Review

Deployment of Zero Trust Access (ZTA) Policy as a Veritable Tool for Protecting Network Infrastructures and Users

Ignatius Ogbaga *, Chijioke Ogbonnaya, , Agwu Chukwuemeka

Posted Date: 3 July 2023

doi: 10.20944/preprints202307.0006.v1

Keywords: zero trust; zero trust access; cyberspace; cybersecurity; trust model

Review

Deployment of Zero Trust Access (ZTA) Policy as a Veritable Tool for Protecting Network Infrastructures and Users

Ogbaga, Ignatius Nwoyibe [1,*], Ogbonnaya, Chijioke Philip [2] and Agwu Chukwuemeka Odi [1]

[1] Department of Computer Science, Ebonyi State University, Abakaliki, ogbagaignatius@gmail.com; emeka2010@yahoo.com

[2] Department of Cyber Security, University of \West England, chijiokephilip@gmail.com

Abstract: As Cybercrimes continue to rise, researchers and industry players have continued to work hard to come up with solutions that could reduce and possibly eradicate these criminalities. This research has been able to discover the major factor that usually causes people to fall prey to these cyber criminals. This was why a school of thought came up with the Zero Trust Access model to strengthen the network framework. While previous network assets relied on the "trust but verify" philosophy, this technology's primary tenet is "never trust, always verify," which applies to every user and device connected to the network. This study interrogated the existing network models of the Integrative Trust Model (ITM) and Zero Trust Access (ZTA) in addition to the trust model (TA) to understand their concepts, implementation needs, strengths, and shortcomings. This made it possible for the study to establish the position of the ZTA model in repositioning the network security architectures vis-a-vis protecting the users

Keywords: zero trust; zero trust access; cyberspace; cybersecurity; trust model

1. Introduction

The volume of transactions that happen in cyberspace is unquantifiable. These volumes of transactions are permitted because cyberspace is a free trade zone that allows free entry and exit. However, because these transactions are performed by humans through the use of technology, these users vary in their expertise and experiences. The bad and the ugly ones amongst them have resorted to exploiting novice users. At some points, these malicious users also target careless and liberal users, thereby swindling or dispossessing them of their privacy and access rights to some resources in cyberspace. These malicious users deploy various methods to deceive their targets, such as unauthorized access [1] data breach [3], denial of service (DoS) [1], social engineering or phishing [4].

Due to this menace, some experts have consciously resorted to seeking solutions that could probably provide levels of security protection to internet users and owners of network infrastructures. These measures they believe could reduce or possibly eradicate the scourge of cybercrimes and criminalities. These measures include the use of password protection, multi-factor authentication methods, use of biometrics identification, use of behavioral analytics, access control techniques, use of firewalls, and intrusion detection techniques [5].

In addition to these numerous security measures already introduced, another school of thought led by John Kindervag proposed a security model known as the Zero Trust Access (ZTA) Model. This model applies a very simple but strict policy. It assumes everything (users) to be hostile by default. It proposes that no user or network devices should be trusted and thus should be continuously verified [6].

This security measure is a major departure from the conventional network security models deployed in centralized data centers. The ZT model architecture relies on the approved internet protocol (IP) addresses, device ports, and media access control (MAC) addresses to establish access controls and validate users of the network. Access to network services and resources is established

 doi:10.20944/preprints202307.0006.v1

based on the following factors: user identity and location, availability of the endpoint's devices, and the kind of application or services that are being requested by the user devices.

2. Literature Review

Some schools of thought have it that digital technologies that can be trusted ought to provide a secure environment for public and private activities. However, [7] noted that some state actors and cyber thieves were actively busy stealing data from the healthcare industries. This made many organizations start enforcing restrictions on their data access by introducing stricter security measures to secure their data. This ideology of zero trust was further echoed by former US President Ronald Reagan in his speech of "doveryai, no proveryai," or "trust but vigilance," used in nuclear armament discussions with former Russian President Mikhail Gorbachev in the 1980s [8].

Research has been carried out on Zero Trust model network access by several researchers and industry players such as [9]. These works focused mainly on network security and data access rights. The research also assessed the quality of service and trust in the network framework using various parameters such as incident management, secured access, log traffic monitoring and management, advanced threat protection, level of securely identifying devices, and data life cycle.

Moreover, [7] conducted a validation study on the ZTA model using the ON2IT model to ascertain the limitations of the Zero Trust Framework developed by the ON2IT architecture. The researcher deployed the Design Science Research (DSR) methodology while Hevner's work was adopted as a frame of reference with Wieringa's approach used to address the challenges and technical hitches encountered.

The following were the Critical Success Factors the research produced as the strength of the Zero Trust Framework after the research:

1. Stakeholders' engagements and collaborations on business applications
2. Easy integration with an existing control framework, such as between second-line risk managers and third-line.
3. Enable adequate administration of critical assets such as (Data, devices, Applications, and Services).
4. It ensures a clear and concise technology roadmap with other security frameworks in terms of role definitions and implementability of the existing governance and reporting processes. [10].

The researchers further validated the above critical success factors through a research questionnaire administered to capture the readiness and fitness of all operational levels of the ZTN framework based on four major improvements that should cover the shortcomings they formulated in their problem statement. The research adopted an iterative design methodology. The four major improvements their research proposed included:

1. There should be alignment between risk management and existing frameworks.
2. There should be a handshake between the board and business involvement and also an explicit sign-off.
3. Someone should bear the responsibility for asset risks and measures.
4. There should be a focus on both the deployment and running of the technology.

The research also made the following recommendations:

a. There should be operational support between the Zero Trust Management and boards to minimize the attack and provide swift-to-the-point incident reports.

b. Policy regulating traffic to and from a Zero Trust segment must be:

i. Specific and narrow, satisfying the 'least access' principle; ensuring that only functionally necessary traffic is allowed into the network

ii. Related to user groups

iii. Contain only the network applications

iv. Be inspected for threat detection/mitigation

v. Visible

c. Logs should relate to individual users;

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 July 2023 doi:10.20944/preprints202307.0006.v1

d. Presence and conformance of policy should be operationally safeguarded;
e. Policy should be orchestrated across multiple components in complex network paths.
f. Operational state and run-time characteristics should be structurally monitored.

2.1. Implementability of Integrative Trust Model (ITM)

[11] investigated the implementability of the Integrative Trust Model (ITM). This was due to a lack of awareness of how ITM can be applied in the context of Zero Trust architectures. In this research, a thought of a more secure system was brought into the trust ideology of "trust but verify"; to never trust and always verify as contained in the research [12]. The researcher adopted scoping review methodology. A comparative analysis was carried out to ascertain the strengths and weaknesses of ITM and ZTN using seven parameters: vulnerability, risk, monitoring, etc. as summarized in Table two:

Table 1 demonstrated that the ITM belong to the Trust model which applies the principle of trust but verify and is always willing to take risk and other attributes of trust. Mainly, this feature is by the traditional networking framework. This ideology of the trust network framework is divergent from the ZTN framework. However, this research aimed to raise awareness of this technology so that industry players and other authorities concerned can adopt this technology in their fight to maintain crime-free cyberspace.

Table 1. Comparative analysis between ITM and ZT Architecture (Allison, 2010).

S/N	Parameter	Trust: Integrative Trust Model (ITM)	Zero Trust (ZT) Architecture
1	Vulnerability	Willingness to be vulnerable	Not willing to accept vulnerability
2	Risk	Risk-taking	Not willing to take risks. Its interest is to reduce risk
3	Outcomes	Trust	It uses the factors of Authentication and authorization to establish trust
4	Control	Absence of Control	There is Constant Control
5	Monitoring	Absence of monitoring	There is Constant monitoring
6	Level of Access	Individual, team, organization	Subject: user (human), non-human (service, device, application)
7	Assessment	Ability, benevolence, integrity	Threat traffic: authentication and authorization

3. Research Method

This study was conducted through the review of some computer networking policy documents. This method enabled the researchers to understand the existing networking principles guiding the infrastructures and the users. The existing policies were compared using some parameters and factors that mostly contribute to security compromises among internet users. The outcome of this analysis guided the researcher's choice of a veritable networking policy that would offer better protection to both the users and owners of IT infrastructures

4.0. Discussions

4.1. Comparative Analysis between ON2IT Model and ITM Framework

On2IT is a network model that stemmed from the ZT framework that has been adopted by some firms to protect their data and network infrastructure. This research studied the framework to ascertain its strength and weakness as a yardstick for assessing the ZT framework.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 July 2023 doi:10.20944/preprints202307.0006.v1

To identify the clear cut between the two technologies, a comparative analysis was carried out as summarized in Table 2

Table 2. Comparative Analysis between ITM and ON2IT framework (Allison, 2021).

S/N	Parameter	ON2IT Model	ITM Framework
1	Framework	It is Under Zero Trust Framework	It is under a trust framework
2	Risk	It is not willing to take risk	It is willing to take risk
3	Trust	It adopts the *Never Trust, Always Verify* principle	It engages *trust but always verifies* the principle
4	Vulnerability	It is not willing to accept vulnerability	It is willing to be vulnerable
5	Control	There is serious control of data and network asset	There is no control
6	Monitoring	There is monitoring	Absence of monitoring

However, the major aim of Allison's research was to help to raise awareness and encouragement among policy-makers, practitioners, and academics on the ITM framework.

4.2. Core Principles of Zero Trust Access

The Zero Trust security model, by default, considers every user, device, and application as being a potential threat to the network. Access is granted or denied only after evaluating the legitimacy of a request determined by role-based access controls (RBACs) and other contextual parameters such as the request origin, timestamp, and user behavioral analytics.

When working to implement a Zero Trust security model, the Zero Trust Extended Security Model defines seven key principles or areas of focus. Five of these principles are based on the "default deny" security posture being applied to various corporate assets [10]. They are:

2. **Networks without trust**: This is one of the major principles of zero trust access. In film Cybersecurity or a Zero Trust policy, trying to defend the traditional network perimeter is not enough. A network without trust is divided into smaller units, with perimeters defined around the film's most valuable assets. Thereby making it easier to prevent the movement of threats through the network and to contain and isolate a potential breach.
3. **Absolutely no workload:** Cloud-based workloads, including assets such as containers, functions, and virtual machines (VMs), are appealing targets for cybercriminals and have unique security requirements. Tailored, granular Zero Trust security monitoring and access management are critical for safeguarding these assets, particularly in the public cloud.
4. **Data without trust:** Data security is one of the main objectives of a Zero Trust security policy. Locating sensitive or important data caches, mapping common data flows, and establishing access constraints based on business needs are all necessary when applying the principles of Zero Trust. The whole IT ecosystem of an enterprise, which includes desktops, mobile devices, application and database servers, and cloud deployments, must also be developed and enforced by these standards.
5. **Individuals without trust**: Based on this, credentials are the leading cause of data breaches, traditional authentication methods such as usernames and passwords are no longer adequate. Zero Trust network access necessitates strong authentication through multi-factor authentication (MFA).

6. **Devices without trust:** A Zero Trust security strategy considers all devices connected to the corporate network to be untrusted and potentially dangerous. Implementing Zero Trust security necessitates the ability to determine whether a device is a threat or not and if it is a threat, it quickly isolates it.

5. Conclusion

This research studied the existing network policies to understand their strengths and weakness. We studied network security policy models such as ITM, ZTA, and TA. Their abilities were compared against each other using some specific parameters. This method enabled the researchers to come up with a result of which among the models has advantages over the other in line with robustness.

Another major finding of this research is discovering the major factor that usually led to security compromises among internet users (devices and humans).

6. Recommendation

In line with the objective of this study, this research recommends zero trust access, which proposes, *never trust, always verify*" as the right policy framework that will *walk the talk* towards curbing the excesses of cyber criminals in cyberspace. The research of [13] proved the fact that people behave more consciously when they are aware that their actions are being monitored.

References

1. N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang, and Y. Xiang, "Data-driven cybersecurity incident prediction: A survey," *IEEE Commun. Surv. tutorials*, vol. 21, no. 2, pp. 1744–1772, 2018.
2. S. T. McIntosh T, Jang-Jaccard J, Watters P, "No TitleThe inadequacy of entropy-based ransomware detection. In: International conference on neural information processing," *Int. Conf. neural Inf. Process. New York Springer;* pp. 181–189, 2019.
3. A. Shaw, "Data breach: from notification to prevention using PCI DSS," *Colum. JL Soc. Probs.*, vol. 43, p. 517, 2009.
4. B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Comput. Appl.*, vol. 28, pp. 3629–3654, 2017.
5. H. Lawaniya, "What is network security, Types of Network Security and Prevention of devices in a network.," *Netw. Secur.*, Jun. 2020.
6. John Kindervag, "Security Round Table," in *A business magazine for executives on cybersecurity management, trends, and best practices*, Security Round Table, 2022. [Online]. Available: https://www.securityroundtable.org/contributor/john-kindervag/
7. Y. Bobbert, "On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering," *Int. J. It/bus. Alignment Gov.*, vol. 8, no. 2, pp. 28–41, 2017.
8. D. Kluge and S. Sambasivam, "Formal information security standards in German medium enterprises," in *CONISAR: The Conference on Information Systems Applied Research*, 2008.
9. M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008.
10. Y. Bobbert and J. Scheerder, "Zero trust validation: from practical approaches to theory," *Sci. J. Res. Rev*, vol. 2, no. 5, 2020.
11. W. Allison, "No Trust: Never rely on; always make sure," Cardiff University Business School, 2021. [Online]. Available: https://orca.cardiff.ac.uk/id/eprint/143206/1/WyldeA21DRAFTZT.pdf
12. A. Kerman, O. Borchert, S. Rose, and A. Tan, "Implementing a zero trust architecture," *Natl. Inst. Stand. Technol.*, 2020.
13. I. Ogbaga and I. A. Ajah, "Co-Designing a Mobile Intervention to Support the Prevention and Control of Malaria in Low-Middle- Income Communities in Nigeria," *Int. J. Inf. Secure. Priv. Digit. Forensics*, vol. 5, no. 1, pp. 64–75, 2021, [Online]. Available: JOURNALS@NCS.ORG.NG