Fall 2022

Zero Trust Architecture

Ahmed Abdullah Syed

ZERO TRUST ARCHITECTURE

By

SYED AHMED ABDULLAH

B.E., Osmania University, 2019

THESIS

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science,

With a Major in Information Technology

Governors State University

University Park, IL 60484

2022

Table of Contents

1. Introduction......1

2. Existing Security Model 2

3. Introduction to Zero Trust......4

3.1 Adopting a Zero Trust mindset......4

3.2 Zero Trust Guiding Principles 5

4. Defining Zero Trust with Government Frameworks 5

5. Pillars of Zero Trust Architecture......6

6. Working of Zero Trust Architecture 7

6.1. Network Controllers 7

6.2. Working of Gateways 9

6.3.Working of Zero Trust Architecture 14

7. Implementing Zero Trust Architecture 15

8. Challenges of a Zero-Trust Security Model 16

9. How to overcome Zero-Trust Challenges 17

10. Literature Review 17

11. Future Research Agenda......18

12. Conclusion 19

13. References......20

Abstract

Cyber threats are becoming increasingly sophisticated, and IT organizations need to continue to modernize their approaches to cybersecurity in light of today's dynamic cyber threat environment. Cybersecurity professionals must adopt a zero-trust security model and the mindset needed to engineer and operate a system specifically designed to operate according to zero trust principles in order to ensure the security of sensitive data, systems, and services as enterprise networks become increasingly dispersed and complex.

Keywords: ZTA, Zero Trust Architecture, Zero Trust Model, cybersecurity.

1. Introduction

Cyber threats are becoming increasingly sophisticated, and IT organizations need to continue to modernize their approaches to cybersecurity in light of today's dynamic cyber threat environment. Cybersecurity professionals must adopt a zero-trust security model and the mindset needed to engineer and operate a system specifically designed to operate according to zero trust principles in order to ensure the security of sensitive data, systems, and services as enterprise networks become increasingly dispersed and complex.

Using Zero Trust, you will develop a coordinated cybersecurity and system management strategy that acknowledges that threats exist both inside and outside of traditional network boundaries. During the implementation of Zero Trust principles and concepts, it is extremely crucial that they permeate the entire network and operations ecosystem to hinder risks and facilitate more robust and timely responses.

Assuming that a breach will happen in the future or that one has already occurred, Zero Trust security assumes that access will be restricted to only what is necessary and that malicious or suspicious activity will be constantly monitored. Zero Trust integrates granular risk-based access controls, comprehensive security monitoring, and system security automation into one platform to protect critical assets (data). An access decision based on contextual factors is made based on the least-privileged access principle in this data centric model.

By using zero-trust principles, systems can be designed to address existing threats more effectively. However, the transition to such a system needs to be carefully planned to prevent security postures from deteriorating. It is imperative that all levels of an organization adopt zero trust as their mindset if they are to achieve Zero Trust model. Zero Trust principles and concepts must be incorporated into the entire operating ecosystem and network to reduce risks and enable more robust and timely responses.

2. Existing Security Model

Due to today's connectedness, diversity of users, wealth of devices, and global distribution of applications and services, we are living in a highly vulnerable environment as a result of our connected world. With the rapid evolution of cyber threats, traditional network security defenses have become ineffective as cloud, multi-cloud, and hybrid network environments become more complex. A number of traditional perimeter-based network defenses with multiple layers of disjointed security technologies fail to meet today's cybersecurity challenges, as the current threat landscape demonstrates and as cybercriminals and nation-state actors have developed more stealthy, persistent, and subtle methods of attacking networks as they routinely breach perimeter defenses. In order to achieve unified and granular access control over data, services, applications, and infrastructure for organizations, there needs to be a better solution to defend dispersed enterprise networks against increasingly sophisticated cyber threats.

Traditional Network security leads to:

- Weak Cloud Infrastructure
- Obsolete Security
- Inconsistent Testing, Monitoring and Analysis
- Security Non-Compliance

Top five Data Breaches in 2022:

These are some of the events that Dr. Sveinsson, R. L. included in his research on top 10 data breaches of (2022).

1. Crypto.com Crypto Theft:

   Nearly 500 cryptocurrency wallets were targeted on January 17th 2022, and approximately $18 million worth of Bitcoin and $15 million worth of Ethereum were stolen along with other crypto currencies. Hackers were able to gain access to users' wallets by bypassing two-factor authentication.

2. Microsoft Data Breach:

A hacking group called Lapsus$ attacked Microsoft on March 20th, 2022 and posted a screenshot on Telegram indicating they had hacked Microsoft, compromising Cortana, Bing, and several other services and products. On March 22nd, Microsoft announced that it had quickly stopped the hacking attempt and only one account had been compromised during the hacking attempt.

3. Ronin Crypto Theft:

Between November 2021 to March 2022, the blockchain gaming platform that relies on cryptocurrency was targeted. The Axie Infinity game of Ronin offers players a chance to earn digital currency as well as non-fungible tokens (NFTs), a financial security based on digital data stored in blockchain technology. The company dialed back security protocols as the game's popularity grew, allowing more players in, as well as criminals who stole $625 million in cryptocurrency.

4. Red Cross Data Breach:

More than 500,000 people receiving services from the Red Cross and Red Crescent Movement were the victims of a hacker attack in January 2022.Data from the hacked servers was related to Restoring Family Links services, which help reunite people separated by war, migration, and violence.

5. News Corp Server Breach:

News Corp acknowledged server intrusions as far back as February 2020 in February 2022. Asserting that no customer data was stolen and that the company's everyday operations were not hindered, News Corp discovered that its journalists' emails were stolen.

Network defenders should implement a modern cybersecurity strategy that integrates visibility from multiple angles, makes access decisions based on risk, and automates detection and response actions in order to better secure sensitive data, systems, apps, and services in the network. As a result, zero trust is a "suspected breach" security model that is intended to serve as a guide for cybersecurity architects, integrators, and implementers in their attempt to integrate.

Since it does not constitute a tactical mitigation response to new adversary tools, tactics, or techniques, re-engineering an existing information system to adopt a Zero-Trust security model will require considerable planning and effort before its benefits can be realized. It is evident from these recent high-profile breaches and their implications that tactical responses are often insufficient to deal with recent breaches and their implications due to widespread weaknesses in systems and deficiencies in system management and defense network operations. Cybersecurity defenders can expect to see more and more opportunities to detect and respond to sophisticated threats as Zero Trust environments mature.

3. Introduction to Zero Trust

Zero Trust is a set of security principles, a framework for designing systems, and a coordinated approach to cybersecurity and system management that acknowledges that threats exist within and outside traditional network boundaries. In a dynamic threat environment, Zero Trust implements granular, dynamic access controls, comprehensive security monitoring, and automated system security to protect critical assets (data) in real time. As the title indicates, Zero Trust questions implicit trust between users, devices, and network components based on their location within a network. In a data centric security model, least privilege access can be applied to every access decision based on answers to the questions of who, what, when, where, and how. Microsoft states that “Zero Trust is a proactive, integrated approach to security that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats, across all layers of the digital estate. ” (2021).

3.1. Adopting a Zero Trust mindset

Effectively addressing the dynamic threat environment of the current day requires that we:

- Assuming that all network traffic and requests for critical resources are malicious.
- Considering that all devices and infrastructure may be compromised.

- Being prepared to assess, control, and recover quickly after approving access to critical resources
- Manage systems aggressively while also engaging in defensive activities.

3.2. Zero Trust Guiding Principles

Microsoft defines three major guiding principles of Zero Trust Model (2022).

Never Trust, Always Verify:

Authenticate and explicitly authorize every user, device, application/workload, and data flow to the least privilege required by using dynamic security policies and treating each as un-trusted.

Assume breach:

Pretend that there is already an adversary in the environment when operating and defending resources. Continually monitor logs for suspicious activity, including changes to configurations, resource accesses, and network traffic.

Verify explicitly:

To make contextual access decisions to resources, all resources should be accessed consistently and securely using multiple attributes (dynamic and static).

4. Defining Zero Trust with Government Frameworks

Zero Trust initiatives require a clear governance definition. This requires federal agencies to assess the federal frameworks that are currently in place. NIST SP 800-207, TIC 3.0, and CDM are a few references for achieving Zero Trust in federal information systems

NIST SP 800-207:

In NIST SP 800-207, the National Institute of Standards and Technology provides a framework for designing zero-trust architecture (ZTA) network strategies (National Institute of Standards and Technology, 2020).

Trusted Internet Connections (TIC):

- A federal cybersecurity initiative called Trusted Internet Connections (TIC) increases network and perimeter security across the federal government.
- The Office of Management and Budget (OMB), the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) and General Services Administration (GSA) are collaborating to develop the TIC initiative.
- For risk management in federal information systems, this handbook offers a variety of security controls, applications, and best practices(Cybersecurity & Infrastructure Security Agency, 2022).

Continuous Diagnostics and Mitigation (CDM) :

- The Cybersecurity and Infrastructure Security Agency (CISA) leads the Continuous Diagnostics and Mitigation program(CDM).
- Cybersecurity tools, services, reporting, and best practices are provided by the CDM program across the federal government.

5. Pillars of Zero Trust Architecture

General Services Administration (2021) states that Zero Trust Architecture is based on eight (8) pillars:

1. User: Utilizes dynamic and contextual data analysis to verify user attempts to connect to a network using user identification, authentication, and access control policies.
2. Device: Assesses the cybersecurity posture and trustworthiness of user-controlled and autonomous devices using "system of record" validation.
3. Network: By dynamically defining network access and deploying micro segmentation techniques, as well as controlling network flows and encrypting data, sensitive resources are isolated from unauthorized access.
4. Infrastructure: Ensures that all systems and services within a workload are protected against unauthorized and unintended access.
5. Application: A set of security controls surrounds each workload and compute container so that no data is collected, no unauthorized access is authorized, and no

sensitive data is tampered with. Secures access at the application layer by integrating user, device, and data components.

6. Data: Data Security involves securing and enforcing data access based on data categorization and classification to isolate data from all but those who need access.
7. Visibility and Analytics: Analyzes the real-time communications between all Zero Trust components to provide insight into user and system behavior.
8. Orchestration and automation: Provides automated security and network operational processes across ZTA through orchestration of functions between similar and disparate security systems and applications.

6. Working of Zero Trust Architecture

Zero Trust Architecture comprises of three main components Controller, gateway and client.

Controller: The controller is a policy decision point or essentially the brains of the system acting as a trust broker. The controller checks context and grant entitlements.

Gateway: The gateway is the policy enforcement point, and they are located wherever resources need to be protected.

Client: Client is the one who needs to access resources.

The controller and the gateway are completely cloaked from prying eyes using a technology called Single Packet Authorization (SPA) with no exposed ports. This protects the system from many types of networks and credential based attacks. Basically you can’t attack what you can’t see.

Before moving forward to the working of zero trust architecture, let us see how network controllers and gateways works.

6.1. Network Controllers

According to Cisco (2022), this is how network controllers works:

1. A network controller is a software that organise network functions and It serves as an intermediary between the business and the network infrastructure.

2. The organization enters their desired business objectives into the controller which in turn sets up the network to deliver on those objectives.

3. Network controllers do their jobs by:

- Maintaining an inventory of devices in the network and their status
- Automating device operations such as configurations and image updates
- Analysing network operations, identifying potential issues, and suggesting remediation's
- Providing a platform for integration with other applications such as reporting systems

How network controllers evolved:

1. Element management systems (EMSs) were one of the early tools for network device control. They aided and monitored certain aspects of specific groups of network devices, and it wasn't unusual to find more than one EMS in a large network. While they were useful, they couldn't control a network globally.
2. Software Defined Networking(SDN) controllers fill a different need. These controllers are driven by applications that bring automation and agility to the devices they control.
3. Network controllers combine and expand on the functions of EMSs and SDN controllers. They help IT teams achieve more simplified, centralized, and agile operations, and they provide much-needed automation, performance analysis, fault detection and correction, and therefore, help achieve desired business outcomes.

   How network controllers solve today's IT challenges:

   - Reduce operating costs
   - Increase availability
   - Improve agility
   - Enhance security
   - Accelerate adoption of intent-based networking

What is a network controller's role in intent-based networking ?

1. An intent-based networking (IBN) architecture builds on SDN and provides the building blocks that transform a hardware-centric, manual network into a software-driven network that continuously captures business intent, translates it into policies, and applies them consistently across the network.

2. A network controller acts as a central control point for network activity in an intent-based network.

3. Network controllers provides the following functionalities in an intent-based network.

- Automation
- Translation
- Activation
- Analytics
- Security
- Integration

6.2. Working of Gateways

Mark Ciampa (2022) in his book CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition, states briefly about how cryptography is used in cybersecurity and here I have fetched some important points about cryptography which is used in the working of gateways in Zero Trust Architecture.

Gateways works on cryptography

What is Cryptography?

1. Information that has been scrambled to prevent reading.
2. Information is protected by transforming it into a secure format that cannot be accessed by unauthorized persons.
3. Encryption: Using cryptography, encryption transforms original text into a secret message.
4. Decryption: Decryption is the process of restoring a secret message to its original form.

5. Plaintext: Unencrypted data that has to be encrypted or the result of decryption is known as plaintext. A cryptography algorithm receives input in the form of plaintext data (also called a cipher).
6. Cyphertext: The unreadable and scrambled result of encryption is called ciphertext.
7. Three categories of cryptographic algorithms are:
   - Hash algorithms
   - Symmetric cryptographic algorithms
   - Asymmetric cryptographic algorithms

Hash Algorithms:

1. Hashing is the process of creating a unique "digital fingerprint" for a set of data.
2. The contents are represented by this fingerprint, referred to as a digest (also known as a message digest or hash).
3. Hash algorithms are primarily used for comparison purposes.
4. In order to ensure that the original data cannot be retrieved through hashing, the digest is intended to be one-way
5. Common algorithms include:
   - Message Digest (MD)
   - Secure Hash Algorithm (SHA)
   - Race Integrity Primitives Evaluation Message Digest (RIPEMD)

Symmetric Cryptographic Algorithms:

1. Documents are encrypted and decrypted with the same key in symmetric cryptographic algorithms.
2. The initial algorithms for cryptography were symmetric.
3. It is also known as *private key cryptography as* the key is kept private between sender and receive.
4. Common algorithms include:
   - Data Encryption Standard (DES)
   - Triple Data Encryption Standard (3DES)
   - Advanced Encryption Standard (AES)

- Rivest Cipher (RC)
- Blowfish

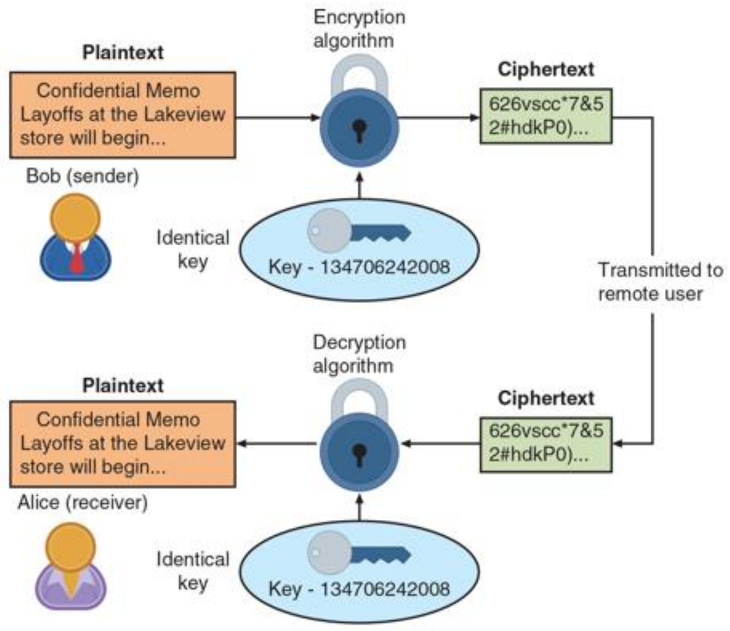

Figure 1 Example of Symmetric Algorithm

Asymmetric Cryptographic Algorithms:

1. The primary weakness of symmetric algorithms is a secure single key must be distributed and maintained among multiple users distributed geographically which is challenging.
2. Two mathematically related keys are used in asymmetric cryptographic algorithms.
3. It is often referred to as public key cryptography.
4. Public key: Everyone has access to the public key, which is freely distributed.
5. Private key: A private key is known only to the individual who owns it.
6. Keys can be used in either direction.
7. Common algorithms include:
    - RSA
    - Elliptic curve cryptography (ECC)
    - Digital Signature Algorithm (DSA)

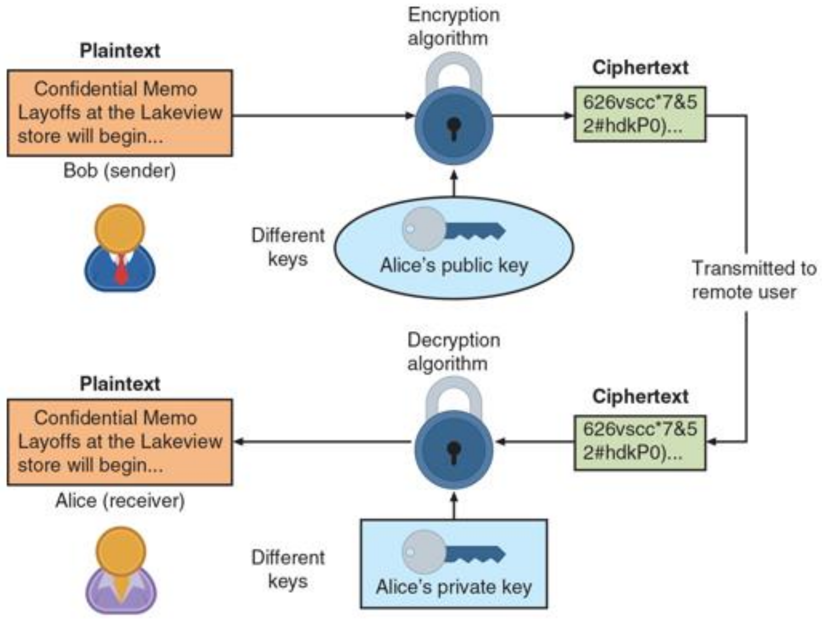

Figure 2 Example of Asymmetric Algorithm

Digital Signature Algorithm (DSA):

1. DSA makes a digital signature, which is an electronic means of confirming the sender.
2. Digital Signatures works on the principles of asymmetric algorithms but it also includes hashing. Basically Digital Signature Algorithm is a mixture of Hash Algorithm and Asymmetric Algorithm.
3. First the sender digest the plaintext through a hash algorithm and then the digest is sent to asymmetric cryptographic algorithms for encryption using a private/public key.
4. When receiver receives the cyphertext then the receiver decrypts the cyphertext using decryption algorithm with a private/public key then matches the digest value with the original hash value for data authenticity.
5. A digital signature can:
    - Verify the sender
    - Prevent sender from disowning the message
    - Prove message integrity

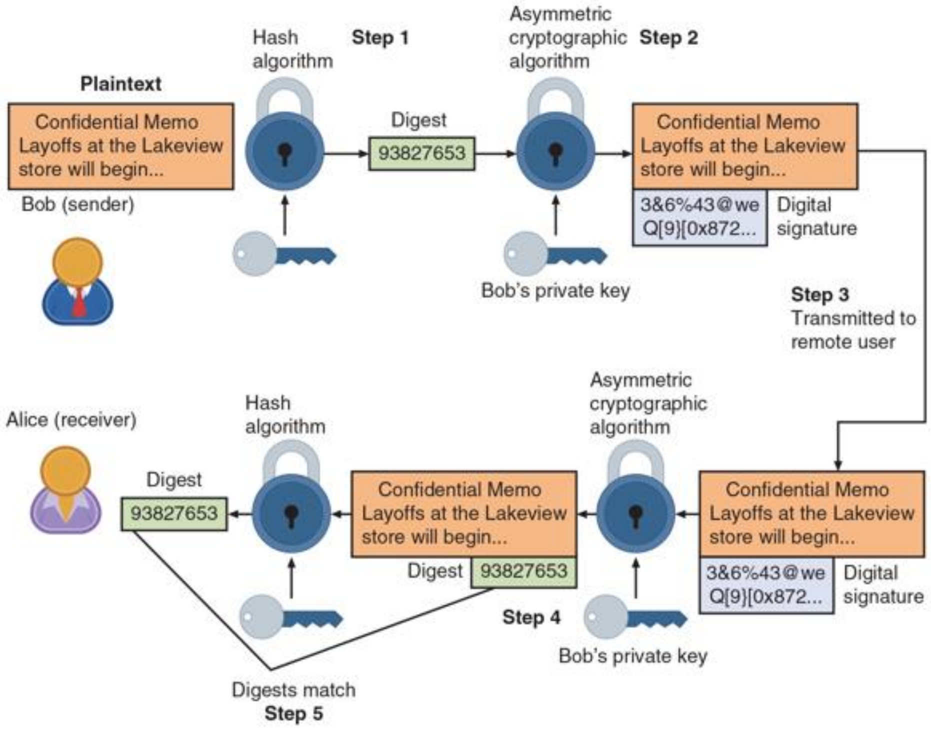
Hash algorithm
Step 1
Asymmetric cryptographic algorithm
Step 2
Plaintext
Confidential Memo Layoffs at the Lakeview store will begin...
Digest
93827653
Confidential Memo Layoffs at the Lakeview store will begin...
3&6%43@we Q[9}[0x872...
Digital signature
Bob (sender)
Bob's private key
Step 3
Transmitted to remote user
Alice (receiver)
Hash algorithm
Asymmetric cryptographic algorithm
Digest
93827653
Confidential Memo Layoffs at the Lakeview store will begin...
Confidential Memo Layoffs at the Lakeview store will begin...
Digest
93827653
3&6%43@we Q[9}[0x872...
Digital signature
Step 4
Bob's private key
Digests match
Step 5

Figure 3 Example of Digital Signature Algorithm

Defining Digital Certificates:

1. To prove that a document was sent by a valid sender, a digital signature is used.
2. Weakness of using digital signatures:
   - It can only prove that the digital signature was encrypted with the sender's private key.
   - Under a sender's name, an imposter could publish a public key.
3. Trusted third party:
   - Used to aid in resolving the identity verification issue.
   - The owner of the public key must be verified as well as the public key's ownership.

4. The purpose of a digital certificate is to tie a public key to a user's identity by having it "digitally signed" by a trusted third party.

6.3. Working of Zero Trust Architecture

When a user needs to access a resource, the client connects to the controller using SPA, the controller then authenticates the user with an identity provider which can use SAML, LDAP or RADIUS to validate and authenticate the user and pull back all configured user claims to use in determining access entitlements. The controller then checks user context, performs a deep device posture check and pulls in data from any third party sources like an ITSM, a SIM, or other security tools.

Based on this multi-dimensional identity profile, the controller generates what we call a live entitlement token and sends it to the client via a signed certificate. It is a live entitlement because it is dynamic based on context and risk at the time of access and therefore not static. Again, using SPA, the client sends that live entitlement packet to the gateway. The client can only connect to gateways where that user has been granted entitlements. Once the gateway validates that the signed token has not been tampered with, it dynamically generates a segment of one that allows access to specific resources that have been granted and other resources remains cloaked. Finally ZTA continuously monitors the system for changes in context and can adjust or revoke access privileges in near real time. It adjusts the segment of one based on this change in context. For example if a user’s role changes, they will lose access to one application and gain access to another.

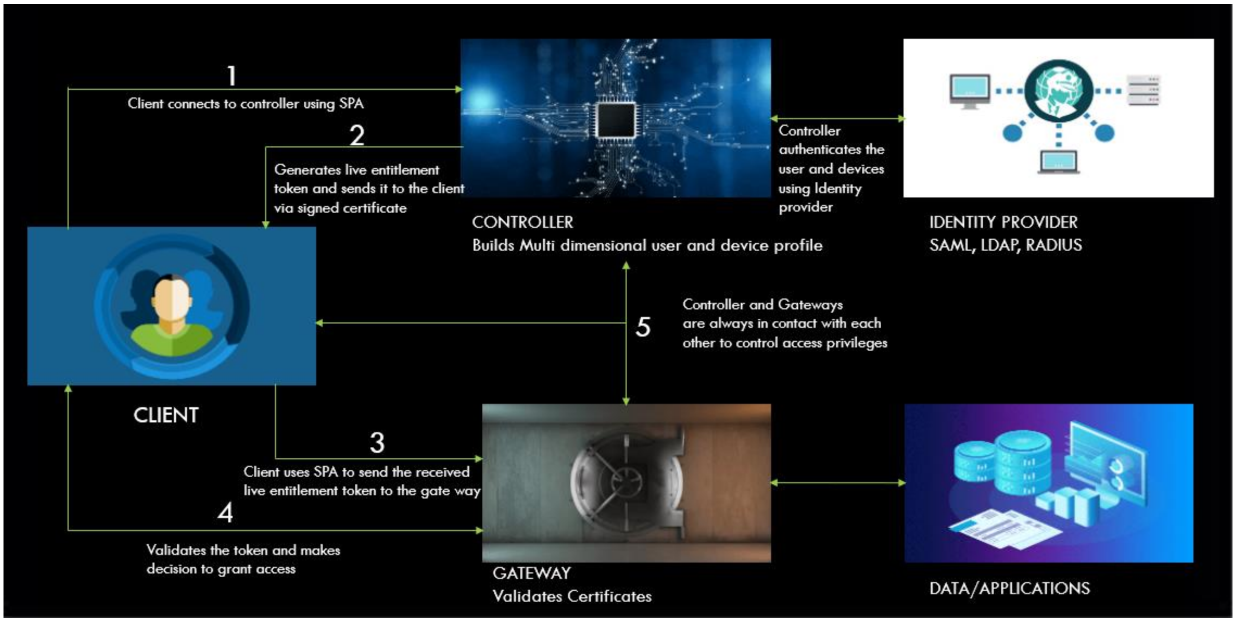
1
Client connects to controller using SPA
2
Generates live entitlement token and sends it to the client via signed certificate
Controller authenticates the user and devices using Identity provider
CONTROLLER
Builds Multi dimensional user and device profile
IDENTITY PROVIDER
SAML, LDAP, RADIUS
5
Controller and Gateways are always in contact with each other to control access privileges
CLIENT
3
Client uses SPA to send the received live entitlement token to the gate way
4
Validates the token and makes decision to grant access
GATEWAY
Validates Certificates
DATA/APPLICATIONS

Figure 4 Example of Working of Zero Trust Architecture

7. Implementing Zero Trust Architecture

According to General Services Administration (2021), It is important for security teams to monitor how data within an organization is used and distributed following approval of access to a Zero Trust network. DAAS (Data, Assets, Applications, and Services) are one of the most valuable assets of an organization and have become one of the most crucial components of its operation. An agency must identify the surface that needs to be protected before implementing a ZTA. In designing a protect surface, it is suggested that the protect surface be relatively small in comparison with the entire attack surface, an analysis of the ingress network flow and outgrows network flow should be performed based on the protect surface.

To ensure secure access to data, you need to know who the users are, which applications they use, and how they connect. Using this interdependencies analysis, the agency will be able to identify exactly where controls will need to be placed, resulting in multiple micro-perimeters around each DAAS.

This micro-perimeter is flexible and will move with the protected surface wherever it is located. Consequently, the agency will effectively establish micro perimeters by deploying segmentation gateways to ensure that only approved traffic or legitimate applications can access the protected surface.

Segmentation gateways are network components (hardware or software) that enforce granular access controls at the Application Layer (Layer 7) and based on the Kipling Method, the segmentation gateway functions as the PEP, which implements Zero Trust policies based on who, what, when, where, why, and how. It establishes who is allowed to transit a micro-perimeter at any given time, preventing unauthorized access to sensitive information and its ex-filtration. As agencies establish a Zero Trust policy around the protect surface, they must actively monitor and maintain their policy in real time, refining the protect surface, identifying potential interdependencies not yet considered, and finding ways to improve the policy.

8. Challenges of a Zero-Trust Security Model

According to TechTarget these are the top 6 challenges of a Zero Trust Security Model.

- Zero-trust cybersecurity can be compromised by a piecemeal approach.
- Lack of all-in-one zero trust products.
- Legacy systems might not be able to adjust to zero trust.
- Ongoing administration and maintenance is required by zero trust.
- Lack of trust might impair productivity.
- There are security issues with zero trust too.

a. Credentials for users could still be stolen.

b. Trust brokers have the potential to be points of failure and are vulnerable to attacks.

c. There is a possibility of attacking local physical devices and exfiltrating data from them.

d. Credentials for zero trust admin accounts makes tempting targets.

9. How to overcome Zero-Trust Challenges

TechTarget also includes how to overcome Zero Trust challenges.

- Running zero trust trials:

You should test zero-trust implementations and evaluate their security before putting them into production.

- Starting small:

Do not abandon legacy systems entirely when zero trust is introduced into live environments.

- Scaling slowly:

It is beneficial to introduce zero-trust security gradually so that a cybersecurity strategy doesn't get disrupted.

- Keeping zero trust and people in mind:

Having zero trust is undoubtedly a team sport. In order to create a successful zero-trust deployment, IT, security, networking, data, and application teams must coordinate with HR, finance, and the C-suite.

10. Literature Review

Deloitte (2021), state that “the Zero Trust concept is not new” - academics have debated its advantages and challenges for more than 20 years, its principle is that we should never trust anything without verifying it. A Zero Trust model was proposed by Forrester Research's John Kindervag in 2010, when he coined the term ("Zero Trust" network architecture). The technology for this concept has only begun to catch up in recent years, turning it from a theory to a concrete reality and as vendors introduce new products with huge sales claims and game-changing potential, this has created a lot of excitement at the same time. Kindervag presented five (5) ideas to make Zero Trust Architecture practicable:

1. Ensure that all resources are accessed securely
2. There is a need-to-know basis for access control
3. People shouldn't be trusted, verify what they are doing
4. Look for malicious activity in all logs coming into the network
5. Networks should be designed from the inside out

Zero Trust is a set of security principles, a framework for designing systems, and a coordinated approach to cybersecurity and system management that acknowledges that threats exist within and outside traditional network boundaries. In a dynamic threat environment, Zero Trust implements granular, dynamic access controls, comprehensive security monitoring, and automated system security to protect critical assets (data) in real time. As the title indicates, Zero Trust questions implicit trust between users, devices, and network components based on their location within a network. In a data centric security model, least privilege access can be applied to every access decision based on answers to the questions of who, what, when, where, and how.

11. Future Research Agenda

- According to (Nextgov, 2022) an executive order issued by President Joe Biden in May 2021 aimed at strengthening federal computer systems and networks with zero-trust architecture.
- There will be increased demand for endpoint security visibility and control in 2022 and 2023 , which will be followed by improving Identity and Access Management (IAM) effectiveness, integrating hybrid cloud, and automating patch management.
- The benefits of cloud-first, zero-trust platforms over legacy systems include cost savings, speed, and scalability. Security and risk professionals believe zero trust is a crucial strategy in their organizations, with 80% implementing it by 2022.
- It is becoming increasingly apparent that zero trust does not have to be expensive or challenging to implement if it is to be effective for organizations and the Chief Information Security Officer (CISOs) leading them and with this realization, coupled with the executive order signed by President Biden mandating zero trust architectures

across all government agencies, adoption across all organizations will accelerate. A 26% Compound Annual Growth Rate is predicted for spending on zero trust network access (ZTNA) solutions by 2025, according to Gartner and by 2025, $233 billion will be spent worldwide on information security and risk management, increasing at an 11% CAGR.

- There are more government agencies utilizing zero trust security architecture in comparison with corporations, with 72% of government agencies using a zero trust framework to 56% for corporations according to Okta.
- Research markets and Markets forecasts that global zero trust security will grow from $19.6 billion in 2020 to $51.6 billion by 2026, thanks to the increasing demand for products that support zero trust.
- The interoperability of these devices will rely on information sent and received over the Internet as the medical field adapts and relies on the Internet of Things (IoT) to report medical metrics from wearable technology to hospitals. The concept of Zero Trust is likely to be used by medical devices that are available outside the hospital as patients gain access to them.
- Software Defined Parameter (SDP) is a network architecture based on zero-trust principles, providing more secure remote access than VPNs and many experts believe that SDP and zero trust will eventually eliminate VPNs.
- Many of the major cloud companies like Microsoft Azure and Amazon web service are also adopting zero trust architecture.

12. Conclusion

In the wake of Zero Trust's announcement, vendors are making lots of claims about what it can offer - but can we trust them? By aligning security with the way businesses do business, reducing risk, improving agility, and reducing operating costs, Zero Trust can offer businesses a number of advantages. A true benefit, however, will only be achieved if the organization as a whole supports and commits to the effort.

13. References

For preparing this paper I have went through the articles from the following sources:

- General Services Administration (2021, June). *Zero Trust Architecture.* https://www.gsa.gov/cdnstatic/Zero%20Trust%20Architecture%20Buyers%20Guide%20v11%2020210810.pdf
- Deloitte(2021). *Zero Trust | Revolutionary approach to Cyber or just another buzz word?* https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf
- Dr. Sveinsson, R. L. (2022). *Top 10 Data Breaches So Far in 2022*.https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/
- National Institute of Standards and Technology (2020).*Special Publication 800-207:Zero Trust Architecture.* https://csrc.nist.gov/publications/detail/sp/800-207/final
- https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
- Mark Ciampa (2022). CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition.
- CISCO (2022). *What is a Network Controller*.https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-network-controller.html
- https://www.techtarget.com/searchsecurity/feature/How-to-implement-zero-trust-security-from-people-who-did-it
- Microsoft (2021, December 06). *Announcing the Microsoft Sentinel: Zero Trust (TIC3.0) Solution.*https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/announcing-the-microsoft-sentinel-zero-trust-tic3-0-solution/ba-p/3031685
- Microsoft (2022). *Embrace proactive security with Zero Trust.* https://www.microsoft.com/en-us/security/business/zero-trust

- Cybersecurity & Infrastructure Security Agency (2022, June 16). *TRUSTED INTERNET CONNECTIONS.*https://www.cisa.gov/tic

- Nextgov(2022, August 16). *Government Implementing Zero Trust Architecture Faster than Corporations. https://www.nextgov.com/cybersecurity/2022/08/report-government-implementing-zero-trust-architecture-faster-corporations/375911/*

- Check point (n.d.). *ZTNA vs VPN. https://www.checkpoint.com/cyber-hub/network-security/what-is-zero-trust-network-access-ztna/ztna-vs-vpn/*

- TechTarget (n.d.). top 6 challeges of zero trust security model. https://www.techtarget.com/searchsecurity/tip/Top-risks-of-deploying-zero-trust-cybersecurity-model