European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 09, 2020

ISSUES WITH PERIMETER BASED NETWORK SECURITY AND A BETTER MODEL TO RESOLVE THEM

Bharatha Sreeja G[1], Mubeen Begum Saleem[2], Venkata Sravya[3], Divya K[4], Jayashree R[5]

[1]Assisstant professor, RMK College of Engineering and Technology, Chennai, Tamil Nadu, India

[2,3,4&5]UG Scholar, ECE Department, RMK College of Engineering and Technology, Chennai, Tamil Nadu, India

Abstract: Network firewalls are becoming irrelevant, neither can we be relied upon the perimeter networks nor can they be trusted. With adoption of bring your own device and convey your own cloud, we must evolve our defences to the devices and therefore the identities. ZTA is a response to enterprise network trends that include remote users, devices and cloud-based assets which are not situated within an enterprise-owned network boundary. In this paper we will be understanding how the security state and the trustworthiness contributes to overall security pose, considerations for automated access to resources via device also the identity conditions and the way to implement these conditions to the road of business SaaS apps or on-premises web apps.

Keywords: user identity, internal assets protection, architecture-zero trust, breaches.

1. Introduction

Some of the challenges faced due to Perimeter-based networks are that they operate on the assumption that all the systems and the users within a perimeter can be trusted. Unable to accommodate modern work styles such as Bring Your Own Device (BYOD) and Bring Your Own Cloud (BYOC), attacker can compromise single endpoint within trusted boundary and will also quickly expand foothold across the entire network. **USERS CAN NEVER BE TRUSTED! (NEITHER CAN THE NETWORK!) [1-5].**

Figure 1. How Breaches Occur

One of the most common attacks to which the users fall for easily is phishing. It is of various types such as smishing, search engine phishing, spear phishing, URL phishing, whaling, etc. Scammers use hidden links in which the user receives emails with action phrase “CLICK HERE” or “DOWNLOAD NOW”. They also use Tiny URL’s or misspelled URL’s. Whereas homograph attacks involve the usage of similar words and characters which can be easily misread like instead of “amazon.com” the user will be redirected to “arnazon.com”.

Here is how the zero-trust network comes to rescue due to new technologies like Internet of Things and mobile devices which force a new approach [7-9]. It eliminates the concept of trust based on network location within a perimeter. Instead Leverages the device and the user trust claims to gate access to data and the resources [1-3, 6].

2. Problems with Perimeter based Networks

- Insider threat is completely omitted.
- Multiple entry point, lots of firewall rules.
- Becomes more challenging talking about clouds, everything is API driven, staring from the entry point.
- All or Nothing Security, once an attacker gets in, lateral movement is really difficult to detect for most organizations as they are perimeter-focused.

2.1. Anectode of target breached through HVAC system

After this breach the question that arose was, how can an HVAC system lead to compromise of the target which was customers credit/debit card data? But it all comes back to the sort of the assumptions of the network.

- HVAC system was connected with the WIFI of store's network.
- The store's network was connected to a VPN backhaul to the corporate network.
- The corporate network was in turn connected to the production database.

So as an attacker they got hold over a weak WIFI encryption protocol from the parking lot. In the parking lot they could break the WIFI and connect to the HVAC system. Once they were able to get to that WIFI network they were able to pivot multiple hubs. Imagine store might be at left, corporate at middle and the production database at right. So they were able to pivot from network to network because they were all trusted/internal zones. They talk to one another until they can get to the database and from there they were able to exfil all the data sitting in the parking lot.

All that comes back to the assumption that the internal network is secure, which is clearly a bad assumption.

3. Zero Trust Architecture

- It eliminates the concept of trust based on network location within a perimeter.
- Zero trust networking is the idea of treating the private network like the public Internet: untrusted and adversarial.
- Zero trust architecture leverages micro segmentation to ensure that even if an attacker does enter the network, the amount of damage they can cause is severely limited.

4. What comprises a Zero Trust Architecture

- It's an Identity provider to keep a track of users and user-related information.

- Device directory to maintain the list of devices that have access to corporate resources, along with their corresponding device information such as the device type , integrity and so on.
- Policy evaluation service to determine if a user or a device conforms to the policy set forth by the security admins.
- Access proxy that utilizes the above signals to grant or deny access to an organizational resource.
- Anomaly detection and machine learning.

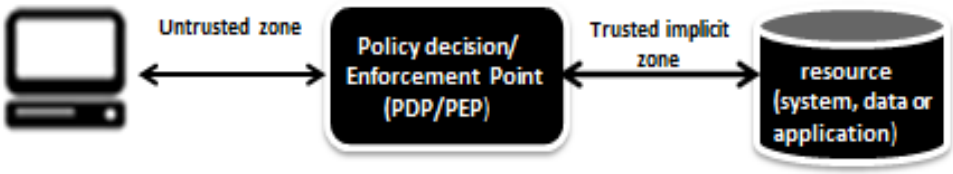


Figure 2. Zero Trust Access

5. Designing a Zero Trust Architecture

5.1. Start by asking questions

- Who are the users? What apps are trying to get access? How are they accomplishing that? Why is it done that way?
- What are the conditions required to access a corporate resource?
- What are the controls required based on the condition?

5.2. Set of conditions to be considered

- Employee and partner, users and control.
- Device health and compliance state.
- User's physical and virtual location.
- Client apps and authorization method.

5.3. Then follow up by a set of controls (If/Then state)

- Allow or deny access.
- Require Multi Factor Authentication (MFA).
- Force the reset of passwords.
- Control session access to the app which generally means allow read but not to download.

5.4. Determine the device health condition

- Determine the risk level of the machine whether if it's compromised by Pass-the-hash etc.
- Determine the integrity of the system which comprises of the Drivers, Kernel, Firmware, Peripheral firmware, Antimalware driver code.
- Validate the integrity as OS is running.

5.4. Identity conditions

- Try identifying the risk level of the user
- Is the sign in coming from:

1. Known botnet IP address
2. An anonymous IP address
3. Unauthorized browser
4. From unfamiliar location?

- Is that a suspicious sign? (i.e.) high number of failed attempts or matches the traffic pattern of other IP addresses such that of an attacker.

Whether the user's credentials are leaked due to dark web or any other black sites

6. Basic Assumptions

For any organization that utilizes ZTA in network planning, there are some basic assumptions for network connectivity and are as follows.

Assumptions for Enterprise-Owned Network Infrastructure:

1. The enterprise private network is not trustworthy. Devices on the network may neither be owned nor be configurable by the enterprise.
2. No device is to be trusted inherently.

Assumptions for Non-Enterprise-Owned Network Infrastructure:

1. Not every enterprise resource is on enterprise-owned infrastructure.

Local network connection cannot be trusted in case of remote users

7. Logical Components of a Zero Trust Network

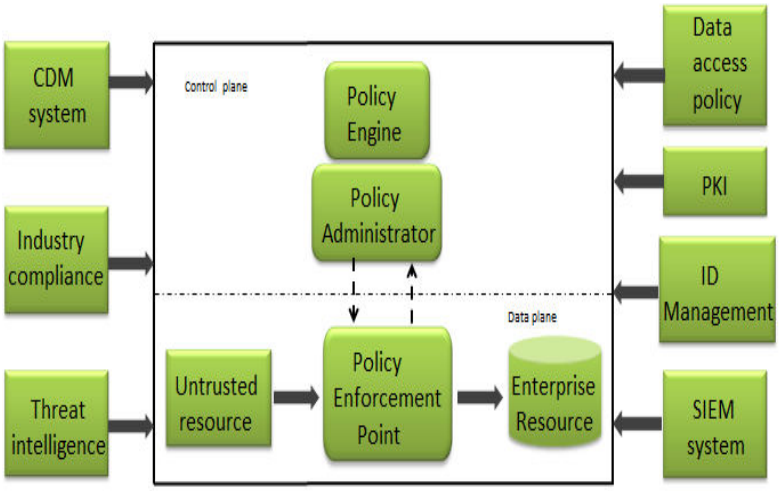
Policy Engine (PE): This component is liable for the ultimate decision in order to grant access to resource for a given client . The Policy Engine uses enterprise policy also as input from external sources (e.g., IP blacklists, threat intelligence services) as input to a "trust algorithm" to form a choice to grant or deny access to the resource.

Policy Administrator (PA): This component is liable for establishing connection between a client and a resource. It would generate any authentication token or credential employed by a client to access an enterprise resource.

Policy Enforcement Point (PEP): This system is liable to enable, monitor, and eventually terminate connections between a subject and an enterprise resource. This is a single logical component in ZTA also broken up into two different components: the client who is the agent on user's laptop and resource side which acts as a gateway component.

Continuous Diagnostics and Mitigation (CDM) System(s): This system gathers information about the current enterprise state and applies an update to configuration and the software components.

Industry Compliance System: This system ensures whether the enterprise remains compliant with any regulatory regime they'll fall under (e.g. FISMA, HIPAA, PCI-DSS, etc.). This includes all the policy rules which an enterprise develops to ensure the compliance.



Threat Intelligence Feed(s): This system enables or provides information from outside sources that help Policy Engine to perform access decisions. It includes DNS blacklists, malware, or command/control systems that the Policy Engine will require to deny access.

Data Access Policies: These are the set of attributes, rules, and policies about data access discovered by the enterprise around enterprise resources. This set of rules could be encoded or dynamically generated.

Enterprise Public Key Infrastructure: This system is liable for generating and logging certificate to resources and applications.

ID Management System: This system creates, stores, and manages enterprise user accounts and identity records. Basically contains the necessary user information such as name, email address, certificates, etc.

Security Incident and Event Management (SIEM) System: The system that aggregates system logs, network traffic, resource entitlements, and other events which provide the required feedback on the security posture of enterprise information systems. This data is then used to refine policies and predict possible active attacks against enterprise systems.

8. Trust Algorithm

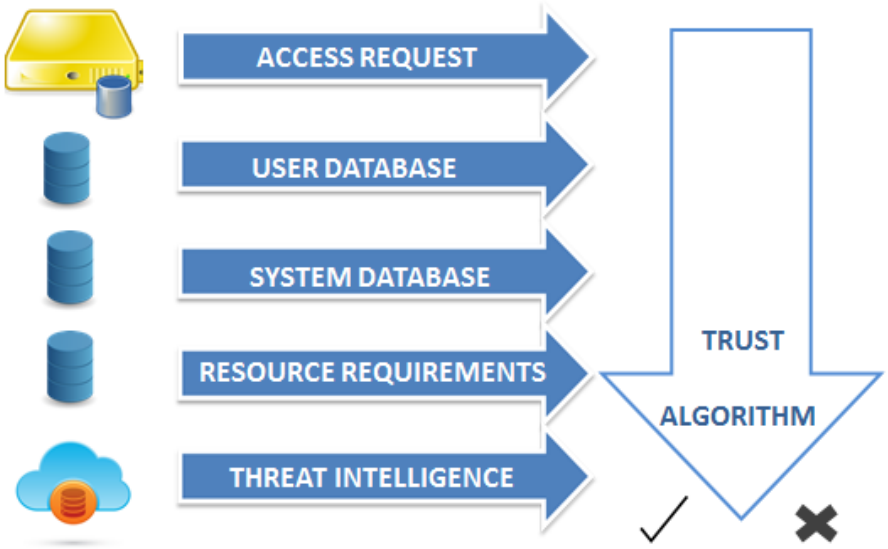
For an enterprise with a ZTA deployment, the Policy Engine can be referred to as the brain and the PE's trust algorithm as its primary thought process. The trust algorithm is the process through which the Policy Engine ultimately grants or denies access to a resource.

The Policy Engine gets its input from policy database with information about users, user attributes/roles, historic user behavioural patterns, threat intelligence sources, and other metadata sources.

Access request: It is the actual request from the application. The resource requested is the primary information used in addition information about the requester is also used.

User identification, attributes, and privileges: This is the "who" that is requesting access to a particular resource. It might be a set of users or a collection of user attributes developed by the enterprise.

System database and observable status: Includes OS version, application being used, location both the network location and the geolocation, Trusted Platform Module (TPM), and patch level. Depending on the system state, access to the internal assets might be restricted or else even denied.



Threat intelligence: This is an information feed(s) about general risks and active malware operating on the Internet. Includes attack signatures and the mitigations.

The weight of importance for each data source is configured. The final determination based on the importance of data is then passed to the PA for enforcement. The PA is responsible for terminating the connection based on the policy.

9. Key Elements of Zero Trust Network

No false sense of security: There are a lot of situations in which users and events in the interior of your perimeter cannot be relied upon. For example, an attacker who has entered with compromised credentials or insider threats, which may abuse privileges or move laterally through the network. A zero trust model makes this understanding explicit, and prioritizes protection against insider threats.

Multifactor authentication: MFA is the use of credentials in combination with an additional authenticator. For example, requiring a user to scan their fingerprint or confirm a PIN sent to a mobile device. A zero trust architecture implements MFA as a double-check against its own security measures.

Micro segmentation: It is the use of access controls to isolate the various components and services in your system. It allows you to layer security measures, such as firewalls or authorization measures, for greater security

10. Operations of a Zero Trust Model

- The key is the automatic gating to applications.

- Based on the device health there is an automatic remediation basically without the user's intervention.
- Policy violations monitoring.
- Prioritizing the alerts based on the sensitivity of data.

11. Benefits of a Zero Trust Model

- Allows conditional access to specific resources while selectively restricting access to the high-value resources on managed or compliant devices.
- Prevents network access and lateral movement with the use of stolen credentials and the compromised device.
- Enables users to be more productive by allowing them to work however they want, wherever they want and whenever they want.

12. Future Area of Research

ATTACKER'S RESPONSE TO ZTA: ZTA aims to reduce the exposure of resources to attackers. However, determined attackers won't be idle but will, instead, change behaviour within the face of ZTA. The issue right now is how the attacks will change. The metrics of "success" of ZTA over older cyber security strategies also will got to be developed.

13. Conclusion

Cyber security is an area of emerging security that has been felt in recent decades as an exponential concern because the number of devices connected to the web is increasing dramatically, with almost 90% of the planet population expected to be connected to the Internet by 2030 and with this, traditional security models are getting more and more impractical due to the increase in the sophistication of the attacks and there fore elimination of the perimeters of computer networks.

With this scenario, there's a requirement to possess another sort of approach on data protection. Considering that it's an "if-this-then-that" automated approach to Zero Trust. Networks which fail to evolve from traditional defenses are susceptible to the new emerging breaches. Thus the general security posture can be improvised by integrating this idea alongside the prevailing cybersecurity strategies

References

1. "cisco 2014 annual security report", published by cisco system inc.,. (last accessed february 9, 2015).
2. "cisco 2015 annual security report", published by cisco system inc.,.(february 9, 2015)
3. "ibm x-force trend and risk report", published by ibm corporation, october 2013 (December 18, 2015)
4. Matt Soseman, no more firewalls! how zero trust network is transforming cybersecurity, march(4-8),2019.
5. Implementing zero trust architecture Alper Kerman (NIST), Oliver Borchert (NIST), Scott Rose (NIST), Eileen Division (MITRE), Allen Tan (MITRE) (march 14, 2020).
6. Office of Management and Budget (2019) Update on Data Center Optimization Initiative (DCOI). (The White House, Washington, DC), OMB Memorandum M-19-19, June 25, 2019.

7. Ross R, Pillitteri V, Graubart R, Bodeau D, and McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach, Final Public Draft NIST Special Publication (SP) 800-160, Vol. 2.

8. zero trust architecture Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly ,Stu2Labs, (september 2019) .

9. Office of Management and Budget (2019) Update to the Trusted Internet Connections (TIC) Initiative. (The White House, Washington, DC), OMB Memorandum M-19-26, September 12, 2019.

10. American Council for Technology and Industry Advisory Council (2019) Zero Trust Cybersecurity Current Trends.

11. Kumar A, Senthil & Logashanmugam,. (2017). Secured Optimal Routing Based on Trust and Energy Model in Wireless Sensor Networks. IIOAB Journal. 9. 3-13.

12. Kumar A, Senthil & Logashanmugam. (2016). Novel key management techniques in Three-Tier Wireless Sensor Networks. 9. 903-910.

13. Thirunavukkarasu, V., Kumar, A. S., Josephine, D. J., & Arasu, T. P. (2020). Selection of Optimistic Nodes for Reputation Based Routing in Wireless Networks. In 2020 7th International Conference on Smart Structures and Systems (ICSSS) (pp. 1-5). IEEE.

14. Kumar, A. S., & Logashanmugam, E. (2016). Secure Acknowledgement based Misbehavior Detection in WSN (S-ACK). Indian Journal of Science and Technology, 9(40), 96063.