FACULTY OF SCIENCE, ENGINEERING AND COMPUTING

School of *Computer Science & Mathematics*

BSc DEGREE
IN
Cyber Security and Digital Forensics

PROJECT PROPOSAL

Name: Sayumi Muthukumarana

ID Number: K2262367

Project Title: Implementation of a Zero Trust Architecture as a proof of concept for modern organizations to increase security.

Project Type: Build

Date: 11.12.2022

Supervisor: Ms. Ama

Kingston University London

Did you discuss and agree the viability of your project idea with your supervisor?	Yes
Did you submit a draft of your proposal to your supervisor?	Yes
Did you receive feedback from your supervisor on any submitted draft?	Yes

Abstract

New threats surface every hour of every day in the technological world of today. By connecting to the Internet, you increase the likelihood that a hacker may target your company. Cyber danger and cybercrime are major global concerns for businesses and governments. If firms don't have a suitable cybersecurity plan, there are significant financial and reputational consequences.

Making sure that your organization's data is secure from intrusions by malicious insiders and outsiders is known as cybersecurity. It can include a collection of methods, tools, procedures, and structures that are employed to guard against illegal access to or deterioration of networks, computers, software, and data. Any cybersecurity strategy should aim to protect data integrity, availability, and confidentiality.

This project aims to develop a solution to address the cyber threats within an organization by implementing the Zero Trust Model. Zero Trust, a security framework, sees every traffic as suspect. It implies that you don't trust any network communication entering or leaving it. These include user, device, network, and application traffic. Traffic between internal systems and external systems is also included.

Contents

List of Figures

List of Tables

1. Introduction & Background

1.1 Introduction

"Zero Trust" is a security tactic. It is an approach to designing and putting into practice the following set of security principles rather than a good or service:

- Verify explicitly
- Use least privilege access
- Assume breach

The foundation of Zero Trust is this. The Zero Trust model assumes breach and verifies each request as though it came from an uncontrolled network, as opposed to thinking that everything behind the company firewall is secure. Zero Trust Model teaches to:

> “Never trust, always verify”

This project is based on the security aspects addressed through the implementation of Zero Trust Architecture within an organization.

1.2 Background and Motivation

The digital universe is evolving into a vast network of connections. In this more complex context, managing security can be challenging. Traditional network security has concentrated on perimeter defenses; once a subject enters the network perimeter, they frequently have unrestricted access to a variety of company resources. Through impersonation and escalation, hostile actors can access the resources from either inside or outside the network if the subjects are compromised. The difficulty of protecting an organization's digital assets is further increased by the proliferation of cloud computing, the Internet of Things (IoT), business partners, and the rise in the number of remote workers. This is because there are now more ports of entrance, exit, and data access than ever before.

In order to combat this trend, a zero-trust architecture (ZTA) focuses on safeguarding resources rather than just network perimeters. The cybersecurity strategy "zero trust" is based on a set of principles that shifts network defenses away from broad, static network perimeters and toward a narrower focus on subjects, enterprise assets (such as devices, infrastructure components, applications, virtual and cloud components), and individual or small groups of resources. An enterprise infrastructure and processes are planned for and protected using zero trust principles by a ZTA. No implicit trust toward assets and subjects, regardless of their physical or network locations, is embraced by a ZTA environment by design. As a result, a ZTA never permits access to resources before a subject, object, or workload is confirmed through trustworthy authentication and authorization.

The zero-trust model is implemented around the following three main principles.

1. Verify Explicitly

   Use all relevant information, such as identity, location, device health, resource, data classification, and anomalies, when making security decisions.

2. Use Least Privilege Access

Just-in-time and just-enough-access (JIT/JEA) and risk-based adaptive policies can be used to restrict access.

3. Assume Breach

   Micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat identification and response can reduce the blast radius.

1.3 Problem in brief

Data now provides competitive difference, consumer insights, and product ideas, making it the lifeblood of the business. Although data presents opportunities, it may also expose businesses to substantial financial and legal risk.

Also, there are several cyber security concerns for small businesses, and each company needs to be secure in every aspect. This means that a security plan needs to be robust enough to counteract both internal and external threats. In addition, maintaining security is a shared duty, and a successful defense depends on effective teamwork.

Therefore, organizations today require a new security paradigm that more successfully responds to the complexity of the contemporary workplace, welcomes the hybrid office, and safeguards users, devices, apps, network, and data wherever they may be.

2. Aim & Objectives

2.1 Aim

This project aims on designing a complete Zero Trust Model, addressing all aspects of it; Identity Verification, Device Verification, and Infrastructure Validation, related to a certain organization.

2.2 Objectives

1. To implement a system that secures identity.

2. To secure corporate devices within an organization.

3. To implement a system that explicitly verifies all types of integrated applications.

4. To verify all types of networks connected to a system.

5. To implement a system for explicit verification of data associated with an organization.

3. Technologies & Resources

For both public and private networks, it is necessary to centralize four key components in order to increase productivity by explicitly validating user accounts and devices before granting access.

The core tenet of Zero Trust is "never trust, always verify," and it must be applied to safeguard each of these components from attackers.

For each access request, different technologies specifically validate trust using Zero Trust for:

1. Identities
2. Endpoints / Devices
3. Applications
4. Network

2.1 Technologies Used

1. **Identities**

- Conditional Access Plan
- Azure AD Multi-Factor Authentication (MFA)

2. **Endpoints /Devices**

- Microsoft Defender for Endpoint
- Microsoft Intune

3. **Applications**

- Application Management in Azure AD
- Microsoft Defender for Cloud Apps

4. **Network**

- Microsoft Defender for Endpoint

- Azure Firewall Threat Intelligence-based filtering

5. **Data**

- Azure Information Protection (AIP)

2.2 Resource Requirement

Licensing Requirements:

1. Azure AD Premium P1 licenses
2. Microsoft 364 E3 or E5

4. Methodology & Work plan

For successful adoption of Zero Trust within the organization, it is a necessity to address all the elements of the Zero Trust Architecture.

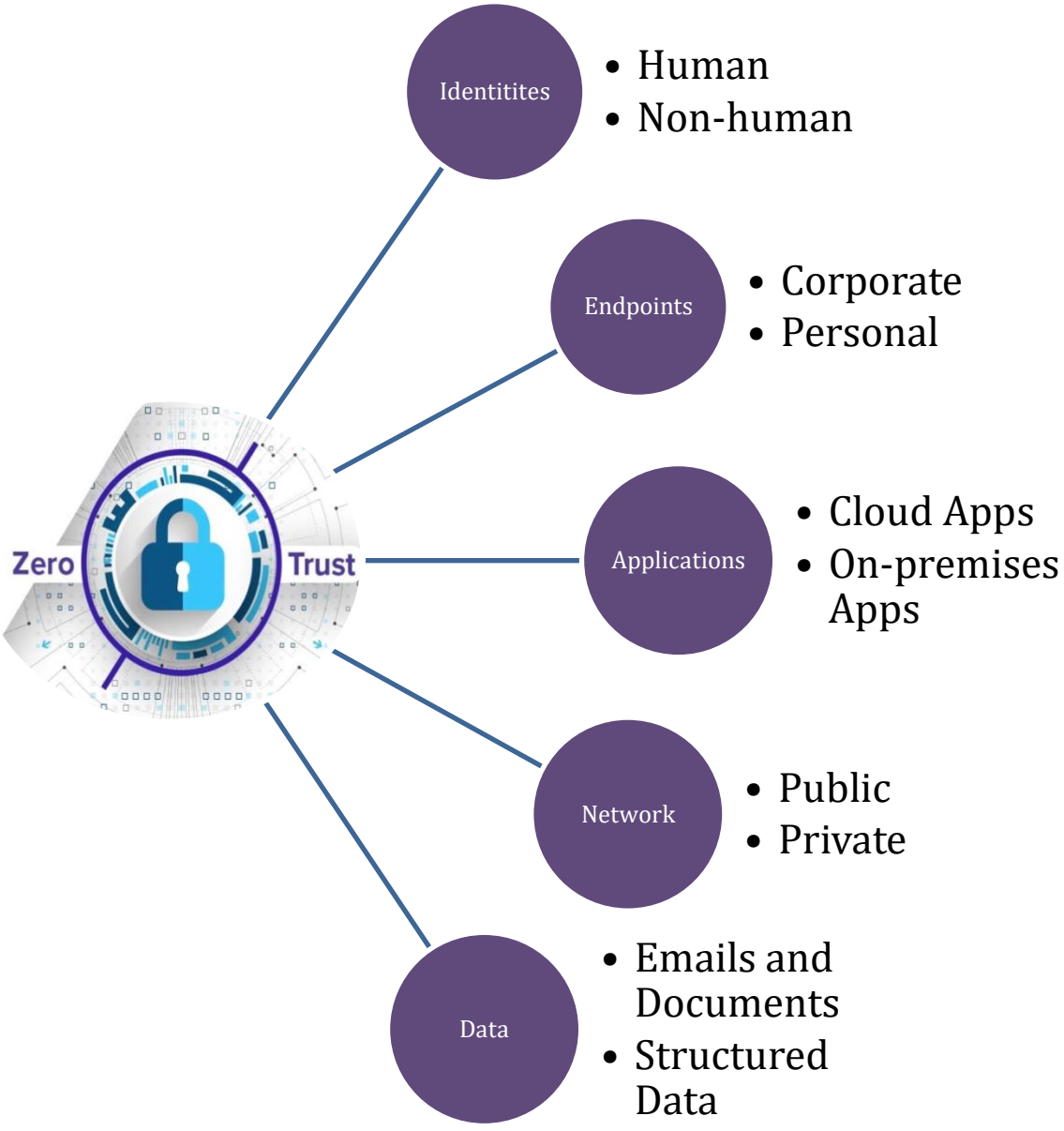


Figure 1: Zero Trust Architecture

Based on the Zero Trust Architecture as above, the implementation of the Zero Trust Model can be staged to a timeline as follows.

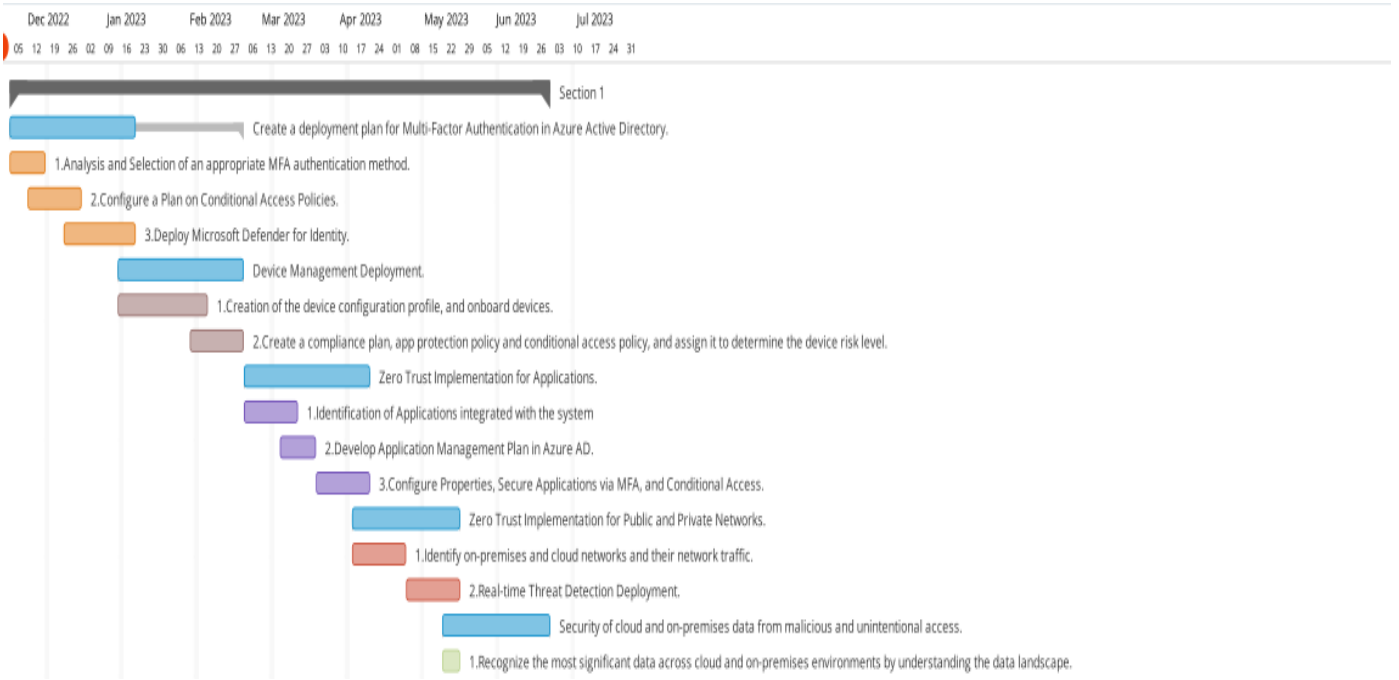


Figure 2: Zero Trust Model Implementation Plan

Project Phase	Milestone	Deliverables
Create a deployment plan for Multi-Factor Authentication in Azure Active Directory.	1. Analysis and Selection of an appropriate MFA authentication method. 2. Configure a Plan on Conditional Access Policies. 3. Deploy Microsoft Defender for Identity.	System Implementation developed with Multi-Factor Authentication for explicit verification of Identities.
Device Management Deployment.	1. Creation of the device configuration profile, and onboard devices. 2. Create a compliance plan, app protection policy and conditional access policy, and assign it to determine the device risk level.	System with device configuration profiles and explicit verification of devices.
Zero Trust Implementation for Applications.	1. Identification of Applications integrated with the system a. Pre-integrated applications b. Your own applications c. On-premises applications 2. Develop Application Management Plan in Azure AD. 3. Configure Properties, Secure Applications via MFA, and Conditional Access.	System of explicit verification of all types of integrated applications.
Zero Trust Implementation for Public and Private Networks.	1. Identify on-premises and cloud networks and their network traffic. 2. Real-time Threat Detection Deployment. a. On-premises traffic →MS Defender for Endpoint	System of explicit verification of both cloud and on-premises networks.

	b. Cloud traffic → Azure Firewall threat intelligence-based filtering	
Security of cloud and on-premises data from malicious and unintentional access.	1. Recognize the most significant data across cloud and on-premises environments by understanding the data landscape. 2. Applying sensitivity labels related to protection activities like encryption, access limits, and more can help to safeguard sensitive data throughout its lifecycle. 3. To monitor, stop, and correct dangerous activities involving sensitive data, implement a uniform set of data loss prevention (DLP) policies across the cloud, on-premises systems, and endpoints. 4. Apply minimal permissions that specify who has access to data and what they are permitted to do with it in order to satisfy business and productivity needs.	Explicit verification system of data associated within the organization.

Table 1: Zero Trust Model Implementation Methodology

5. Proposed Solution

Based on the principal “never trust, always verify”, Zero Trust Model needs to be embraced by organizations for real-time detection and reaction to anomalies.

> “The mandate emerged for a Zero Trust approach to verify and secure every identity, validate device health, enforce least privilege, and capture and analyze telemetry to better understand and secure the digital environment.”

‘Evolving Zero Trust’, November 2021, *Microsoft*

Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT

Adhering to the three main principals:

1. Verify explicitly
2. Use least privileged access
3. Assume breach

Zero Trust controls and technologies are implemented within the organization across five fundamental aspects. Each of these is a signal source, an enforcement control plane, and a vital resource that needs to be protected.

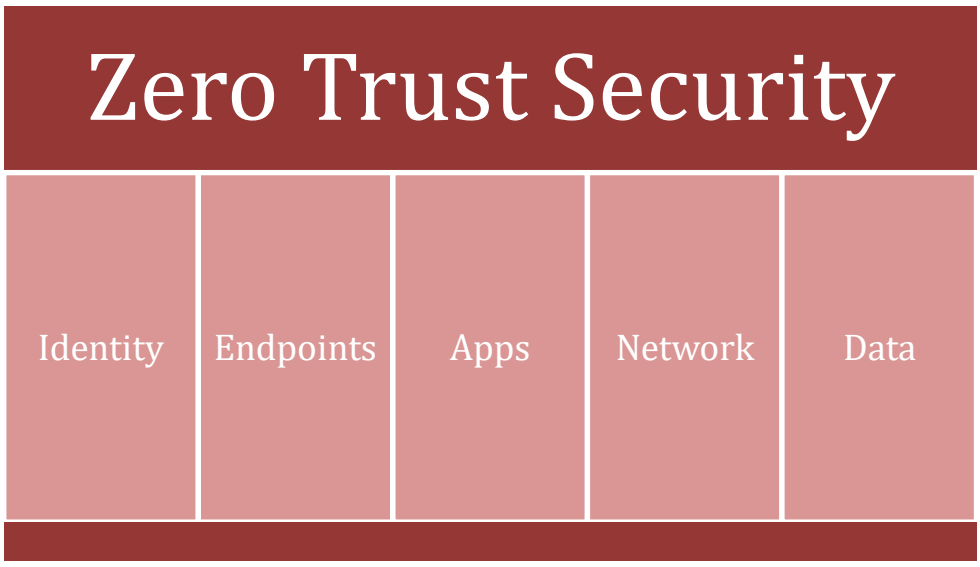


Figure 3: Foundational Elements of Zero Trust Model

The Zero Trust model assumes breach and verifies each request as though it came from an uncontrolled network, as opposed to thinking that everything behind the company firewall is secure.

The way a Zero Trust security model implementation is planned is influenced by various organizational requirements, existing technology implementations, and security stages. The Zero Trust Model will be developed in accordance with these specific needs and to assist clients in securing their business.

5.1 Suggested Starting Point

Zero Trust equips corporate networks to counter both known and undiscovered cyberthreats. Considering the proper precautions to avoid any sensitive data leaks, implementing a Zero Trust security model wouldn’t necessarily be incredibly difficult.

Initial stages of implementation of the Zero Trust Model can be categorized as follows:

1. **Recognition of the areas that need to be protected.**

   Company networks are dynamic, ever-expanding entities that are challenging to comprehensively define, control, or safeguard. Instead of mapping out the entire network, initially it should be figured out what and where the most protected Data, Applications, Assets, and Services are. The first step toward Zero Trust is to outline this "Protect Surface."

2. **Understanding how the network's apps interact.**

   Observe and document the interactions between particular applications. this would be helpful to obtain a true understanding of where restrictions are required. Knowing how the systems operate can help determine where access controls are needed.

3. **Outline of the Zero Trust architecture.**

   Since networks are not universal, it will be possible to sketch out the architecture of the Zero Trust framework while mapping the Protect Surface of the network. The next step is to include security controls to restrict access to vital network areas.

6. Discussion

No company can completely avoid cybersecurity risk. Zero Trust Architecture can lessen total risk exposure and defend against common threats when used in conjunction with current cybersecurity policies and guidelines, identity and access management, continuous monitoring, and basic cyber hygiene. When a Zero Trust Architecture is used, some threats have peculiar characteristics.

1. **Denial-of-Service or Network Disruption**

Millions of internet customers experience service interruptions as a result of huge DoS attacks launched by botnets like Mirai targeting important internet service providers. Additionally, it's conceivable for an attacker to snoop on and stop traffic coming from some or all the user accounts inside of an organization. Only a small percentage of enterprise users are impacted in such situations.

Both SaaS and infrastructure as a service in the cloud have already been disrupted. If the policy engine or policy administrator component is not reachable across the network, an operational issue could prohibit the entire organization from operating.

2. **Stolen Credentials / Insider Threats**

To gain the login information for valued accounts, attackers may use phishing, social engineering, or a mix of techniques. Accounts with access to banking or payment resources, for instance, may be equally desirable to attackers seeking financial gain as corporate administrator accounts. The risk of access from a hacked account may be decreased by using MFA for network access. A malevolent insider or an attacker with legitimate credentials may still be able to access the resources for which the account has been given access, just like in traditional companies. An employee database might still be accessible to an attacker or compromised employee who has the credentials and an enterprise-owned asset of a legitimate human resources worker.

3. Storage of Network Information

The analysis component itself poses a hazard to business network traffic analysis. Attackers can target network traffic and information if they are being saved for the purpose of developing contextual policy, forensics, or future study. These materials should be safeguarded just as network designs, configuration files, and other varying network architectural documents. An attacker might be able to understand the network architecture and pinpoint assets for additional reconnaissance and assault if they can successfully access stored traffic data.

4. Reliance on Proprietary Data Formats

Zero Trust Architecture uses a variety of data sources to make access decisions, including information about the user who requested access, the asset in question, enterprise and outside intelligence, and threat analysis. Frequently, however, the assets used to store and process this data lack a common, open standard for information exchange. Due to interoperability problems, this may cause a business to become tied into a specific group of providers. A company might not be able to switch to a different provider without incurring significant costs or going through a protracted transition program if one supplier has a security problem or disruption.

7. References / Bibliography

1. ‘Embrace proactive security with Zero Trust’, *Microsoft Security* < https://www.microsoft.com/en-ww/security/business/zero-trust>

2. ‘Zero Trust Guidance Centre’, *Microsoft | Learn*, < https://learn.microsoft.com/en-us/security/zero-trust/>

3. ‘Zero Trust Rapid Modernization Plan’, *Microsoft | Learn*, < https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview>

4. ‘How to start Implementing the Zero Trust Model’, 4th November 2021, *NordLayer*, < https://nordlayer.com/blog/how-to-implement-zero-trust/>

5. Scott W. Rose, Oliver Borchert, Stu Mitchell, Sean Connelly | National Institute of Standards and Technology (August 2020) | ‘Zero Trust Architecture’

   Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

6. Microsoft (November 2021) | ‘Evolving Zero Trust’
   Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT

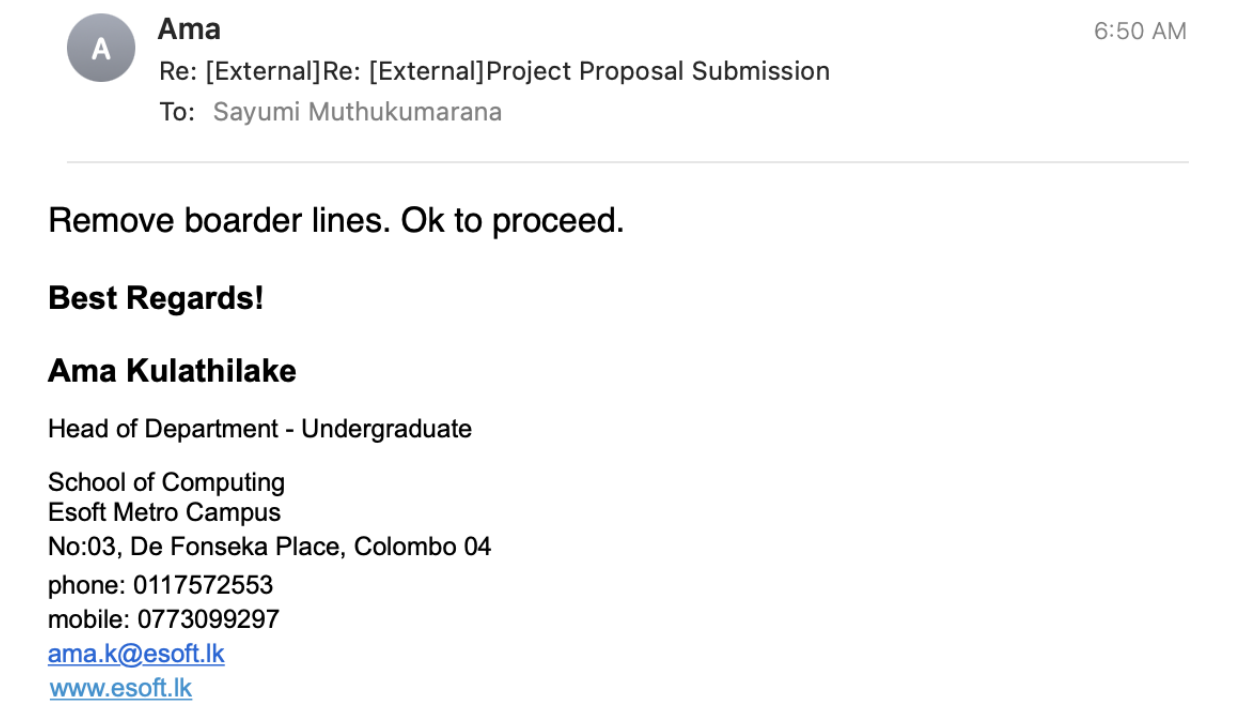
Appendices

Appendix A: Zero Trust Architecture Components

Security Pillar	Definition
Identities	Identities—whether they represent people, workloads, endpoints, or IoT devices—define the Zero Trust control plane. When an identity attempts to access a resource, we need to verify that identity with strong authentication and ensure access is compliant and typical for that identity and follows least privilege access principles.
Endpoints	Once an identity has been granted access to a resource, data can flow to a variety of different devices—from IoT devices to smartphones, BYOD to partner managed devices, and on-premises workloads to cloud hosted servers. This diversity creates a massive attack surface area, requiring we monitor and enforce device health and compliance for secure access.
Networks	All data is ultimately accessed over network infrastructure. Networking controls can provide critical "in pipe" controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in-network micro segmentation) and real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.
Applications	Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lift-and-shifted to cloud workloads, or modern SaaS applications. Controls and technologies should be applied to discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control user actions, and validate secure configuration options.
Data	Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Data should be classified, labeled, and encrypted, and access restricted based on those attributes.
Infrastructure	Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services) represents a critical threat vector. Assess for version, configuration, and JIT access to harden defense, use telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.
Policy optimization	The organization-specific security policies applied throughout an organization's programs across the entire digital estate. The policies are optimized for business processes, governance, compliance, and the end user experience.
Policy enforcement	The Zero Trust policy intercepts the request, and explicitly verifies signals from all 6 foundational elements based on policy configuration and enforces least privileged access. Signals include the role of the user, location, device compliance, data sensitivity, application sensitivity and much more. In additional to telemetry and state information, the risk assessment from threat protection feeds into the policy to automatically respond to threats in real-time. Policy is enforced at the time of access and continuously evaluated throughout the session.
Threat protection	Telemetry and analytics from all the 6 foundational elements feeds into the threat protection system with our Zero Trust architecture. Large amounts of telemetry and analytics enriched by threat intelligent generates high quality risk assessments that can either be manually investigated or automated. The risk assessment feeds into the policy engine for real-time automated threat protection.

Microsoft (November 2021) | 'Evolving Zero Trust'
Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT

Approval from the Supervisor:



Ama 6:50 AM

Re: [External]Re: [External]Project Proposal Submission

To: Sayumi Muthukumarana

Remove boarder lines. Ok to proceed.

Best Regards!

Ama Kulathilake

Head of Department - Undergraduate

School of Computing
Esoft Metro Campus
No:03, De Fonseka Place, Colombo 04
phone: 0117572553
mobile: 0773099297
ama.k@esoft.lk
www.esoft.lk