یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

US approach to moving toward Zero Trust Cyber Security Principles

Seyyed Mahdi Hashemi Karouei
Electrical and Computer Engineering Department
MalekAshtar University
Tehran,Iran
smmehdyhashemi@gmail.com

Vahid Monfared Gohar
Electrical and Computer Engineering Department
MalekAshtar University
Tehran,Iran
Vahid.mg@gmail.com

Abstract— **Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture uses zero trust principles to plan industrial and enterprise infrastructure and workflows. The US Government is presenting the zero trust strategy document, requiring agencies to meet specific cybersecurity standards and objectives by the end of fiscal 2024 to strengthen government defenses against complex and persistent threat campaigns. Microsoft has taken one of the biggest steps in updating the security philosophy in the world with the production of Windows 11 based on zero trust security principals.**

Keywords-component; zero trust; architecture; cybersecurity; network security;wndows11

1. Introduction

Zero trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure. An operative definition of zero trust is: “Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.”[1] The acceleration of digital transformation and the expansion of both remote and hybrid workplaces brings new opportunities to organizations, communities, and individuals.[2]

In the current threat environment, the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data. In May of 2021, the President issued Executive Order (EO) 14028, Improving the Nation’s Cybersecurity,2 initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks. [3]

2. Zero trust architecture

The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access.[4]

2.1. Zero trust basics

In the abstract model of access shown in Figure 1, a subject needs access to an enterprise resource. Access is granted through a policy decision point (PDP) and corresponding policy enforcement point (PEP).

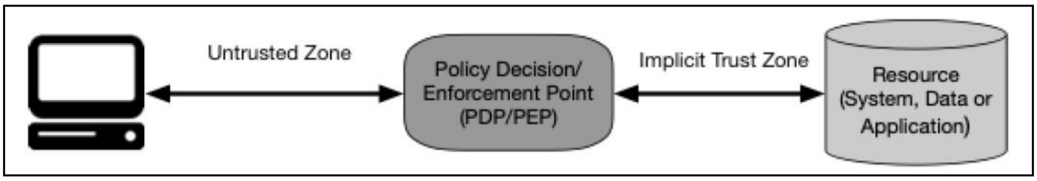

Figure 1. Zero Trust Access

The system must ensure that the subject is authentic and the request is valid. The PDP/PEP passes proper judgment to allow the subject to access the resource. This implies that zero trust applies to two basic areas: authentication and authorization. This means that an enterprise should not rely on implied trustworthiness wherein if the subject has met a base authentication level, all subsequent resource requests are assumed to be equally valid.[1]

2.2. Tenet of zero trust

A zero trust architecture is designed and deployed with adherence to the following zero trust basic tenets:

1- All data sources and computing services are considered resources.

2- All communication is secured regardless of network location.
3- Access to individual enterprise resources is granted on a per-session basis.
4- Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

The above tenets attempt to be technology agnostic. For example, “user identification (ID)” could include several factors such as username/password, certificates, and onetime password.[1]

2.3. Logical components of zero trust architecture

There are numerous logical components that make up a ZTA deployment in an enterprise. From Figure 1, the policy decision point (PDP) is broken down into two logical components: the policy engine and policy administrator (defined below). The ZTA logical components use a separate control plane to communicate, while application data is communicated on a data plane.[1]

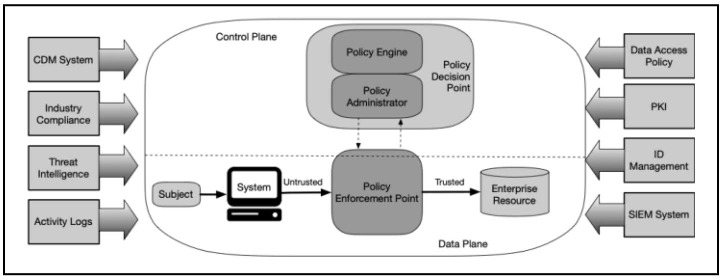

Figure 2. Core Zero Trust Logical Components

The component descriptions:

- Policy engine (PE): This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sourcesas input to a trust algorithm to grant, deny, or revoke access to the resource.
- Policy administrator (PA): This component is responsible for establishing and/or shutting down the communication path between a subject and a resource. It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start.
- Policy enforcement point (PEP): This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA.

A full ZT solution will include elements of all three approaches. The approaches include enhanced identity governance–driven, logical micro-segmentation, and network-based segmentation.[1]

Enhanced identity governance-based approaches for enterprises are often employed using an open network model or an enterprise network with visitor access or frequent nonenterprise devices on the network. Network access is initially granted to all assets but access to enterprise resources are restricted to identities with the appropriate access privileges. There is a downside in granting basic network connectivity as malicious actors could still attempt network reconnaissance and/or use the network to launch denial of service attacks either internally or against a third party. Enterprises still need to monitor and respond to such behavior before it impacts workflows.[5]

An enterprise may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources. The key necessity to this approach is that the PEP components are managed and should be able to react and reconfigure as needed to respond to threats or change in the workflow.[5]

The last approach uses the network infrastructure to implement a ZTA. In this approach, the PA acts as the network controller that sets up and reconfigures the network based on the decisions made by the PE. The clients continue to request access via PEPs, which are managed by the PA component. In this implementation, the agent and resource gateway establish a secure channel used for communication between the client and resource. There may be other variations of this model, as well for cloud virtual networks, non-IP based networks, etc.[1]

2.4. Device Agent/Gateway-Based Deployment

In this deployment model, the PEP is divided into two components that reside on the resource or as a component directly in front of a resource. The agent is a software component that directs some (or all) traffic to the appropriate PEP in order for requests to be evaluated. The gateway is responsible for communicating with the policy administrator and allowing only approved communication paths configured by the policy administrator.[1]

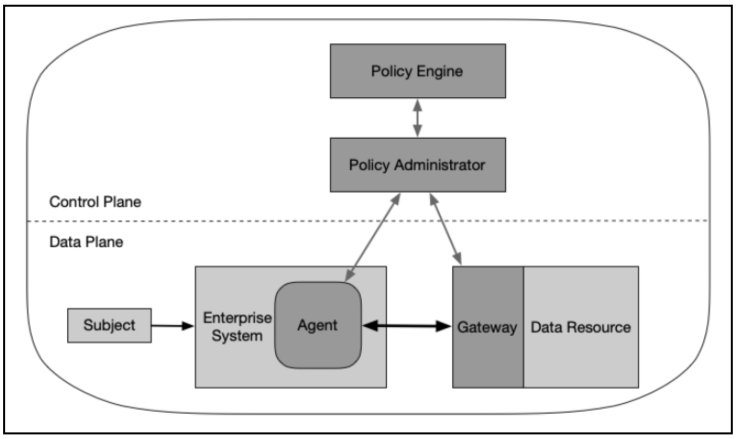

Figure 3. Device Agent/Gateway Model

3. US Strategy

A transition to a “zero trust” approach to security provides a defensible architecture for this new environment. The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction.[3]

This strategy envisions a Federal Government where:

• Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks.

• The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources.

• Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.

• Enterprise applications are tested internally and externally, and can be made available to staff securely over the internet.

• Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information[3]

3.1. Actions

Agencies should make use of the rich security features present in cloud infrastructure. This strategy frequently references cloud services, but also addresses on-premise and hybrid systems. The us government requires agencies to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024. CISA's zero trust model describes five complementary areas of effort .

1. Identity: Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant Multi-factor authentication[1] protects those personnel from sophisticated online attacks.

2. Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.

3. Networks: Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.

4. Applications and Workloads: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

5. Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.[3]

3.2. OMB[2] *Policy Alignment*

Moving to a zero trust architecture involves changes to nearly every aspect of an enterprise's security posture. As a result, this strategy necessarily touches on a large number of enterprise security practices, which can intersect with other existing OMB policies. Agencies are undergoing a transition to IPv6, while at the same time migrating to a zero trust architecture. Agencies should coordinate the implementation of these initiatives when they revisit their enterprise network infrastructure and policies. M-21-07 is not intended to require commercial shared service providers (e.g., ISPs, CSPs, CDNs) to migrate their internal infrastructures to support IPv6 alone. Instead, agencies should prioritize working with shared services platforms to ensure they provide IPv6 support on the interfaces exposed to system owners and other organizations.

To the greatest extent possible, agencies should centrally implement support for alternative authenticators in their enterprise identity management systems, so that these authenticators are centrally managed and connected to enterprise identities.

OMB M-19-26 and OMB M-21-31 – Alternatives to network inspection Current OMB policies neither require nor prohibit inline decryption of enterprise network traffic. Agencies are expected to balance the depth of visibility they need with the risks presented by broadly trusted network inspection devices.

Network traffic that is not decrypted can and should still be analyzed using visible or logged metadata, machine learning techniques, and other heuristics for detecting anomalous activity.

[1] MFA

[2] Office of Management and Budget

M-21-31 describes this conditional requirement: “If agencies perform full traffic inspection through active proxies, they should log additional available fields as described in Appendix C and can work with CISA to implement these capabilities. If agencies do not perform full traffic inspection, they should log the metadata available to them.”

OMB Memorandum M-15-1338 requires agencies to encrypt HTTP traffic that travels over the public internet to or from a Federal system, using HTTPS and HTTP Strict Transport Security (HSTS). M-15-13 specifically exempts internal connections, stating, “[T]he use of HTTPS is encouraged on intranets, but not explicitly required.” An “intranet” is defined as “a computer network that is not directly reachable over the public internet.”[3]

4. Windows 11 security

Windows 11 is a build with Zero Trust principles for the new era of hybrid work. Microsoft has provided modern security solutions that deliver end-to-end protection anywhere. Windows 11 raises the security baselines with new requirements built into both hardware and software for advanced protection from chip to cloud.[2]

The Zero Trust principles are threefold in windows11. First, verify explicitly. That means always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies. The second uses leastprivileged access, which limits user access with just-in-time and just-enough-access, riskbased adaptive polices, and data protection to help secure both data and productivity. And lastly, assume breach. Assume breach operates in a manner that minimizes blast radius and segments access. Verify end-to-end encryption and use analytics to gain visibility to improve threat detection and defenses.[2]

Windows 11 provides chip-to-cloud security, giving IT administrators the attestation and measurements to determine whether a device meets requirements and can be trusted. Directory, so access decisions and enforcement are seamless. Plus, IT Administrators can easily customize Windows 11 to meet specific user and policy requirements for access, privacy, compliance, and more. Individual users also benefit from powerful safeguards including new standards for hardware-based security and passwordless protection. Now, all users can replace potentially risky passwords by providing secure proof of identity with the Microsoft Authenticator app, signing in with face or fingerprint,[2] a security key, or a verification code sent to a phone or email.[2]

4.1. Hardware Security

Once inside, intruders can be difficult to detect while engaging in multiple nefarious activities from stealing important data or credentials to implanting malware into low level device firmware that becomes difficult to identify and remove. These new threats call for computing hardware that is secure down to the very core, including hardware chips and processors which store sensitive business information. By building security capabilities in hardware we can remove entire classes of vulnerabilities that previously existed in software alone.

A hardware root-of-trust helps protect and maintain the integrity of the system as the hardware turns on, loads firmware, and then launches the operating system. Hardware root-of-trust meets two important security goals for the system. It securely measures the firmware and operating system code that boots the system so that malware cannot infect boot code and hide its presence. Hardware root-of-trust also provides a highly-secure area isolated from the operating system and applications for storing cryptographic keys, data, and code. This protection safeguards critical resources such as the Windows authentication stack, single sign-on tokens, the Windows Hello biometric stack, and BitLocker volume encryption keys.

In addition to a modern hardware root-of-trust, there are numerous other capabilities in the latest CPUs that harden the operating system against threats such as by protecting the boot process, safeguarding the integrity of memory, isolating security sensitive compute logic, and more.[2]

4.2. Operating System Security

Hardware-based protection is only one link in the chain of chip to cloud security. Security and privacy also depend on an OS that guards your information and PC from the moment it starts. Windows 11 is the most secure Windows yet with extensive security measures in the OS designed to help keep you safe. These measures include built-in advanced encryption and data protection, robust network and system security, and intelligent safeguards against ever evolving viruses and threats. Windows 11 enhances built-in hardware protection with OS security out-of-the box to help keep your system, identity, and information safe.[2]

4.2.1. Trusted Boot (UEFI Secure Boot + Measured Boot)

The first step in protecting the operating system is to ensure that it boots securely after the initial hardware and firmware boot sequences have safely finished their early boot sequences. Malware attacks on the Windows boot sequence are blocked by the signature-enforcement handshakes throughout the boot sequence between the UEFI, bootloader, kernel, and application environments. Trusted Boot takes over where Secure Boot leaves off. The Windows bootloader verifies the digital signature of the Windows kernel before loading it. Often, Windows can automatically repair the corrupted component, restoring the integrity of Windows and allowing the PC to start normally.[2]

4.2.2. Cryptography

Cryptography is a basis for privacy to prevent anyone except the intended recipient from reading data, provides integrity checks to ensure data is free of tampering, and authentication that verifies identity to ensure that communication is secure. Cryptography on Windows 11 is subject to Federal Information Processing Standards (FIPS) 140 certification. FIPS 140 certification ensures that US government approved algorithms are correctly implemented (which includes RSA for signing, ECDH with NIST curves for key agreement, AES for symmetric encryption, and SHA2 for hashing), tests module integrity to prove that no tampering has occurred and proves the randomness for entropy sources.[2]

4.2.3. Certificates

Windows offers several APIs to operate and manage certificates. Certificates are crucial to public key infrastructure (PKI) as they provide the means for safeguarding and authenticating information. Windows offers users the ability to auto-enroll and renew certificates in Active Directory with Group Policy to reduce the risk of potential outages due to certificate expiration or misconfiguration. For certificate revocation, a certificate is added as an untrusted certificate to the disallowed CTL that is downloaded daily causing the untrusted certificate to be revoked globally across user devices immediately.[2]

4.2.4. Code signing and integrity

Code signing, while not a security feature by itself, is integral to establishing the integrity of firmware, drivers, and software across the Windows platform. Code signing creates a digital signature by encrypting the hash of the file with the private key portion of a code signing certificate and embedding the signature into the file. This ensures that the file hasn’t been tampered with, the Windows code integrity process verifies the signed file by decrypting the signature to check the integrity of the file and confirm that it is from a reputable publisher.[2]

4.2.5. Device health attestation

Device health attestation and conditional access are used to grant access to corporate resources. This helps reinforce a Zero Trust paradigm that moves enterprise defenses from static, network- based perimeters to focus on users, assets, and resources. Windows 11 supports remote attestation to help confirm that devices are in a good state and have not been tampered with. This helps users access corporate resources whether they’re in the office, at home, or when they’re traveling.[2]

4.2.6. Windows security app

Visibility and awareness of device security and health is key to any action taken. The Windows built-in security application found in settings provides an at-a-glance view of the security status and health of your device. These insights help you identify issues and take action to make sure you're protected. You can quickly see the status of your virus and threat protection, firewall and network security, device security controls, and more.[2]

4.3. Identity and Privacy

Malicious actors launch an average of 50 million password attacks every day—579 per second. And phishing attacks have increased, making identity a continuous the battleground for attacks. Windows 11 devices protect user identities by removing the need to use passwords from day one. With Windows Hello for consumers and Windows Hello for Business, customers can adopt passwordless multifactor authentication (MFA), significantly reducing the risk of compromise. Individual users can remove the password from their Microsoft account and use the Microsoft Authenticator app, Windows Hello[5] , a security key, or a verification code sent to their phone or email.[2]

4.4. Cloud Services

Today's workforce has more freedom and mobility than ever before. With the growth of enterprise cloud adoption, increased personal app usage, and proliferation of available apps, the risk of data exposure is at its highest. Enabling Zero Trust protection, Windows 11 works with Microsoft cloud services to help organizations strengthen their multi-cloud security infrastructure, protect hybrid cloud workloads, and safeguard sensitive information while controlling access and mitigating threats. [2]

4.5. Security Foundation

The end to end (E2E) Windows Supply Chain is complex and opaque, extending from developer's check-in to build, chips to firmware, drivers, core OS, 3rd party apps, manufacturing/factory, all the way to secure updates. Microsoft also put significant attention and investment to ensure the security of the E2E supply chain for Windows 11.[2]

5. Conclusion

Implementing a zero trust architecture requires extensive planning and it's a continuous process. The Zero Trust model of security is showing a great deal of promise in this regard. While Zero Trust has traditionally been used as a network security model, the principles also apply to data security and security architecture in general Organizations should consider classifying and identifying their critical assets and processes and implement zero trust architecture principles appropriately. Built on the principles of Zero Trust, every component of the Windows 11 technology stack, from chip-to-cloud, is purposefully designed to help ensure ultimate security. Windows 11 meets the modern threats of today's hybrid work environments by delivering hardware-based isolation, end-to-end encryption, and advanced malware protection.

References

[1] Scott Rose ., 2022 . Zero Trust Architecture , NIST Special Publication 800-207

[2] Microsoft ., 2022 .Microsoft Security Signals, September 2021

[3] Shalanda D. Young .,2022. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

[4] Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using .Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF))

[5] Software Defined Perimeter Working Group “SDP Specification 1.0” CloudSecurity Alliance. April 2014.