eclypses®

WHITE PAPER

Zero Trust Architecture

www.eclypses.com

Document ID: ECLYPSES-1532395320
Version No.: 2.0

Contents

Introduction

The Zero Trust Architecture (ZTA) is a strategy for completely protecting computer infrastructure and systems. In June 2021, the Cybersecurity and Infrastructure Security Agency (CISA) published a draft for public comment entitled Zero Trust Maturity Model which can be found at the following link: https://www.cisa.gov/publication/zero-trust-maturity-model .

As stated in that draft, “The path to zero trust is an incremental process that will take years to implement”, however one must start down that path. This document describes some practical ways that an organization can begin that journey.

Definition

As outlined in the reference document, the working definition of ZTA is as follows:

> ***“Zero trust** 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.*
> ***ZTA** is an enterprise’s cybersecurity plan that uses 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 ZTA plan.”*

The Challenge

The document then proceeds to layout the challenge of addressing this strategy.

> *“The Federal Government faces several challenges in transitioning to ZTA. First, legacy systems rely on “implicit trust”; this concept conflicts with the core principle of adaptive evaluation of trust within a ZTA. Additionally, existing infrastructures are also built on implicit trust and must either be rebuilt or replaced. To rebuild or replace information technology (IT) infrastructure and mission systems requires a significant investment on the part of agencies. Lastly, there is no consensus on or formal adoption of a maturity model for ZTA. While proposals for maturity models have been put forth, current initiatives for kickstarting zero trust adoption are often focused on the network layer and do not present a holistic approach for transition.”*

The Five Pillars

The document describes five pillars that one should consider while designing and implementing ZTA.

1. **Identity** - An attribute that uniquely describes a participant.
2. **Device** - A hardware asset that can connect to a network.
3. **Network / Environment** - An open communications mechanism used to transport messages.
4. **Application Workload** - Systems, computer programs, and services, either on-prem or cloud based.
5. **Data** - Information, both at rest and in transit.

These are fully documented in the reference document including strategies for supporting the protection of each.

Where to Start?

The full implementation can be overwhelming, but every step an organization can undertake is not wasted effort, as it plugs a potential threat vector and makes one’s enterprise a little more secure.

With that in mind, one must ask not, what is the low hanging fruit, but rather what is the most valuable fruit that effort must be expended on to protect the value of an organization.

The easiest situation to remedy may not be the most valuable. Bad actors will look for an easy pick, but state actors have the patience and resources to attack even the most difficult entities because they base their targets not on ease of compromise, but rather on value.

Consider the expense and risk of having a system compromised, especially if it was a preventable breach. The expense is not only monetary, but also a risk of loss of reputation or divulging of corporate secrets.

In a true ZTA, there is no implicit trust, but how can we enable that within the stated five pillars?

Identity

For any two endpoints to interact, there must be a means of identification and an assurance that the trust between these endpoints is warranted. Simply put, authentication and authorization. An initial exchange of authentication involves one endpoint identifying itself to its partner in the communication, and the partner determining if the identified endpoint is allowed to perform the action or access the system.

In a human interaction such as a web or mobile application, this is typically the exchange of a user identifier and a user secret. Many systems today rely on a method of Multi-Factor Authentication (MFA) to establish that original trust. However, even with MFA, credentials are transmitted across networks. MFA brings a better layer of security since it must employ multiple paths of communication for the various bits of information that must be validated on both ends, however, there are still public communication pathways that the information must traverse.

An ideal situation would be one that the exposure of credential exchange was held to a minimum, or possibly not at all. This would be ZTA with full knowledge. If an endpoint would be forced to register itself through an independent application and that registration was maintained at both ends of the conversation, the information exchange of user identifier and user secret could be protected over the communication channel in a way that interception would be fruitless.

In a system-to-system interaction, such as a set of services in a micro-services architecture, when a system is installed or updated, that trust relationship can be established and used to ensure that only authorized services can communicate with each other.

In an industrial control situation, a sending device is transmitting information to a receiving device for analysis, feedback, and control. The receiving device quite often will need to send control information back to the original sending device so that it can alter its behavior to compensate for anomalies in the information that was analyzed. When a replacement or maintenance action needs to be performed on either endpoint, trust must be re-established to ensure that the integrity of the system is maintained. This, again, relies on proper authentication and assured identity.

Device

If a legacy device is in a critically valuable position within a system, quite often this may be quite expensive or difficult to replace. Yet, an organization must assess the risk involved if that device were compromised. However, creating secure access to legacy endpoints that protect the transmission of information between them can then seamlessly present that information to the endpoint in the intended format for its consumption.

If the device is an application, the ability to alter it or replace it becomes more feasible. An update to an application endpoint can be designed to protect the exchange of information between endpoints and present the original data to the application so that it can continue to operate as intended.

One must think of the protection of a device as not only physical (is it isolated in a secure area), but also logical (can we be assured that it performs its duties as originally intended).

Network / Environment

There are many solutions that can be implemented to provide security on the edge of networks, but one must also consider the interactions between individual endpoints within a network. Again, the proper identification of endpoints prior to communication, and the hardening of information that travels between internal endpoints must be protected and no system should implicitly trust another endpoint, just because it is “within a protected sub-network” or “behind a firewall”.

Application Workload

Applications most often provide the gathering of information, the analysis of that information, and the result of that analysis as information returned to the originator of a request.

One must ensure that the information received, and the information transmitted assumes that the other endpoint is not trusted and can only create or consume that information in a way that the application can be assured of its integrity.

Data

Finally, as one can see from the above narrative, it all comes down to data. The assets of an organization are its data. How is it used, how is it analyzed, and how it is transmitted are the key points one must consider in building out a safe and secure system.

In the case of identity, the most vulnerable situation is in the transmission of registration or credential information. This must be protected at all costs.

In the case of a device, the assurance that the identity of the device is protected is key to its participation as an endpoint in an application.

The network is the means of the communication of that data but protecting it (while extremely important) is not the full answer. The data that is transmitted between endpoints, whether internal or external must be protected.

How can Eclypses help?

Eclypses has a technology that is optimized for protecting data as it flows between endpoints. This technology is FIPS 140-3 certified and is available today.

The Eclypses MTE® technology completely protects data that is transmitted between endpoints. It accomplishes this with no transmission or exposure of information to any network or communication system. It is a highly performant layer that is built into an application, and it assures that the endpoints in the conversation are the only participants that can act on the data.

In the case of protecting initial identity, the exchange of registration or credential information can be protected so that an interception of that data is useless. Furthermore, the receiving end of that data can be assured that the information originated from one and only one intended endpoint. Pattern recognition is rendered impossible since the exact same data between the exact same endpoints is different each time it is sent. Finally examining the data for inference based on the size of the transmitted payload is also protected since every transmission is exactly the same length regardless of the content.

In the case of protecting ongoing exchanges of data within an end-user application, each transmitted payload can easily be protected using MTE that provides the same level of protection as in the initial exchange.

When operating in a server-to-server environment, MTE can be utilized to protect every data stream between the participating endpoints ensuring not only the tamper-proofing of the data, but also the assurance that only the intended pairs can operate on the data.

In a legacy environment, a secure tunnel can be created using MTE to isolate the participating endpoints while providing the intended data stream to a specific endpoint.

If an application is highly secure, and the application vendor wants to ensure that it can only be accessed from trusted phone devices, MTE can be configured to fail a transmission if the device has been “rooted” or “jail-broken”.

MTE is available for a wide range of technologies and is ideally suited to add as a layer of protection at the application level to assist an organization on its journey to a Zero Trust Architecture.

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today’s environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies, websites, and IoT devices. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses’ patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

This technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT

contact@eclypses.com
www.eclypses.com
(719) 323-6680