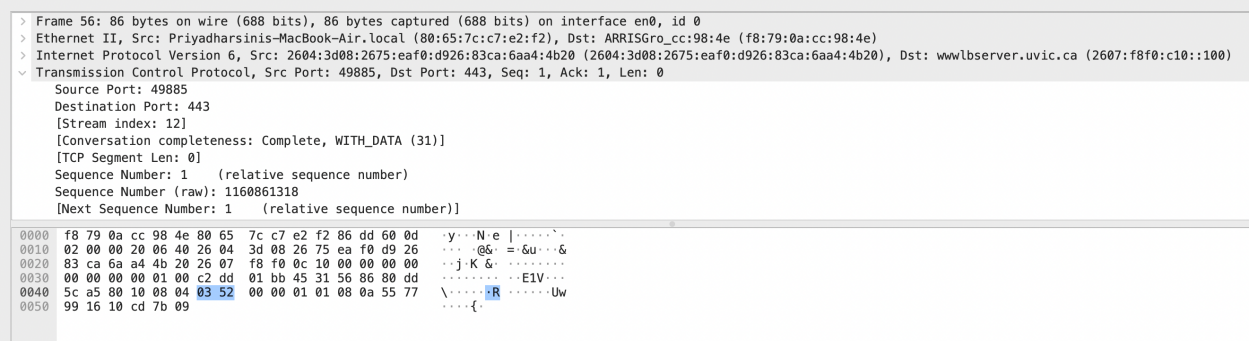

Figure 4.5 Frame 56 responsible for establishing the connection between the client browser and the UVic server

The packet (frame 56) indicated in Figure 4.5 is responsible for establishing the connection between the client browser and the UVic Server. This is an acknowledgment packet, the flag involved is ACK. Sequence number and acknowledgement number of the packet is 1. When the credentials entered by the user through the client browser are valid and authenticated successfully, the secondary authentication to the Duo Security service is initiated. If the credentials are invalid, primary authentication fails and a packet with the flag FIN is sent to terminate the connection.

Secondary Authentication Via Duo Security Service :

The network packet (frame 96) shown in Figure 4.6 is responsible for initiating the connection between the client browser and the Duo security service server. api-ce86e224.duosecurity.com is used by Duo Security as one of its authentication endpoints.

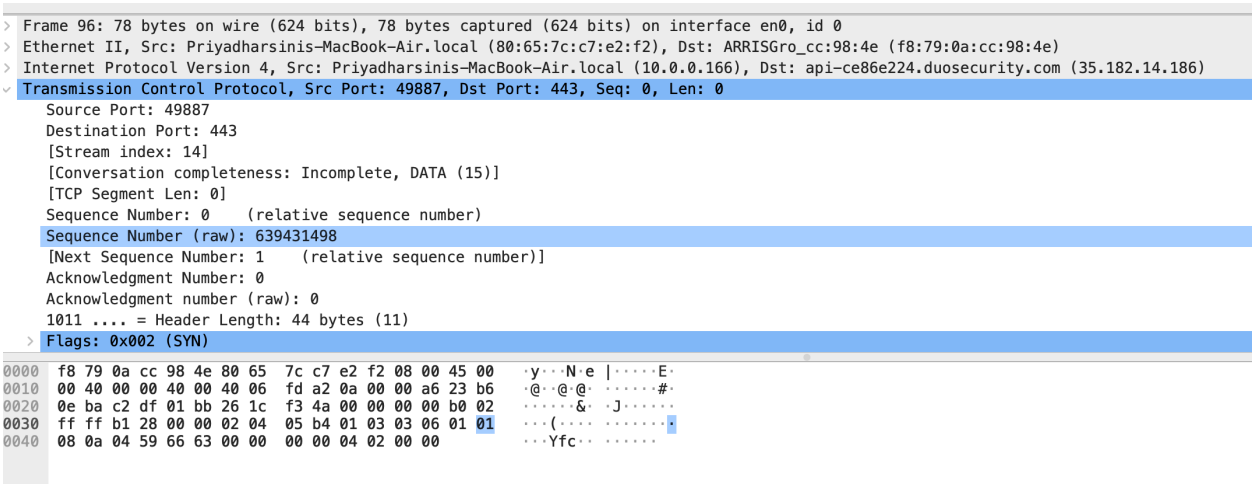

Figure 4.6 Frame 96 responsible for initiating the connection between the client browser and the Duo security service server

- The flag involved is SYN indicating that the connection is initiated.
- The client browser's IPv4 address is included as the source IP address(Src).
- The IP address of the Duo security service server is the destination address(Dst).
- Transport protocol involved is TCP.
- Source port of 49887 and a Destination port of 443 indicate communication between the client application and the server using the HTTPS protocol.

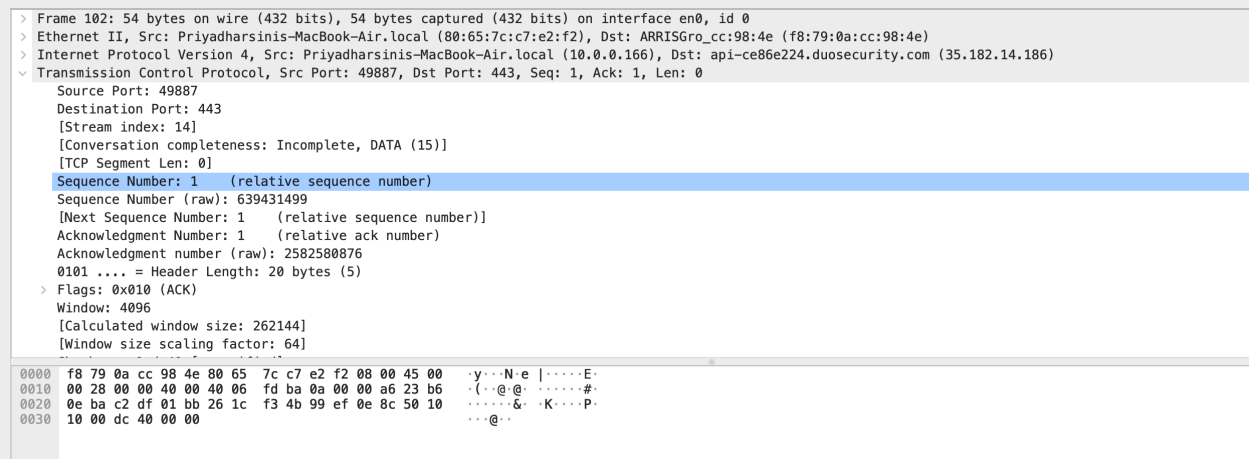

Figure 4.7 Frame 102 responsible for establishing the connection to the Duo security service server

Connection is established to the Duo over tcp port 443 as shown in the figure 4.7. It is an acknowledgement packet with an acknowledgement number of 1. This ack flag is sent by the client to the duo server to acknowledge its previous SYN-ACK packet. The sequence number and acknowledgement number of the packet is 1. When the user approves the push notification sent to the Duo application, authentication is passed and then the UVic Online tools page is delivered.

Microsoft Login :

The network packet (frame 3829) shown in Figure 4.8 is responsible for initiating the connection between the client browser and the Microsoft server. The domain name EAT-efz.ms-acdc.office.com is a subdomain of ms-acdc.office.com, that is used by Microsoft for authentication.

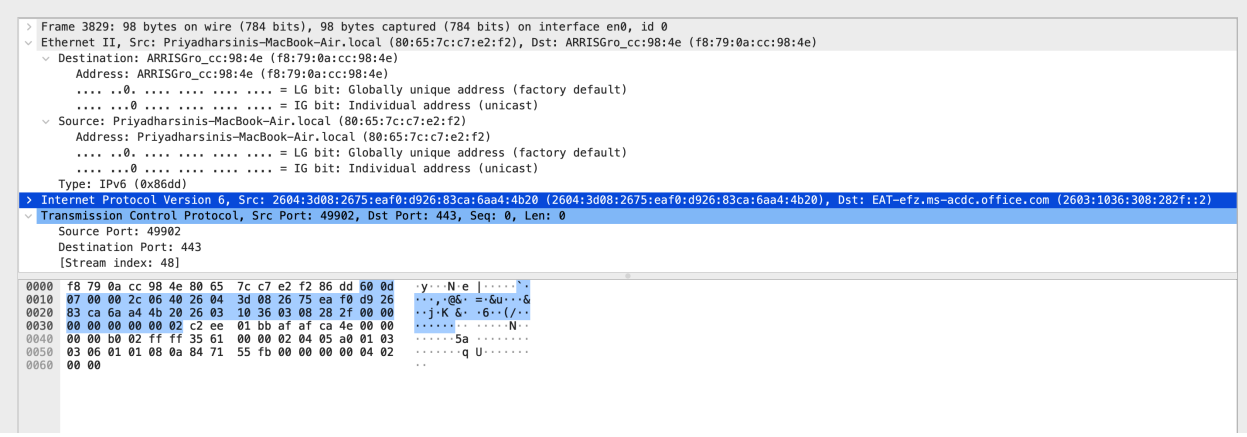

Figure 4.8 Frame 3829 responsible for initiating the connection between the client browser and the Microsoft server

- The client browser's IPv6 address is included as the source IP address(Src).
- The IP address of the Microsoft server is the destination address(Dst).
- The transport protocol involved is Transmission Control Protocol, TCP is responsible for establishing the connection between the two hosts involved.
- Since this packet is initiating the connection, it contains an SYN flag and a sequence number of 0.
- Source port of 49902 and Destination port of 443 indicate communication between the client and the server using the HTTPS protocol.

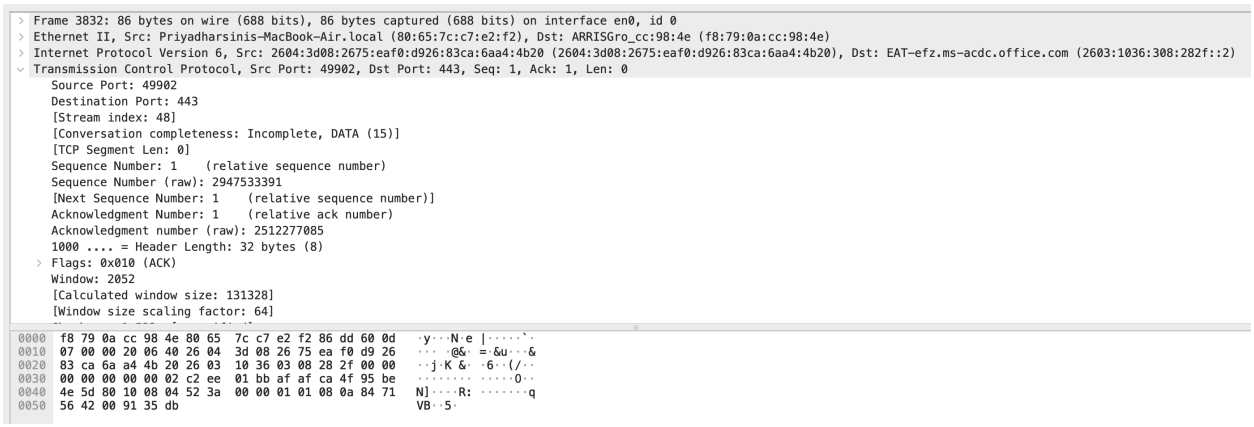

Figure 4.9 Frame 3832 responsible for establishing the connection between the client browser and the Microsoft server

The packet (frame 3832) indicated in Figure 4.9 is responsible for establishing the connection between the client browser and the Microsoft Server. This is an acknowledgment packet, the flag involved is ACK. The sequence number and acknowledgement number of the packet is 1. The credentials entered are checked with Microsoft Azure database, if the credentials are valid, primary authentication succeeds and secondary authentication is initiated via Duo security service.

Secondary Authentication Via Duo Security Service :

The network packet (frame 5745) shown in the figure 4.10 is an acknowledgement packet indicating that a connection is established between the client and the duo server. cc1.azureauth.duosecurity.com is used by Duo Security as one of its authentication endpoints to facilitate communication between the protected resource and Duo Security's service.

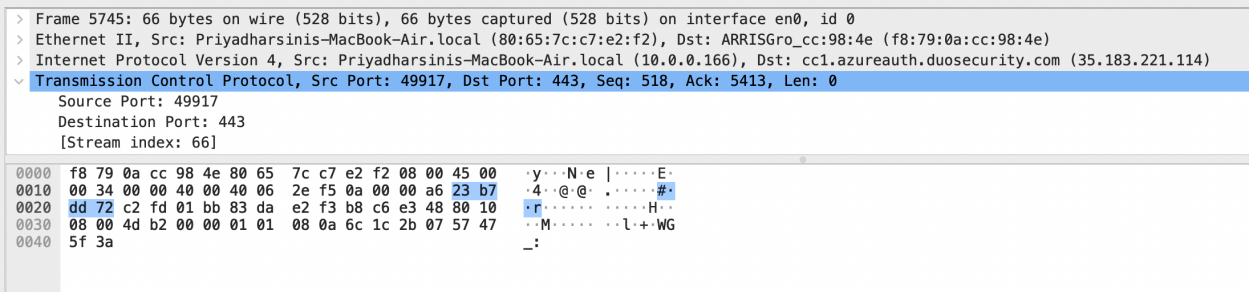

Figure 4.10 Frame 5745 responsible for establishing the connection between the client browser and the duo server

- The client browser's IPv4 address is included as the source IP address(Src).
- The IP address of the Duo security service server is the destination address(Dst).
- Transport protocol involved is TCP.
- The flag involved is ACK.
- Source port of 49917 and Destination port of 443 indicate communication between the client and the server using the HTTPS protocol.

Once the push notification in the Duo security application is approved by the user, Access to the Outlook application is granted.

Chapter Five

Applications of Zero-Trust In Various Fields

5.1 Applications of Zero-Trust in the Internet of Things

It is quite difficult to secure the applications, data, users, and devices in a complicated network as a humongous number of devices are connected to the Internet by the Internet of Things, and the number of devices connected is also tremendously increasing [19]. IoT also faces a variety of challenges, such as access to a large number of IoT devices, network performance, security, and standardization [20]. The zero-trust security, which follows the "Never Trust, Always Verify" approach, holds the principle that every attempt to the resources in IoT should be verified before granting access to the resource [19].

Adopting a zero-trust management framework for IoT could help ensure that every infrastructure resource has its credentials and configuration verified each time it wakes up to join the network. Cheating activity is thus avoided. A zero-trust management paradigm may also assist in ensuring that each message sent between resources is verified using a security technique (such as cryptography) to make sure that messages are not forged. Finally, the zero-trust management model could make sure that each transaction's nature is confirmed before it is carried out. Unusual transactions are therefore cached and deleted [21].

This subsection discusses the application of the zero-trust concept in the field of the Internet of Things (IoT) and provides examples of various research studies to support this discussion.

In the paper "Future Industry Internet of Things with Zero-trust Security" by Shan Li et al.[20], the authors suggest using a zero-trust security approach to secure IoT devices in industrial settings. The authors argue that traditional perimeter-based security models are inadequate for safeguarding IoT devices due to the dynamic and distributed nature of these devices [20].

The authors have proposed a blockchain-enabled authentication for IoT known as 'BasIoT.' BasIoT uses digital signature-based identity and authentication to secure the IoT system's devices, applications and users. Therefore, BasIoT offers a zero-trust software-defined security perimeter by implementing strong, secure authentication using a private permission blockchain. The RSA signature, therefore, allows IoT devices/users to authenticate and authorize resource access within a dynamic security perimeter in the IoT network. This way, BasIoT enables zero-trust security for users, devices, and critical infrastructure in IoT systems [20].

In the paper "Zero-Trust Hierarchical Management in IoT," Mayra Samaniego[21] suggests a zero-trust security approach for managing IoT devices. The architecture is made up of multiple levels of trust, each of which denotes a different degree of access and control over the devices. Higher levels possess greater access privileges than lower levels due to the hierarchical structure of the layers. A centralized management system that connects the multiple levels and gives the system a single point of control is part of the proposed design. The management system uses multi-factor authentication to authenticate users and devices. Also, it provides continuous monitoring and auditing of device behaviour in order to detect and respond to potential security threats. This is a fundamental principle of the zero-trust security strategy, which involves a continuous device, user, and application authentication and authorization [21].

5.2 Applications of Zero-Trust in Cloud Computing

Due to the dynamic nature of cloud-based systems, implementing the Zero Trust concept in a computing environment is of utmost importance. Because cloud-based systems have blurred the borders between internal and external networks, the old perimeter-based security models that focus on securing the network perimeter are no longer effective. Maintaining a safe perimeter has been harder as employees access company resources from different places and gadgets. The Zero Trust model offers a more flexible and dynamic approach to security, where access to resources is based on continuous verification and authentication of users and devices. Organizations can improve visibility, gain control over traffic, and lower the risk of data breaches by implementing Zero Trust [7].

Organizations can show their commitment to security and compliance by implementing a Zero Trust approach and ensuring that they are following the latest security standards. A Zero Trust strategy can also aid firms in quickly detecting and responding to security problems, which is essential for compliance with many data breach notification laws. In a cloud computing environment, implementing Zero Trust is essential for maintaining the security and integrity of corporate resources and adhering to legal and regulatory requirements [7].

This subsection discusses the application of the zero-trust concept in the field of Cloud computing and provides examples of various research studies to support this discussion. The study "ZTIMM: A Zero-Trust-Based Identity Management Model for Volunteer Cloud Computing" proposes a novel identity management model for volunteer cloud computing based on zero-trust fundamentals. The suggested model, ZTIMM, is based on zero trust principles and employs a multi-layered approach to identity management in order to provide a reliable and secure identity management solution for volunteer cloud computing settings. The authors define the model's multiple layers as follows: the identity layer, authentication layer, authorization layer, and auditing layer. [22].

In the Identity Layer, each user is assigned a unique identifier to track their activities

within the cloud environment. In the Authentication Layer, multi-factor authentication is used to verify the identity of the user. The third layer is the Authorization Layer, in which the user's access level with respect to the cloud resources based on their identity is determined. Last, the Auditing Layer records all the user activities within the cloud environment, which can be used for compliance and security purposes [22].

The ZTIMM model derives trust scores for each user based on their historical behaviour within the cloud environment in addition to the multi-layered approach to identity management. The number of successful and unsuccessful login attempts, the frequency of resource access, and the types of resources accessed are some variables used to compute the trust score. The ZTIMM model offers a more secure and reliable way of managing identities in decentralized cloud environments by combining the zero trust principles with trust scores and a multi-layered approach to identity management [22].

Another example would be the proposed autonomic security framework in the paper "Autonomic Security for Zero Trust Networks," which has been designed to incorporate the principles of Zero Trust to enhance the security of Zero Trust networks [23].

The framework uses a security policy that defines the rules and guidelines for access control and resource allocation in the network. Based on the Zero Trust concept of least privilege, this policy only permits users access to the resources they need to carry out their assigned tasks [23].

The framework's security enforcement mechanism monitors network traffic for potential threats and carries out the security policy. Before allowing access to resources, this method verifies and authenticates users and devices using the zero trust principles [23].

Finally, the framework's autonomic decision-making engine analyzes the network traffic and makes real-time judgments regarding resource allocation and access control using machine learning and other methods. By continuously authenticating individuals and devices based on their behaviour and context, this system includes the principles of Zero Trust [23].

5.3 Applications of Zero-Trust in Big Data Security

Big data security is currently the primary concern for organizations due to the big data's increasing volume, diversity, and velocity, which have resulted in severe security vulnerabilities. These risks consist of compliance violations, insider threats, unauthorized access, data loss, and data breaches. Due to the complicated and dynamic nature of big data environments, which involve distributed data storage, processing, and sharing across various systems and platforms, traditional security approaches are sometimes ineffective for big data security. Organizations must therefore implement a more proactive and diligent security strategy that can handle different challenges associated with big data security [24].

The importance of the zero-trust model for big data security is highlighted in the paper "Fine-grained Big data security method based on zero-trust model." According to the zero-trust model, access to resources should only be given to users and devices who can be identified as trustworthy and behave appropriately. To protect sensitive data and resources, the model uses various layers of security controls, such as identity and access management (IAM) and event management (SIEM), data loss prevention (DLP), and data encryption [24].

Organizations can successfully manage the security concerns associated with big data environments by implementing the zero-trust paradigm and its corresponding security measures. This approach ensures that all users and devices are authenticated and authorized before accessing resources and that all data is protected and monitored continuously. By implementing a number of security controls that verify user identity, device security posture, and user behaviour, the proposed fine-grained security solution strengthens the zero-trust model even further. Organizations can discover and respond to possible risks in real-time due to continuous monitoring and auditing of user behaviour, which lowers the risk of data breaches and compliance violations. As a result, the fine-grained security mechanism and the zero-trust paradigm are crucial for protecting big data environments and making sure

the confidentiality and integrity of sensitive data and resources are not compromised [24].

In the proposed security solution, the IAM layer manages user identities and access rights, making sure that users are authenticated and given permission before they may access resources. The SIEM layer keeps track of user activity and looks for any security risks, sending out instant notifications and prompting responses. While the data encryption layer protects data in transit and at rest, the DLP layer stops data leakage and protects sensitive data against unauthorized access. This security solution emphasizes the value of continuous user identification and behaviour monitoring and verification in order to identify and address potential threats quickly. It can successfully protect sensitive data and resources in big data environments by adopting the zero-trust model [24].

Chapter Six

Real World Zero-Trust Architecture Implementations

This chapter gives a detailed description of the real-world implementations of zero-trust architecture. The two examples discussed are (1) BeyondCorp by Google and (2) Microsoft's Zero-trust Model.

6.1 BeyondCorp by Google

One of the first implementations of a zero-trust architecture was Google's BeyondCorp project. Figure 6.1 describes the overview of the BeyondCorp model, comprising the various components and its access flow. It gets rid of the privileged corporate network and establishes trust by verifying device and user credentials, allowing fine-grained access to network resources. It also eliminates the requirement for a VPN to access the privileged network. Remote workers benefit from a better user experience as a result of this [10].

BeyondCorp makes use of device and user authentication to establish trust. Google manages the device identification component by keeping track of managed devices in an inventory database. Digital certificates and encryption keys are used to secure and identify these devices. Google tracks and manages people using a User and a Group database [10].

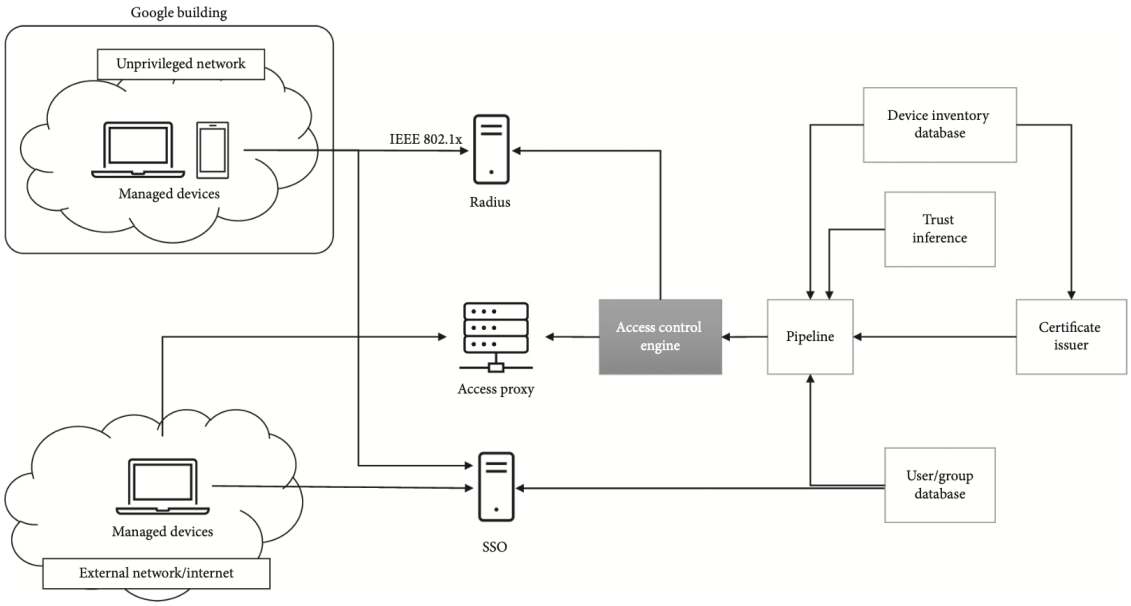

Figure 6.1 An Overview of BeyondCorp's components and its access flow [11]

To have a better insight into all the devices used in the network, all the devices the user typically uses are kept in a device inventory database in this model. It is crucial to collect all of this information about devices and users to understand what applications are used internally and what security policies have to be applied in each application. It is significant to understand the roles and responsibilities of the position and determine who has access to particular services to have effective control [25].

Based on device state and user credentials, all access to enterprise resources is thoroughly authenticated, fully authorized, and fully encrypted [25].

To implement this model, Google uses a combination of device management, multifactor authentication, network segmentation, and access control. Multifactor authentication (MFA) is necessary to identify users, and controlled devices may perform MFA using an SSO platform or through RADIUS using the 802.1x protocol [11].

Another significant component of BeyondCorp is Network segmentation, which requires transferring managed devices to a non-privileged network in order to remove implicit trust

from the old network of BeyondCorp. Unrecognized and unmanaged devices are automatically assigned to a guest or quarantine network for further remediation, whereas authorized devices are assigned to an independent virtual network using VLAN. Google additionally set up an access proxy that can be accessed from the internet, where all requests from both public and private networks are directed [11].

As part of its transition to a zero-trust architecture (ZTA), Google is additionally requesting verification and authorization for all access requests, irrespective of the user's location, network, or the type of device. In order to implement ZTA, Google first selects candidate workflows , moving from low-risk to more crucial workflows once they feel confident enough in the transfer process. The ZTA framework focuses on implementing ongoing verification, monitoring, and authentication, can aid in preventing data breaches and cyberattacks [11].

6.2 Microsoft's Zero-trust Model

Microsoft is implementing Zero Trust by taking a structured approach across many technologies and organizations. They have defined four pillars of Zero Trust implementation: Verify identity, Verify device, Verify access, and Verify services as shown in figure 6.2 [26].

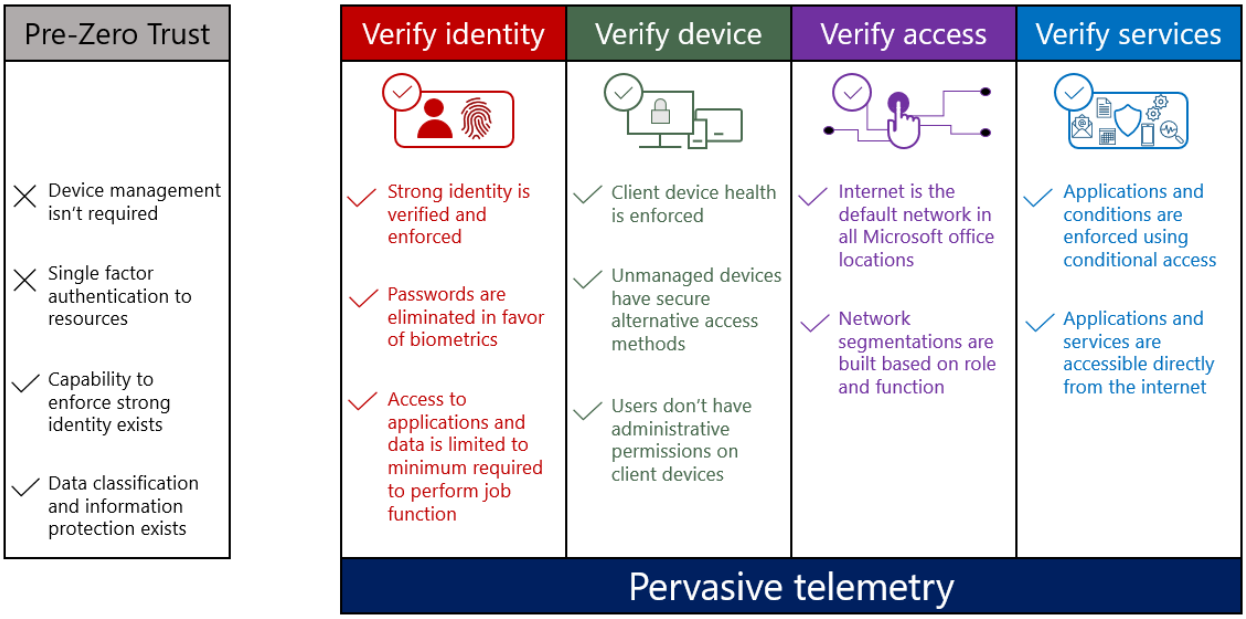

Figure 6.2 Figure depicting Microsoft's major goals for each Zero-trust pillar [26][27]

Microsoft has implemented multi-factor authentication (MFA) using smart cards, phone-based challenges, and the Microsoft Azure Authenticator application in the Verify identity pillar. The latest progress in this area is the widespread deployment of Windows Hello for Business for bio-metric authentication [26].

In the Verify device pillar, Microsoft has enrolled devices into a device-management system, set and enforced health policies for accessing Microsoft resources, and used Windows Autopilot for device provisioning. Microsoft has created a secure access model for personal devices called Microsoft Azure Virtual Desktop [26].

In the Verify access pillar, Microsoft has segmented users and devices across purpose-

built networks, migrated all Microsoft employees to use the internet as the default network, and created a device-registration portal [26].

In the Verify services pillar, Microsoft has enabled conditional access across all applications and services, modernized legacy applications, and implemented solutions for applications and services that cannot natively support conditional access systems [26].

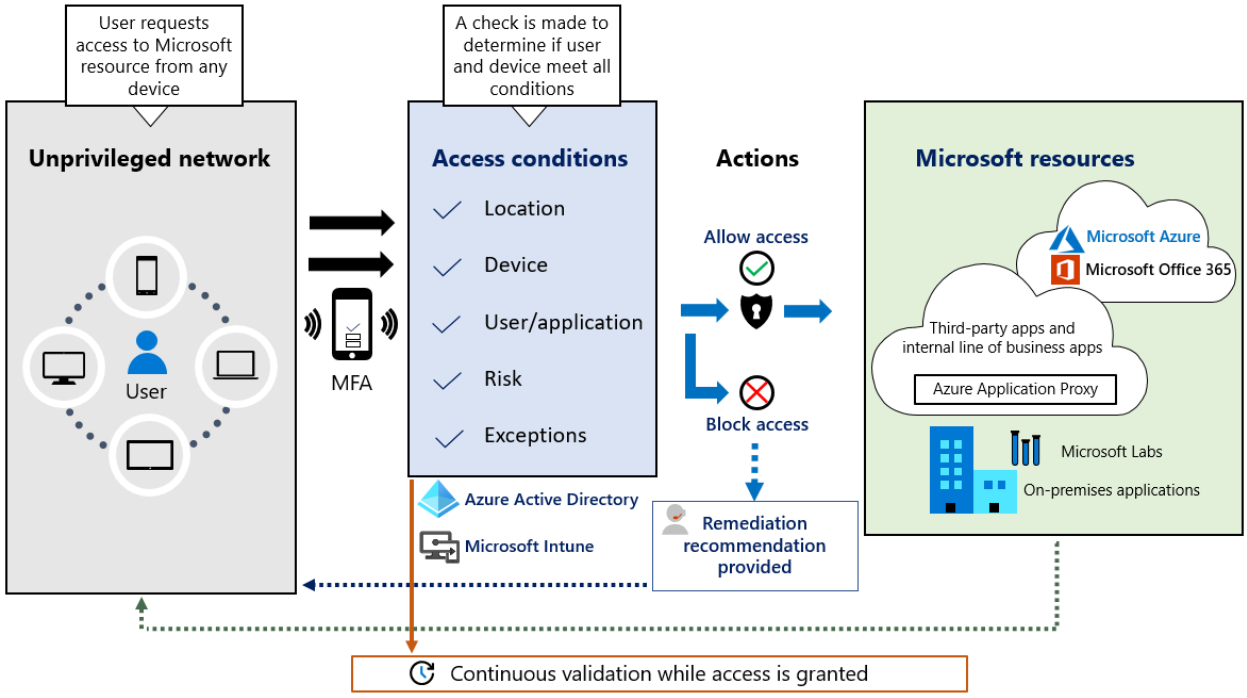

Figure 6.3 Figure depicting Microsoft's Zero-trust Architecture [26][27]

Figure 6.3 depicts Microsoft's Zero-trust Architecture. Microsoft's approach to Zero Trust involves various Microsoft services such as Intune for device management and security policy configuration, Microsoft Azure Active Directory (Azure AD) conditional access for device health validation, and Azure AD for user and device inventory. The implementation of Zero Trust requires ongoing effort and investment to maintain the highest level of security, and Microsoft is continually evaluating their goals and adjusting them as necessary [26][27].

Chapter Seven

Future Research and Conclusion

This study has investigated the zero-trust architecture (ZTA) as a cybersecurity approach that addresses the limitations of traditional perimeter-based security solutions. The ZTA follows the principle of "never trust, always verify" and emphasizes the importance of continuous verification and authentication of users and devices before granting access to resources.

The study examined the background and related work on ZTA, the supporting techniques, models, and architecture of Zero Trust Network Access (ZTNA), and the applications of zero-trust in various fields, such as IoT, cloud computing, and big data. Real-world implementations of ZTA, including Google's BeyondCorp and Microsoft's Zero Trust Network, were also analyzed.

Zero Trust Network Access (ZTNA) relies mainly on multi-factor authentication (MFA), which provides an additional layer of security to the authentication process and this makes it more difficult for unauthorized users to access sensitive resources. This study involves an analysis of Cisco Duo's Multi-Factor Authentication (MFA), an important security measure that uses at least two authentication factors to verify user identity. The study involves capturing network data on a local PC using Wireshark and analyzing the Cisco-Duo MFA system's inner workings. Flowcharts and network diagrams are created to demonstrate the observed patterns of network traffic and system behaviour. The details of the key packets involved in the UVic Online tools login, Microsoft account login, and Duo secondary au-

thentication processes are also discussed. Through a detailed analysis of the network traffic, valuable insights into the Cisco Duo MFA system's mechanisms and procedures are gathered, helping to better understand its role in strengthening security.

In conclusion, ZTA provides a more adaptable and secure method of cybersecurity that is suitable for the age of digital transformation. The popularity of ZTA is anticipated to increase, offering improved security for digital resources, as businesses continue to adopt new technologies and migrate to cloud-based settings.

Future research will concentrate on creating more complex trust algorithms and methods for continuous verification and authentication in ZTA, as well as improving the way ZTA is applied in certain industries and use cases. Further research on ZTA's scalability in large-scale networks, its integration with cutting-edge technologies like blockchain and artificial intelligence, and the creation of standardized frameworks and implementation guides for Zero-Trust architecture might all make significant contributions to cybersecurity.

REFERENCES

[1] Casimer DeCusatis et al. "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication". In: *IEEE Conference on Smart Cloud* (2016).

[2] Hosney et al. "An Artificial Intelligence Approach for Deploying Zero Trust Architecture (ZTA)". In: *International Conference on Computing and Informatics (ICCI)* (2022).

[3] Alper Kerman et al. "Implementing a zero trust architecture". In: *National Institute of Standards and Technology (NIST)* (2020).

[4] Christoph Buck et al. "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust". In: *Elsevier* (2021).

[5] Jason Garbis. *Zero trust security : an enterprise guide*. eng. Apress, 2021. ISBN: 1-4842-6702-8.

[6] John Kindervag, S Balaouras, et al. "No more chewy centers: Introducing the zero trust model of information security". In: *Forrester Research* 3 (2010).

[7] M. Tariq Banday Saima Mehraj. "Establishing a Zero Trust Strategy in Cloud Computing Environment". In: *International Conference on Computer Communication and Informatics (ICCCI -2020)* (2020).

[8] Rizwana Shaikh and Dr. M. Sasikumar. "Trust Model for Measuring Security Strength of Cloud Computing Service". In: *International Conference on Advanced Computing Technologies and Applications (ICACTA- 2015)* (2015).

[9] Maliha Sultana. "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology". In: *BMC Medical Informatics and Decision Making* (2020).

[10] John Flanigan. "Zero Trust Network Model". In: (2018).

[11] Songpon Teerakanok et al. "Migrating to Zero Trust Architecture: Reviews and Challenges". In: *Security and Communication Networks* 2021 (2021).

[12] Scott Rose et al. *Zero Trust Architecture*. en. 2020-08-10 04:08:00 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420.

[13] Naeem Firdous Syed et al. "Zero Trust Architecture (ZTA): A Comprehensive Survey". eng. In: *IEEE access* 10 (2022), pp. 57143–57179. ISSN: 2169-3536.

[14] aws.amazon.com. "What Is Multi-Factor Authentication (MFA)?" In: (2023). URL: https://aws.amazon.com/what-is/mfa/.

[15] Duo. "Two-Factor Authentication(2FA)". In: (2023). URL: https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa.

[16] Microsoft.com. "Client Access server". In: (2023). URL: https://learn.microsoft.com/en-us/exchange/client-access-server-exchange-2013-help.

[17] Sophos Limited. "Active Directory". In: (2021). URL: https://docs.sophos.com/nsg/sophos-utm/utm-on-aws/9.707/help/en-us/Content/utm/utmAdminGuide/AuthServicesServersActiveDirectory.htm.

[18] Microsoft. "What is Azure Active Directory authentication?" In: (2023). URL: https://learn.microsoft.com/en-us/azure/active-directory/authentication/overview-authentication#azure-ad-multi-factor-authentication.

[19] Shancang Li et al. "Editorial: Zero Trust based Internet of Things". In: *EAI Endorsed Transactions on Internet of Things* 5.20 (2019).

[20] Shan Li et al. "Future Industry Internet of Things with Zero-trust Security". In: *Springer* (2022).

[21] Ralph Deters Mayra Samaniego. "Zero-Trust Hierarchical Management in IoT". In: *IEEE International Congress on Internet of Things* (2018).

[22] Abdullah Albuali et al. "ZTIMM: A Zero-Trust-Based Identity Management Model for Volunteer Cloud Computing". In: *Springer* (2020).

[23] Dayna Eidle et al. "Autonomic Security for Zero Trust Networks". In: *IEEE* (2020).

[24] Yang Tao et al. "Fine-Grained Big Data Security Method Based on Zero Trust Model". In: *IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)* (2018).

[25] Carla Cordeiro and Hugo Barbosa. "Proceedings of the Digital Privacy and Security Conference 2019". In: (2019).

[26] Inside Track staff. *Implementing a Zero Trust security model at Microsoft - Inside Track Blog — microsoft.com*. https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/. []

[27] Aniket Deshpande. "A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic". In: *New Visions in Science and Technology* vol. 1 (2021).