Zero Trust Architecture: Different Technologies Used to Implement ZTA in a Commercial Environment

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Joseph Padraic Bannon

Spring, 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Rosanne Vrugtman, Department of Computer Science

Zero Trust Architecture: Different Technologies Used to Implement ZTA in a Commercial Environment

CS4991 Capstone Report, 2023

Joseph Padraic Bannon
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
jb9war@virginia.edu

ABSTRACT

The largest security concern that many companies face is the increasing number of both devices and methods used to access corporate networks. The solution to this issue is removing traditional network security boundaries and implementing a zero-trust architecture (ZTA) model for all users. In my summer internship, I worked for a consulting firm to implement a zero-trust architecture-based identity and access management solution for a state government client. To design our solution, we communicated with the client to determine compliance, risk and user requirements. From this analysis, my team selected Symantec VIP and used features such as multi-factor authentication and context-based authentication. For this project, we tailored our implementation choices towards the specific technology the client required. Communication with the client throughout the design and implementation process was vital to the success of the project. The future work necessary for this project is to provide a monitoring process for security incidents. As threats change over time, adapting to a changing attack surface becomes a crucial aspect of the zero-trust model.

1. INTRODUCTION

One of the most important and most overlooked aspects of web application development is security. Part of what makes security difficult is implementing an identity and access management (IAM) system while satisfying realistic customer requirements. Our team's design for the IAM system was based upon ZTA principles. ZTA is designed to eliminate traditional network security boundaries and verify the identity of users as they access resources regardless of their network location (Rose, et al, 2020). “Never trust always verify” allows users to access network resources from any network location on any device without compromising security.

In my summer internship, I worked for a consulting firm to implement ZTA-based IAM solution for a state government client. The technical implementation of the project included the features of multi-factor authentication, context-based authentication and fine-grained authorization. Additionally, team leveraged communication with the client to achieve a design that satisfied the client’s security requirements. We obtained requirements in three specific ways: 1) by communicating directly with the client; 2) by researching government security compliance specifications; and 3) by determining technical necessities for the project.

2. RELATED WORKS

Rose et al. (2020) discussed implementation details of ZTA as a solution to providing security for resources not located within an enterprise-owned network

boundary. The authors posited that zero trust could improve an enterprise's overall information technology security posture, though if not implemented properly, ZTA can restrict access to necessary resources. My project utilized Collins' approach to ZTA but addressed the potential deadlock it can cause by using role-based access control to standardize access.

A number of experts in the field of ZTA have proposed the use of multi-factor authentication as a potential solution to passwords being a single point of failure (Ometov et al., 2018). The major advantages to adopting this approach include reducing the risk of attackers compromising accounts; though the security of multi-factor authentication relies on all users having access to second factors, which can limit usability. My approach to the problem of MFA utilized the authors primary recommendation, but my team and I addressed the potential drawbacks by expanding the scope of second factors to SMS and email.

According to Sarkar et al. (2022), the primary advantage of utilizing context-based authentication as an element of design for authentication is that it can more accurately assess risk of a login based on additional information provided by the user other than usernames and passwords. He also cites potential drawbacks to this approach, including having to configure sensitivity of risk. My project borrowed a portion of the authors' recommendation to assess the risk of each login but avoided potential drawbacks of generating high false positive rates by increasing the risk tolerance.

3. PROJECT DESIGN

The most significant elements of my project design were system architecture, which consisted of the VIP Enterprise, identifying the client's needs and system limitations.

3.1 Review of System Architecture

The enterprise's perimeter network (DMZ) has a VPN gateway to enable remote users to access internal network resources. Remote users sign in to the VPN or web server using their current Active Directory user name and password. The VPN gateway authenticates these by a call to the company's Active Directory. If the username and password are correct, the VPN gateway authorizes the user to connect to the corporate network to access protected resources. If the username and password are not correct, the VPN gateway denies a user's sign-in.

The addition of the VIP separates the authentication from the active directory/ business logic and includes a VIP Enterprise Gateway to communicate with the rest of the architecture. First, remote users arrive at the sign-in page of an enterprise's VPN gateway or web server. They enter their enterprise user name, password, and security code (from the MFA application). The VPN gateway or web server forwards these credentials via RADIUS to VIP Enterprise Gateway. VIP Enterprise Gateway authenticates the user's credentials against the enterprise's Active Directory/ LDAP. Once authentication is successful, VIP Enterprise Gateway validates the user's security code against the VIP validation service in the cloud. If the code is validated, VIP Enterprise Gateway responds to the VPN gateway's RADIUS authentication request by granting access to the network resources (Figure 1).

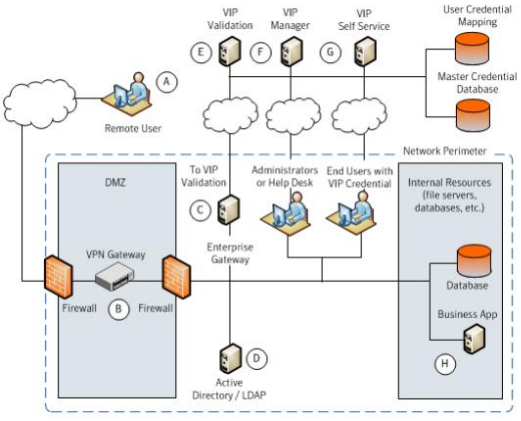

Figure 1: Network architecture with Symantec VIP

3.2 Requirements

To understand my requirements, it is important to understand the context of the client being a state agency with requirements to state, federal and citizen stakeholders.

3.2.1 Client Needs

I determined the client's needs in three ways: 1) by communicating directly with the client; 2) by researching government security compliance specifications; and 3) by determining technical necessities for the project. By communicating with the client, we determined the need for system that included using email and SMS as a second factor. Additionally, the client requested to be able to customize the risk-based authentication for factors including geo-location, IP address, geo-velocity, device sanitization, etc. We gathered these requirements by communicating with the stakeholder in the design phase as well as eliciting feedback from a minimum viable product.

We obtained the government security compliance specifications by consulting documentation from federal agencies. In particular, NIST outlines security measures for storing Personally Identifiable Information (PII) of customers, as well as multi-factor authentication configuration. McCallister, et al. (2010) lays out a precaution to take for storing PII such as hashing passwords, strength of encryption and not using PII as database identifiers. Furthermore, we set up the web agents required to obtain user information for context-based authentication (Sarkar et al., 2022). Similarly, we implemented a RADIUS system as a way to centralize the communication with the active directory and provide fine-grained authorization (Tang, 2011).

3.2.2 System Limitations

The most relevant system limitation in terms of security was the user's ability to spoof information during authentication. While the VIP system can collect user information, this information can easily be spoofed by attackers trying to compromise user accounts. Although this creates a more secure environment, it can result in a false sense that security does not need to be maintained. Another key limitation is the tradeoff between security and usability. This tradeoff is exposed when dealing with MFA for SMS/email.

3.3 Key Components

The key components of my project are the VIP Enterprises software, Azure cloud and commercial features.

3.3.1 Specifications

The system uses a traditional three-tiered web architecture with separate business logic, database and presentation layers. For authentication, the system collects login requests at a central RADIUS server and sends them to the VIP Enterprise Gateway to verify with the active directory and MFA. The active directory was hosted on Azure Active Directory. The VIP service is hosted on Microsoft Azure cloud using Azure Kubernetes Services. The client's information is collected using ingress and egress filters such as Kibana and Elastic Search.

3.3.2 Challenges

One of the challenges while implementing the system was disagreement between my team and the client as to whether the implementation should use a Commercial-off-the-shelf (COTS) solution or an in-house developed solution. The primary issue came down to flexibility of the system configurations. The client wanted a system totally controlled by them, while my team wanted a solution that was proven to work in a variety of network environments.

3.3.3 Solutions

The solution to the challenge of determining whether to implement a COTS or an in-house solution came from identifying

the capabilities of the client and relating to the strengths and weakness of each system (Petersen et al., 2018). The major advantages of COTS solutions are reliability in multiple environments, dedicated customer support and developer providing sole focus on providing the COTS service.

4. ANTICIPATED RESULTS

We completed the design phase and a minimum viable product for the client. The outcome of the design phase was choosing three features for Symantec VIP used in the context-based authentication, which were IP address blocking, device hygiene and geo velocity. The anticipated result of the project is a significant decrease in the incidence of user accounts compromised.

5. CONCLUSION

ZTA is a worthwhile security investment; however, to be successful, the implementation must be clearly defined with the clients' needs in mind to be successful. The essence of this implementation was separating the authentication from the rest of the business logic by using the COTS product, VIP Enterprise. This modular implementation provided security features including multi-factor authentication, context-based authentication and fine-grained authorization and it satisfied the client's security requirements.

Another important aspect of the implementation was communication with the client and determining the requirements. Being a state government agency, the client was subject to a variety of state and federal compliance regulations. Furthermore, they had to make sure the system was available for all citizens that needed to use it. In some cases, the requirements for availability and security conflicted and had to be resolved through communication between the team and the client. Through this project, I gained both technical and communication skills by working with a client to satisfy their requirements.

6. FUTURE WORK

Future work for this project includes finishing the implementation and deploying the final product to the consumer. Out of the software development phases of project initiation, planning, development, production and operations, the project still needs to complete the development, production and operations phases. This entails creating a working implementation in the client environment, testing the system, deploying the system to customers and managing post deployment operations.

The most important aspects of future work on the implementation are scalability and fault tolerance. The client being a state government agency have an elevated responsibility to the citizen to be able to reliably access the system. Implementing load balancing and performing load tests will be crucial to validating the reliance of the system against depletion resources.

REFERENCES

McCallister, E., Grance, T., & Scarfone, K. *Confidentiality of Personally Identifiable Information (PII)* (NIST Special Publication (SP) 800-122). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-122

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Petersen, K., Badampudi, D., Shah, S. M. A., Wnuk, K., Gorschek, T., Papatheocharous, E., Axelsson, J., Sentilles, S., Crnkovic, I., & Cicchetti, A. (2018). Choosing Component Origins for Software Intensive Systems: In-House, COTS, OSS or Outsourcing?—A Case Survey. *IEEE Transactions on Software*

Engineering, *44*(3), 237–261. https://doi.org/10.1109/TSE.2017.2677909

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability*, *14*(18), 11213. https://doi.org/10.3390/su141811213

Tang, Q. (2011). Towards Public Key Encryption Scheme Supporting Equality Test with Fine-Grained Authorization. In U. Parampalli & P. Hawkes (Eds.), *Information Security and Privacy* (pp. 389–406). Springer. https://doi.org/10.1007/978-3-642-22497-3_25