NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ZERO TRUST ARCHITECTURE IMPLEMENTATION FOR THE MARINE CORPS TACTICAL CLOUD

by

Dane M. Oshiro

September 2023

Thesis Advisor: Alan B. Shaffer
Co-Advisor: Gurminder Singh

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
ZERO TRUST ARCHITECTURE IMPLEMENTATION FOR THE MARINE CORPS TACTICAL CLOUD

5. FUNDING NUMBERS

6. AUTHOR(S) Dane M. Oshiro

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

A critical knowledge gap exists in the Department of Defense (DOD) zero trust architecture (ZTA) implementation strategy. The majority of published academic research and technical documentation focuses on maturing zero trust (ZT) capabilities for enterprise networks without any detailed analysis on identifying risks that commanders and troops at the tactical edge will face. Laminating enterprise ZTA solutions to the tactical edge without first adapting technologies, system models, and policies to operate in a denied, degraded, intermittent, or latent (DDIL) networking environment could lead to severe mission consequences. This thesis proposes a tactical ZTA (TZTA) framework that expands on existing DOD ZTA reference architecture. Additional components and features are defined to meet the dynamic network conditions at the tactical edge. These components integrate legacy devices into a TZTA and identify suitable interfaces for federation between ZTAs. Supplementary features of these components enable identity and application federation, device attestation, weapon systems employment, and comprehensive IDS coverage within the architecture. Future implementation and testing of the proposed framework will lead to identification of suitable technologies and models using quantitative analysis to form the technical basis for future acquisition strategies that guide the DOD's transition to ZTA in both enterprise and tactical environments.

14. SUBJECT TERMS
zero trust architecture, Marine Corps, tactical cloud

15. NUMBER OF PAGES
85

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ZERO TRUST ARCHITECTURE IMPLEMENTATION FOR THE MARINE CORPS TACTICAL CLOUD

Dane M. Oshiro
Captain, United States Marine Corps
BS, United States Naval Academy, 2015

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2023

Approved by: Alan B. Shaffer
Advisor

Gurminder Singh
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A critical knowledge gap exists in the Department of Defense (DOD) zero trust architecture (ZTA) implementation strategy. The majority of published academic research and technical documentation focuses on maturing zero trust (ZT) capabilities for enterprise networks without any detailed analysis on identifying risks that commanders and troops at the tactical edge will face. Laminating enterprise ZTA solutions to the tactical edge without first adapting technologies, system models, and policies to operate in a denied, degraded, intermittent, or latent (DDIL) networking environment could lead to severe mission consequences. This thesis proposes a tactical ZTA (TZTA) framework that expands on existing DOD ZTA reference architecture. Additional components and features are defined to meet the dynamic network conditions at the tactical edge. These components integrate legacy devices into a TZTA and identify suitable interfaces for federation between ZTAs. Supplementary features of these components enable identity and application federation, device attestation, weapon systems employment, and comprehensive IDS coverage within the architecture. Future implementation and testing of the proposed framework will lead to identification of suitable technologies and models using quantitative analysis to form the technical basis for future acquisition strategies that guide the DOD's transition to ZTA in both enterprise and tactical environments.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A2/AD	Anti-Access/Area-Denial
CAC	Common Access Card
CENTRIXS	Combined Enterprise Regional Information Exchange System
CRAFT	Continuous Remote Attestation Framework for IoT
CSI	Channel State Information
CSP	Credential Service Provider
D2D	Device to Device Authentication
D3A	Decide, Detect, Deliver, Assess
DDIL	Denied, Degraded, Intermittent and/or Latent
DevSecOps	Develop, Security, and Operations
DNS	Domain Name Service
DOD	Department of Defense
DoS	Denial of Service
EABO	Expeditionary Advance Base Operations
EZTA	Enterprise Zero Trust Architecture
GPS	Global Positioning System
ICS	Industrial Control System
IDS	Intrusion Detection System
IoBT	Internet-Of-Battlefield-Things
IoT	Internet-Of-Things
IPS	Intrusion Prevention System
LCDA	Lightweight Continuous Device to Device Authentication
LD	Legacy Device
LEG	Legacy Encapsulating Gateway
LIF	Legacy Interface Function
MANET	Mobile Ad Hoc Network
MFA	Multi-Factor Authentication

MPE	Mission Partner Environment
NIPR	Nonsecure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entities
PA	Policy Administrator
PAM	Privileged Access Management
PE	Policy Engine
PEP	Policy Enforcement Point
PIN	Personal Identification Number
SDN	Software Defined Network
SIEM	Security Incident and Event Management
SIPR	Secret Internet Protocol Router Network
SoA	Service Oriented Architecture
SUAS	Small Unmanned Aerial System
TEE	Trusted Execution Environment
TPM	Trusted Platform Model
TZTA	Tactical Zero Trust Architecture
US-AID	Unattended Scalable Attestation of IoT Devices
VPN	Virtual Private Networks
ZT	Zero Trust
ZTA	Zero Trust Architecture

ACKNOWLEDGMENTS

I would like to acknowledge the support of my thesis advisors for assisting me with the generation of this thesis. This thesis would not have been possible without the help from the Graduate Writing Center coaches as well.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Implementation of zero trust within the Department of Defense (DOD) rests on five tenets and seven pillars [1]. The five tenets are: (1) Assume a hostile environment, (2) Presume breach, (3) Never trust, always verify, (4) Scrutinize explicitly, and (5) Apply unified analytics. These tenets set the basis for DOD zero trust architecture (ZTA). The seven pillars based upon these tenets provide key focus areas for implementation of ZTA spanning several categories. The seven pillars are: (1) User, (2) Device, (3) Network/ Environment, (4) Application and Workload, (5) Data, (6) Visibility and Analytics, and (7) Automation and Orchestration. Based on these tenets and pillars of implementation, this thesis contextualizes a ZTA suitable for ground-based tactical cloud operations.

The five tenets describe a high-level overview of what drives ZTA. Assuming a hostile environment and presuming a breach has or will occur, the focus of security shifts from the perimeter to end devices, users, and data. Operating under the assumption that adversaries have access behind firewalls requires security architects to develop additional measures to mitigate risks against these threats. These measures are based upon authentication and access control principles impacting users and devices. Every asset on the network is untrusted and requires a thorough authentication scheme in which access control is enforced. Actions in a zero trust environment are logged through granular access control mechanisms and can be scrutinized via unified analytics to determine abnormal behavior. Continuous authentication and granular access control bolster security measures responsive to dynamic operational environments.

The seven pillars provide the framework for how zero trust can be implemented in an existing operational architecture. Within the user pillar, the concept of privileged access management complements existing traditional authentication and authorization security measures. Users are given limited access to resources within the environment based on operational and/or mission requirements. The heterogenous mix of devices that enable kill-webs (resilient and dynamic systems that integrate kill chains across the joint force [2]) offer varying levels of security measures, thus a ZTA requires access control measures that perform identification, authentication, and authorization whenever any of these devices is

used. Continuous monitoring of devices and the ability to isolate them are essential for implementation as well.

The tactical edge is a highly dynamic environment, and a variety of networks are employed to support its communication and data sharing needs. Connections to sensors, shooting platforms, and command and control nodes are non-persistent. Inconsistent policies applied to these devices can create a porous security environment if devices become compromised from malicious actors. Network segmentation efforts at the macro and micro level protect against adversarial lateral movement within the system. Controlling privileged access within ZTAs shore up these vulnerabilities as well.

Comprehensive analytics and intelligent policy orchestration are the final elements to completing ZTA implementation. Monitoring systems provide real-time data on network activity. Robust user activity collection capabilities are necessary for generating policies within a ZTA. Detection of anomalous traffic and user activity triggers events where a policy orchestrator may restrict certain behaviors in the tactical edge ZTA.

A holistic implementation of zero trust will be a large step forward in hardening kill-webs at the tactical edge. An ideal zero trust framework at the tactical edge will provide commanders with a resilient network that is capable of handling incursions without taking all cloud services offline. Prior to the realization of ZTA at the tactical edge, the challenge of continuous authentication and identity management of users and devices in a denied, degraded, intermittent and/or latent (DDIL) network environment must be overcome. This thesis investigates the applicability of various continuous authentication and identity management solutions for ZTA at the tactical edge.

A. RESEARCH QUESTIONS

This research explores the challenges of implementing a ZTA framework at the tactical edge. The following questions are addressed in this research:

1. What are the key components of a ZTA suitable for the tactical edge?
2. How do users, devices, weapon systems, applications, and security services interact within a ZTA implementation at the tactical edge?

B. KEY FINDINGS

This work proposed a ZTA architecture suitable for the tactical edge based on requirements generated from STRIDE threat-based modeling [3]. The framework contains components that reflect an enterprise ZTA solution such as the policy engine, policy administrator, and policy enforcement points. Enterprise, tactical, and legacy gateways were introduced to address the unique challenges of deployment at the tactical edge. This research explored features that should be included to effectively support users, devices, weapon system employment procedures, applications, and security services at the tactical edge. These features enable identity and application federation, device attestation within the internet-of-battlefield-things (IoBT), and a comprehensive solution for IDS (intrusion detection system) deployment in constrained networks.

This thesis also identified additional avenues for research in the field of tactical ZTAs. Future research on implementation and testing of the proposed tactical ZTA components supports technical analysis of these components in a tactical environment. Researchers familiar with administering networks alongside coalition partners could expand on the topic of tactical ZTA federation in a coalition environment. Further surveys on network architecture will identify appropriate methods of incorporating emerging technologies such as software defined networking, fifth generation networking architecture, and mobile ad-hoc networks. Finally, further analysis of blockchain applicability in a tactical ZTA for user authentication, identity and application federation, or device attestation is warranted.

C. SCOPE

This thesis identifies key considerations for ZTA implementation at the tactical edge in relation to continuous authentication, identity and application federation, device attestation, and IDS deployment. Architectural features that address these topics are evaluated, but are not implemented or tested in this research.

D. BENEFITS OF STUDY

A properly implemented ZTA hardens the security of tactical networks. Since trust is not implicit in ZTA, adversaries within the network must evade authentication mechanisms that protect data and services. In addition to safeguarding data, ZTAs preserve operational tempo in the event of a confirmed breach. Within a defense-in-depth security paradigm, entire network enclaves or essential applications need to be taken offline to prevent further exploitation [4]. One of the benefits of a ZTA is that it preserves unaffected segments and applications within the network. This allows system administrators to focus on isolation and removal of malicious actors, while warfighters continue the fight.

E. ORGANIZATION OF THESIS

Chapter II contains an in-depth discussion of the principles of ZTA outlined in [1]. Chapter III proposes an architecture for a ZTA implementation at the tactical edge. Chapter IV analyzes how users, devices, weapon systems, services and security interact with the proposed architecture. Chapter V summarizes research, draws conclusions, and lists further avenues for research.

II. BACKGROUND

This chapter reviews the fundamental concepts of ZTA and related research area topics. Guiding principles of ZTA [5] are introduced in accordance with current DOD cybersecurity policies derived from the reference architecture described in [1]. The core of ZTA implementation at the tactical edge rests on the employment of continuous authentication mechanisms. The importance of continuous authentication at the tactical edge will be revealed after the principles of ZTA are discussed. Application of these mechanisms at the tactical edge requires additional considerations that are explored in this chapter as well. Finally, an overview of the U.S. Marine Corps tactical cloud will be used to identify the problem areas that this research addresses.

A. PRINCIPLES OF ZERO TRUST ARCHITECTURE

Implementation of zero trust within the DOD rests on five tenets derived from zero trust principles and seven pillars that provide the framework for implementation. Contrary to the traditional security paradigm that focuses on perimeter security of a system, where implicit trust within the perimeter grants access to all objects that are available to the subject based on credentials used to enter the perimeter, ZTA provides resiliency to interior components in the event of a breach. Zero trust implements mechanisms that force subjects to continuously reauthenticate themselves as they attempt to access resources within the system.

1. Tenets of Zero Trust Architecture

The tenets of zero trust provide a high-level overview of what drives ZTA. These tenets are derived from concepts such as enforcing granular access control mechanisms and principles of least privilege, and in-depth logging and auditing of events and network traffic introduced by Kindervag and Balaouras in their seminal report introducing ZT more than a decade ago in [4].These concepts are references and expanded in ZTA implementation strategies. Instead of focusing on traditional security reference architectures that reinforce perimeter security of networks, ZTA centers on the protection of data contained within. the

zero trust tenets referenced in [1] include: 1) *Assume a Hostile Environment*; 2) *Presume Breach*; 3) *Never Trust, Always Verify*; 4) *Scrutinize Explicitly*; and, 5) A*pply Unified Analytics*.

Assume a Hostile Environment reflects the realities of the current operational cybersecurity environment in addition to the demands of information-age warfare. Traditional network boundaries no longer delineate areas of a network where sensitive information can or cannot be trusted. The reality of insider threats in an enterprise network and the presence of malicious integrated circuit technology from compromised supply chains require additional measures to protect data within the network. Users, assets, devices, network segments, and other non-person entities (NPEs) need to be treated as untrusted and must require sufficient authorization and authentication mechanisms.

Presume Breach sets a proactive security posture where information is secured from untrusted access. Security professionals operate on the assumption that unauthorized users are already on the network. Micro-segmentation and other granular resource access controls serve to mitigate the impact of a breached network. System administrators enforce and refine policies that scrutinizes access and authorization requests for resources complementing the segmented architecture. This cohesive effort serves to limit attack surfaces within the organization and reduce the consequences of a breached network.

Never Trust, Always Verify adheres to the foundational core of ZT – the principle of least privilege. Users, devices, applications, and services have explicitly defined resources accessible to them. These resources are assigned to users and NPEs based on their specific roles within their organization or information enterprise. For example, medical administrators have access to medical records but should not have access to payroll information. Access to a specific resource does not automatically give a user or NPE carte blanche for access to everything else on the system. Authorization for access is continuous and multifactor, utilizing various technical means. Various schemes implement continuous multifactor authentication (MFA) between users, users and NPEs, and between NPEs. These methods will be further examined in the chapter.

Scrutinize Explicitly introduces contextual decision-making for access and authorization. Multiple features derived from agents requesting resources to include analysis of behavior provide contextual information to establish confidence levels for access. These features include device information, historical behavioral data collected from users, or location information as mentioned in [6]. For example, if a Marine administrative clerk normally accesses 15–20 personnel records on a typical workday, a ZTA with contextual decision making would raise an alert should that Marine suddenly start accessing over a hundred records on the weekends and outside of normal duty hours. Abnormal behavior outside the scope of regular operations increases the potential that an agent has been compromised. The task of establishing baselines for "normal behavior" is covered in the final tenet regarding ZTA.

Apply Unified Analytics establishes the baseline for normal agent behavior in the enterprise. An agent is considered to be an entity within the heterogenous mix of users, devices, applications, and services within the ZTA. Auditing and logging all actions for each agent produces a vast trove of data. Analysis of this data from agents forms the foundation of each agent's baseline of behavior. Efficient storage of data and effective application of analytics requires a comprehensive solution bolstered by artificial intelligence. Within the broad field of artificial intelligence, machine learning can be used to effectively automate user and device authentication procedures as described in [7]. Machine learning algorithms can perform deep network packet analysis on web application firewalls as mentioned by Appelt et al. in [8]. Combining these analysis methods and more to a data lake of information gathered from agents within the enterprise provide security professionals with enhanced situational awareness of what is occurring on the network.

2. Pillars of Zero Trust Architecture

The ZTA pillars introduced in the National Institute of Standards and Technology (NIST) ZT reference architecture [1], provide the implementation framework for ZTA. The reference architecture for ZT rests on the controls developed to address each of these pillars: *Users; Devices; Applications and Workloads; Data; Network and Environment; Automation and Orchestration;* and *Visibility and Analytics.*

Users encompass all persons and NPEs on the enterprise. Identity controls for multifactor authentication (MFA) and privileged access management (PAM) incorporate most of the functions necessary to support ZT in this pillar. Most security conscious enterprise networks already incorporate some level of MFA within their organizations, which makes implementation of this pillar somewhat intuitive to security professionals within the network. The other important component of the *User* pillar deals with the management of privileged users within the enterprise. System administrators and other privileged roles need to be managed and audited in order to deter deliberate and unintentional malicious acts from these elevated accounts on the enterprise. This requires both policy measures and subsequent logging, analysis, and enforcement mechanisms in order to fully implement this pillar.

Devices are the assets that users and other NPEs interact with on the network. Like users, devices require continuous MFA mechanisms. Implementing a consistent and continuous MFA policy across an enterprise network that includes IoT devices present several challenges. Traditional user MFA comprises of the things a user knows (password), possess (one-time password), or is (biometrical analysis such as a fingerprint). Device MFA requires that the device be trusted through certificates or having some sort of trusted module within the device before access to resources are granted. The diverse mix of devices present on the enterprise means that there is a comparable number of MFA schemes specific to various device manufacturers. This presents quite the challenge for authentication engines in ZTA to perform their role. Analysis of the Mirai botnet conducted by Antokakis et al. in [9] presents the risks associated with IoT devices, especially devices without configurable security interfaces. Policies or technical controls such as network segmentation need to be implemented in order to best comply with the tenets of ZTA. Network segmentation that logically isolates sub-networks of devices that lack security interfaces is a method to achieve compliance.

Application and Workloads within a ZTA should be developed and deployed in accordance with Development Security Operations (DevSecOps) principles. Shifting the incorporation of ZT enforcement rules at the earliest stages possible in development and the automation of security testing provides development teams with the tools necessary to

identify and remediate security issues quickly. Security controls for applications should include enforcement points where ZT decisions can be applied. Logging and automated data tagging assist with ZT continuous authentication and inventorying of data. Workloads on virtual machines require similar granularity of enforcement mechanisms available for hypervisors to manage workloads with ZT. This means that the controls to manage hypervisors need to extend to the virtual machines as well.

Data is the chief resource in ZTA. Accurate data classification and tagging provides ZTA components with the necessary information to allow or restrict access to resources in the enterprise. Common data formats across multiple organizations within an enterprise significantly reduces the complexity for ZT enforcement. Data is encrypted at rest. Communication security should be implemented to protect data in transit. Data loss prevention (DLP) technologies also support this pillar of ZT implementation.

Network and Environments require granular segmentation to mitigate lateral malicious movement. Logical and physical segmentation controls should be leveraged to the maximum extent possible to manage data flow. One cost-effective method to perform granular network is through the establishment of software defined networks and software defined perimeters. In addition to segmentation of internal network, ZT needs to apply to remote connections to the internal network as well. Virtual private network technologies need to be able to support ZT authentication principles for users and devices accessing the network remotely.

Automation and Orchestration refers to the main enforcement mechanisms within ZTA. Manual security processes automated with the assistance of comprehensive and consistent security policies promote a responsive and dynamic defensive posture in an enterprise network. Integration of security information and event management (SIEM) and other tools such as intrusion detection system (IDS) or intrusion prevention system (IPS) and other tools such as IDS or IPS provides a robust framework to respond to a variety of threats to the network. SIEM helps administrators by managing the trove of logs and events occurring on the network to detect and respond to security events and provide insight to the overall security posture of the enterprise.

Visibility and Analytics leverages the massive trove of auditing and logging from ZT compliant users, services, and NPEs to provide a contextual visualization of things happening on the network. Application-level firewalls that perform deep packet scanning support contextual analysis of data flowing throughout the enterprise. Artificial intelligence and other machine learning applications employed in ZTA digest the massive trove of contextual information to inform administrators and monitoring systems of real-time anomalous behavior on the network.

3. Continuous Authentication in Zero Trust Architecture

The core of ZTA is in the employment of continuous authentication mechanisms within the enterprise. Traditional entry-point authentication and static access control measures are susceptible to data exploitation and exfiltration when trust is implicit in a certain network or environment. One-time authentication to allow access to sensitive system resources creates a single point of failure within the defense-in-depth security paradigm. Although sophisticated MFA applications raise the barrier to entry, they do not protect the enterprise from lateral movement within the boundary defenses. Continuous authentication is fundamentally different from Single-Sign-On as discussed in [10], which requires users to login once before accessing all resources within the network. Instead, continuous authentication mechanisms described by Abduwahid et al. in [11] verifies user authenticity through periodic or constant means transparent to a user. Continuous authentication can use biometric means, behavioral patterns, and physical features to authenticate with minimum interruption to user interaction.

Biometric means use the physiological traits of users, or modalities, to authenticate them. The top five most common modalities utilize the user's face, ear, fingerprint, palmprint, or iris [11]. Although biometric means of authentication have become increasingly common in mobile devices today, they only capture a subset of all devices that are employed on the battlefield. For example, remote-based sensors and unmanned shooting platforms lack the necessary user for authentication. Thus, other methods of authentication will need to be used.

Behavioral patterns are another means of continuous authentication. Aliomomeni and Safavi-Naini in [12] proposed that behavioral authentication patterns should be hard to delegate and hard to emulate, meaning that users should not be able to delegate their behavioral patterns to other users, nor should their patterns be easy to emulate after a period of observation. Several studies suggest that behavioral authentication can take the form of analyzing hand gestures, keystrokes, touchscreen manipulation, gait, signatures, voice, and other user activity actions on small form factor devices [13], [14]. Continuous authentication using behavioral patterns can be done with minimum disruptions to the operator. For example, Lee et al. in [15] demonstrated wearable sensors that could identify specific users with over 95% accuracy. The incorporation of behavioral patterns using wearable technologies could complement other continuous authentication methods to provide a solid foundation for continuous MFA across the tactical edge.

Physical means of continuous authentication apply to specific unique and inherent characteristics of a user or device in physical space. Location-based continuous authentication architectures as described in [16], [17] manage user sessions with access to specific resources based on their location. Sessions are terminated upon leaving a notional geographic fence. Full-stack location spoofing techniques described by He et al. in [18] can subvert geographic fences, requiring additional measures for authentication. These techniques range from using open-source software that can falsify global positioning system information to hacking directly into the global positioning system hardware modules on devices. Information can be falsified at the hardware level prior to being passed to the software accessing location data.

There are challenges associated with implementing location-based continuous authentication schemes, e.g., accurate and persistent Global Positioning System (GPS) is a requirement, which is not always possible for users and devices operating at the tactical edge in a DDIL environment. Near-peer adversaries possess capabilities that can disrupt and spoof GPS signals in a tactical environment as suggest in [19]. This promotes a potential vector for adversaries to pursue a denial-of-service (DoS) against previously authorized users and devices within the effective range of anti-GPS capabilities.

Other physical means for authentication described by Shah et al. in [20] include various device-to-device (D2D) authentication schemes based on analysis of radio signals captured by wireless network cards in devices. The protocol highlighted in [21] fingerprints devices using channel state information (CSI) obtained from wireless network cards. This protocol was shown to be computationally prohibitive for edge devices that must balance power consumption considerations with processing power, since swapping battery modules in remote and sensitive environments incurs significant operational risk.

Analysis of predicted and reported battery capacity values of sensors was proposed by Chuang et al. in [22]. A sensor or remote device would report its current battery capacity level to its respective gateway or server, where authentication of the device would be based on a comparison of predicted and reported battery levels on the gateway. The monotonically decreasing battery capacity values makes this scheme susceptible to adversaries inferring and spoofing the predicted and reported values.

Another method for using physical traits in D2D authentication by Shah et al. in [20] proposed the use of a Lightweight Continuous D2D Authentication (LDCA) protocol based on CSI without the computational cost attributed to the protocol described in [21]. LCDA is comprised of three distinct phases that initialize, mutually authenticate, and continuously authenticate devices. The initialization phase occurs in a secure space where identifier information is exchanged to set up the parameters for the subsequent mutual authentication phase between the two devices. The next phase seeks to mutually authenticate each device to the other prior to the exchange of protected data. Devices leverage CSI and a simple hash-based message authentication code generated from previous shared secret parameters determined from the initialization phase. Once mutually authenticated with one another, data exchange occurs.

Throughout the data exchange, authentication is achieved through a lightweight algorithm generated from previously exchanged information. Further tuning of algorithm parameters can decrease computational complexity, alleviating power consumption concerns described in [21]. Constriction of values used during the initialization phase can reduce key-sizes to 8-bits, reducing storage requirements. Although these characteristics lead to the lightweight nature of the protocol, Aman et al. points out in [23] the relationship

between the number of bits in a key with the security of the protocol. This highlights the importance of identifying risk acceptance between each component that fits their mission requirements.

The challenge of implementing continuous authentication in tactical environments need to address connectivity, power consumption, and storage considerations. The ability for a protocol or authentication scheme to address the limited processing power and intermittent connectivity found in the tactical environment will be the most important aspect of implementing continuous authentication in a tactical environment.

B. MARINE CORPS TACTICAL CLOUD OPERATIONAL ARCHITECTURE

This section explores the current enterprise computing framework employed by the Marine Corps at the tactical edge. Administrative, technical, and physical security controls facilitate Marine Corps tactical clouds and are implemented at varying levels within the service. Operating concepts such as Expeditionary Advance Base Operations (EABO) employed by the Marine Corps provides the necessary context to understand the challenges posed by ZTA implementation. Operating under the adversarial Anti-Access/Area Denial(A2/AD) umbrella requires additional considerations for planners. For example, signature management restricts external data pipelines for units operating in expeditionary advanced bases. Adversarial electro-magnetic sensing capabilities can detect a persistently connected expeditionary advanced base far easier than a base that is connected to external units intermittently throughout the day using low-probability of detection emitters. Additional factors stemming from an increased geographic distribution of forces as well as adversarial capabilities contribute to a denied, degraded, intermittent and/or latent (DDIL) environment. Non-persistent communication pathways and small-form-factor communication platforms are a small subset of challenges that will need to be addressed in a ZTA at the tactical edge. These factors challenge enterprise solutions for ZTA implementation.

1. Overview of Marine Corps Tactical Clouds

Marine Corps tactical clouds focus on the flow of information between the tactical edge and enterprise command and control nodes. These clouds are deployed along different classification enclaves, such as the Non-Secure Internet Protocol Routing (NIPR), Secure Internet Protocol Routing (SIPR), or Combined Enterprise Regional Information Exchange System (CENTRIXS). The tactical edge consists of warfighters using devices that require a smaller electro-magnetic footprint and rely on renewable energy or limited battery power. These requirements reflect the current operating environment, where adversarial A2/AD capabilities challenge the assumptions made in a traditional cybersecurity paradigm of defense-in-depth.

One of the key assumptions made in the defense-in-depth security paradigm is that trust is implicit inside the security perimeter. The Marine Corps uses network security devices to establish technical controls, such as firewalls, virtual private networks, web application firewalls, and network access control. Additional physical control measures that are used to enforce access control include manned security checkpoints within the command post, network enclaves that are air-gapped, and adequate security fencing. Once a user is authenticated in the network enclave, they are entrusted to all resources in accordance with role-based access control policies. Administrative controls that enforce identity management solutions are derived from thoroughly examined personnel manning documents. These manning documents dictate which personnel have physical access to computing and networking devices. This leaves all resources within the security perimeter susceptible to exploitation or data exfiltration if a malicious agent is able to gain physical access to the network.

Another assumption made in defense-in-depth is that authentication is only required once per session. Although session lengths can be limited to force user reauthentication, this can hinder warfighting tempo and efficiency, e.g., forcing a user to reauthenticate in the middle of coordinating a casualty evacuation is not an acceptable course of action for implementing continuous authentication. By making authentication a once-per-session requirement, resources become susceptible to replay attacks that can be used to hijack a legitimate session. Making continuous authentication between users, devices, and

resources transparent to operational requirements is a major goal in implementing ZTA at the tactical edge. The application of multifactor continuous authentication schemes will need to consider the diverse backdrop of users, assets, applications, and services that make up the informational landscape. A drone operator relying on satellite connectivity has a smaller portion of bandwidth resources to allocate towards MFA versus an intelligence analyst operating out of an operations center on a 100 gigabyte fiber optic connection. A centralized engine that generates policies and enforces them within the environment will need to accommodate all sorts of continuous authentication mechanisms and provide an accurate assignment of trust levels.

2. Challenges Facing ZTA in Marine Corps Tactical Clouds

The presence of A2/AD capabilities in current and future operating environments highlights the importance of maintaining a low signature footprint for kill web sensors and shooters. Offensive cyber capabilities of near-peer adversaries require a paradigm shift from traditional defense-in-depth security models to ZTA. The implementation of a ZTA at the tactical edge will require that solutions maintain a low signature while providing appropriate security measures to protect the confidentiality, integrity, and availability (i.e., the security) of network resources.

Maintaining a low signature will require ZTA implementations to maintain a lightweight profile in terms of power consumption and storage requirements. Power is consumed in these devices through two primary means – processing power, and communication overhead. Communication overhead for continuation authentication needs to be reduced to the maximum extent possible to provide adequate bandwidth and edge processing power for mission data requirements. Schemes that require a massive amount of processing power to generate keys, or that require persistent connections to maintain a "trusted" state need to be interpreted differently or discarded. For example, creating large keys or tokens using blockchain, as discussed by Hu in [24], carries considerable bandwidth and storage requirements which would not be practical for deployment at the tactical edge.

Operating in a DDIL environment creates additional uncertainty when performing continuous authentication. Burst transmissions and low probability-of-detection emission controls limit the amount of data that can be delivered from a device. As stated previously, incorporation of a lightweight continuous authentication scheme can optimize transmission links, further reducing risk to mission, while continuous authentication in an intermittent environment requires a decision on risk acceptance from the mission commander. ZTA implemented at the tactical edge will need to be flexible enough to accommodate sensitive communications that may not have the tactical bandwidth to authenticate in a continuous manner. This is not to say that authentication will not occur at all for sensitive devices placed far forward within the area of operations. Rather, an alternative method to ensure device authentication on a per session basis would need to be incorporated, ensuring that data, applications, and services that are connected to each transaction are protected through network micro-segmentation. Data tagging and further analysis of the data through machine learning applications can further verify authenticity of data transmitted from those devices.

The challenges facing Marine Corps ZTA implementation are numerous at the tactical edge. They differ significantly from problem sets currently being addressed at the enterprise level. Although the Marine Corps fights through its enterprise network, certain resources and assumptions held at the enterprise level do not apply to scenarios at the tactical edge. It will be necessary for continuous authentication mechanisms to be implemented at the tactical edge, not only for compliance but to reflect the evolving security threats faced at the tactical edge. These mechanisms will require a policy engine that is flexible and scalable to accommodate the wide array of networked devices, sensors and shooting platforms, and that will need to be able to derive information from this heterogenous mix of sources and deliver accurate decisions of trust levels.

C. CHAPTER SUMMARY

This chapter introduced the fundamental concepts of ZTA, including the five tenets and seven pillars as described in [1]. ZTA implementation at the tactical edge will need to address the challenge of continuous authentication. Although a wide variety of schemes

exist to address continuous authentication at the enterprise, not all of them will be applicable at the tactical edge. An overview of the Marine Corps tactical cloud operation provided the backdrop necessary to understand the challenges posed by ZTA implementation in this unique environment. The evolution of adversarial A2/AD capabilities amplify the importance of implementing ZTA at the tactical edge for assured command and control of forces within the battlespace. Finally, we provided an overview of the concept of a comprehensive continuous authentication policy engine to synthesize trust relationships between system users and devices. This is the fundamental issue that this thesis addresses.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ZTA FRAMEWORK AT THE TACTICAL EDGE

As introduced in the previous chapter, the tactical edge provides a variety of challenges that are not addressed by current ZTA implementation frameworks for enterprise systems. Requirements need to be identified to provide guidelines for developing the proposed ZTA framework for the tactical edge. This chapter seeks to introduce a flexible, scalable, and responsive lightweight ZTA framework that addresses the unique nature of tactical edge systems.

A. REQUIREMENTS FOR A ZTA FRAMEWORK AT THE TACTICAL EDGE

Prior to proposing a framework, requirements need to be identified to ensure overall framework effectiveness. One method to determine security focused requirements is to apply a set of similar threat categories found in threat-based modeling. A threat model approach incorporates a variety of methods that decompose system components and map a generalized set of threats to system components to objectively evaluate effectiveness of a framework. In a review of twelve threat-based models conducted by Rocchetto et al. and Shevchenko et al. [25], [26], the STRIDE methodology stood out as the most mature method in use today. STRIDE is a mnemonic-based methodology introduced by Kohnfelder and Garg [27] in 1999 that is still incorporated in Microsoft's software development life cycle today and has been applied to evaluating security controls of cyber physical systems in a recent study by Khan et al. [3]. Each letter in STRIDE is associated with a general category of cyber threat as described in Table 1, based on definitions gathered or interpreted from the National Institute of Standards and Technology (NIST) glossary [28].

Table 1. STRIDE Threat Categories. Sources: [28]–[32].

Threat Category	Description
Spoofing	An attempt to gain access to a system by posing as an authorized user [29].
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data [29].
Repudiation	The ability of a user or system to deny having performed a certain action or transaction [30].
Information disclosure	An event involving the exposure of information to entities not authorized access to the information [29].
Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided) [31].
Elevation of privilege	Techniques used to gain higher-level permissions on a system or network [32].

The primary advantage to using STRIDE over other threat-based modeling techniques is that it decomposes data flows within the system and evaluates each system component's ability to protect that data. This data-centric approach complements the central tenet of ZTAs, namely data security. ZTA is entirely focused on protecting data within the system, rather than focusing on defending system boundaries. This is the primary reason STRIDE threat categories will be used to generate ZTA framework requirements at the tactical edge.

It is necessary to consider how cyber threats change when considered in a tactical context. The Denied, Degraded, Intermittent, and/or Latent (DDIL) environment introduced in the previous chapter represents serious challenges for current military

networks. Simply extending enterprise services such as chat, email, or command and control (C2) over a persistent network connection to clients at the tactical edge is no longer an acceptable communications plan. Mission commanders at the tactical edge require a robust and resilient architecture to support their operations in a DDIL environment. Two security threat categories represented within the STRIDE model must be addressed in a ZTA implementation at the tactical edge: denial of service (DoS) and spoofing. Immediately following these concerns are the threats that impact the confidentiality of data at the tactical edge. Together, these concerns generate the basis for security requirements in a ZTA framework operating in a DDIL environment. We have defined the security requirements below to prioritize the threat categories within the STRIDE model:

1. Security Requirements for a ZTA Framework at the Tactical Edge

a. Security Requirement 1: The Framework Shall Guarantee Mission Critical Services Remain Operational in a DDIL Environment.

The primary security concern that a ZTA framework must face is the availability of services in a DDIL environment, which may require establishment of local policies to ensure delivery of services in a dynamic or isolated networking environment. If a tactical ZTA is unable to secure resources or provision critical services in a DDIL environment, the mission is put at risk. Some local mechanism to administer and enforce policies must be present within a tactical ZTA. Authentication schemes must also persist in a disconnected state, e.g., if an adversary jams the primary satellite communication link the ZTA must be able to authenticate and authorize local subjects and resources through alternate routing pathways. ZT policies should not preclude resource accessibility issues in a DDIL environment. Local means to authenticate requests and authorize access to resources available at the edge should remain accessible in a disconnected state with appropriate security mitigations implemented. Dynamic and scalable policies that work regardless of network connectivity should be developed prior to network deployment.

b. *Security Requirement 2: The Framework Shall Facilitate Granular Access Control Through Use of Continuous Multifactor Authentication (MFA) Mechanisms.*

Granular access control is a central tenet of a ZTA. Each resource (i.e., data object or service) within the network must be aligned with a policy governing access to it. Policy enforcement should rely on continuous MFA mechanisms that provide verification of a subject's identity for every session and transaction. Subjects are not limited to users on the network but NPEs as well (discussed in Chapter 2). Incorporation of a local Policy Engine (PE) and Policy Administrator (PA) facilitates continuous MFA in a disconnected or degraded environment. Despite the DDIL network environment, administrators retain their ability to manage local policies. The ability to manage local policies provides units with a responsive network that can adapt to a dynamic operating environment. An example of how a dynamic MFA scheme can enhance a mission would be if a battle watch officer lost a physical access token to log into the network. In a traditional security framework, there are no exceptions for that battle watch officer to use an alternate means to authenticate into the battle network. The unit can adjust policies to incorporate alternative means to authenticate the user or restrict available resources to that user in an un- or under-privileged state. The under-privileged watch officer could use a username and password to log into the system and use alternative means to attest his identity thorough a variety of contextual authentication mechanisms. The PE can use previously captured behavioral patterns such as keyboard typing signatures or biometric samples to authenticate the user and elevate their trust level throughout a probationary period before granting permanent access to resources. This process would allow the unit to continue to function with all available manpower to continue operations.

c. *Security Requirement 3: The Framework Shall Deploy a Robust Intrusion Detection System Capable of Capturing and Tagging Pertinent Metadata Within the Tactical Environment.*

A robust intrusion detection system (IDS) capable of logging is a critical security requirement within a ZTA. An IDS capable of recording all observed events within the environment can lead to further analysis for intelligent policy generation. An example of intelligent policy generation was proposed by Hosney et al. [33]. They implemented

policies that were generated using a decision tree algorithm to tune application firewalls using log data gathered from network resources. Tagging network metadata assists administrators with contextualized situational awareness. Maintaining a repository of logs within the PE and processing them locally can establish baselines of user and resource activity specific to the tactical network. Profiles of subjects and resources differ based on the operating environment. A user operating from a persistent connection will most likely not access the same services that require significant bandwidth, such as online video conferencing when operating in a DDIL environment, where they may opt for asynchronous communication using email or lightweight chat applications. Profiling of subjects and resources within the network aids in rapid detection of anomalous activity. If a user that is assigned to work during the daytime suddenly starts accessing different system resources during odd hours in the evening, the PE can immediately notify system administrators of suspicious or unusual activity. A robust logging and log processing capability at the tactical edge is essential to maintaining an aggressive security posture.

The STRIDE threat modeling methodology informs the three security requirements for a ZTA at the tactical edge. The first requirement addresses the DoS threat by establishing local policies that guarantee mission critical services remain operational in a DDIL environment. Spoofing, information disclosure, and elevation of privileges are mitigated in the second security requirement by implementing granular access control on resources in the network to prevent unauthorized information disclosure. The threat of privilege escalation is limited when granular access control rules are enforced. Users that produce and consume data will not be able to manage other resources in the system from the same account, nor should it be possible for them to elevate their privileges from a user role. Continuous authentication is a powerful tool for reducing the spoofing threat. By verifying the identity of a user at regular intervals, continuous authentication can help to protect against unauthorized accesses and data breaches. The third security requirement is met by the deployment of a robust IDS within the ZTA. Maintaining comprehensive logs that record events, activities, and transactions within the ZTA provides the PE with essential clues to baseline user and resource activities. A local IDS capable of processing locally-generated log repositories enables the architecture to adjust baselines to changes in

tactical operations in a disconnected environment. Together, these three requirements form the baseline level of security necessary in a ZTA at the tactical edge and cover the six threat categories introduced in the STRIDE model. Each of these requirements is mapped to an associated threat category in Table 2.

Table 2. Security Requirements Mapped to STRIDE Threat Categories

Threat Category(s) Addressed	Security Requirement
Denial of Service	**Security Requirement 1***:* The framework shall guarantee mission critical services remain operational in a DDIL environment.
Spoofing, Information disclosure, Elevation of privileges	**Security Requirement 2***:* The framework shall facilitate granular access control through use of continuous multifactor authentication (MFA) mechanisms.
Repudiation, Tampering	**Security Requirement 3***:* The framework shall deploy a robust intrusion detection system capable of capturing and tagging pertinent metadata within the tactical environment

2. Operational Requirements for a ZTA Framework at the Tactical Edge

In addition to the security requirements presented above, a tactical ZTA framework must also consider the following operational requirements proposed by the author:

a. Operational Requirement 1: The Framework Shall Be Able to Support Legacy Systems on the Network.

The diverse mix of sensor systems, shooting platforms, and other devices on a tactical network realistically will not use the same security measures to implement ZT authentication/authorization policies. The transition from the current cybersecurity

paradigm of defense-in-depth to a ZTA will be methodical in nature, requiring ZT security mechanisms to co-exist with legacy systems. A mix of policy and technological means employed within the transitional framework must maintain the core tenets of ZTA in a heterogenous system. Mission requirements will still need to be satisfied during migration to a ZTA, requiring ongoing technological or administrative means to protect resources on the network.

b. Operational Requirement 2: The Framework Shall Have an Ad-Hoc Capability Within the Joint and Coalition Networking Environment at the Tactical Edge.

Building resiliency into a ZTA framework is essential at the tactical edge, where availability of enterprise resources is not guaranteed. A framework must work whether it is connected to the enterprise environment or not. It should also be able to adapt to a dynamic ad-hoc environment. During an operation, adjacent networks and their resources might need to interconnect and users from adjacent networks may need to access local system resources based on mission requirements. An example of this is if a reconnaissance element needs to upload sensory data into a database that is located on the enterprise. A tactical ZTA that meets this operational requirement would enable reconnaissance elements to upload data quickly and securely to enterprise networks, even when they are not directly connected. This would ensure that critical intelligence is available to higher command formations during intermittent communication windows, while also allowing tactical edge reconnaissance elements to remain focused on their mission.

These security and operational requirements must be considered and integrated into any proposed ZTA framework at the tactical edge. Effective assimilation of these requirements addresses a large swath of security concerns and tactical considerations, providing a robust and resilient platform for a successful ZTA implementation at the tactical edge.

B. PROPOSED ZTA FRAMEWORK AT THE TACTICAL EDGE

Per the DOD ZTA reference architecture design, any ZTA framework must contain the same three logical components according to NIST ZT Reference Architecture: a Policy

Engine (PE), a Policy Administrator (PA), and one or more Policy Enforcement Points (PEP) [1]. Together, these components form the foundation for access control within the ZTA. Brief summaries of each component follow:

The Policy Engine (PE) is the component that performs access control decisions aligned with policies based on what a subject can request given the subject's quantitative level of trust assigned by a trust algorithm (TA). Levels of trust are determined based on a subject's role, requested resource classification, existing policies assigned to resources, and other contextual information associated with the subject, such as behavioral information. The PE uses the TA to assign trust levels to subjects within the architecture.

The Policy Administrator (PA) is the component that explicitly allows or denies resource access to subjects. The PA is the main interface between the PEP and the PE. Resource requests and subject attributes are gathered from the PEP, and authorization for each session or transaction is determined by the PA from the PE, to be enforced by the PEP.

A Policy Enforcement Point (PEP) is the main gateway between resources on the network and subjects. The PEP is responsible for enabling connections and requests to resources from the data plane of the architecture, whereas the PE and PA reside in the control plane. The separation of logical components between the control and data planes is necessary for framework scalability and flexibility from a managerial standpoint. When new resources are added to the network, an associated PEP should be added as well. There should only be one PE/PA in a specific environment and should have a hierarchical relationship between the enterprise and tact. This means that policies that govern access to resources residing in the parent domain are inherited at lower levels.

The proposed framework in Figure 1 is structured into two layers that represent the two ZTA deployment environments. The Enterprise ZTA (EZTA) hosts enterprise-level resources and subjects, whereas the Tactical ZTA (TZTA) hosts subjects and resources found at the tactical edge; the latter was our focus. The segmentation between the EZTA and TZTA reflects current DOD cloud computing strategies outlined by DISA [34]. The main distinction between the two architectures is the TZTA's ability to deploy into a

tactical environment that may not have a persistent connection to enterprise resources. The ability to continue to provision resources in accordance with the tactical ZTA requirements such as the principle of least privilege or continuous authentication, requires the same logical infrastructure to enact policies in a disconnected environment. The tactical PE and PA serve in the same capacity as the enterprise PE and PA with respect to the subjects and resources within the TZTA. The three main features of the ZTA framework are the legacy gateway, enterprise gateway, and tactical gateway, which are discussed next.

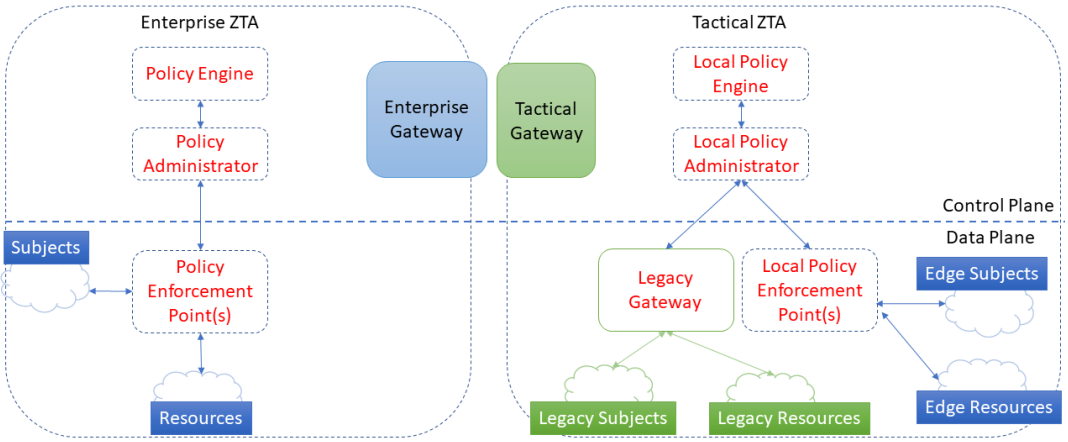

Figure 1. Zero Trust Architecture Framework at the Tactical Edge

1. Legacy Gateway

Legacy subjects and resources are mission critical entities in the tactical architecture that are technologically incompatible with ZT policy administration or enforcement. These devices or resources may not be able to enforce granular access control mechanisms or have the ability to deploy security patches. An example of a legacy device (LD) operating in a tactical network is a Small Unmanned Air System (SUAS) that does not have the ability to interface with a local PEP. Within the scope of this framework, the following assumptions are held for LDs:

- It is infeasible to replace LDs prior to TZTA deployment.
- Updates are unavailable for LDs to interface properly with PEPs.
- The LDs have appropriate authorization to connect privileges to the network with specific implementation guidelines that mitigate security risks to an acceptable level as determined by the mission commander.
- The LD resides in an untrusted domain.
- The LD lacks security measures that complement TZTA security tenets.

An architectural abstraction for industrial control systems (ICS) proposed by Geir Køien [35] is applicable to handling LDs within the TZTA. Køien's Legacy Component Architecture, shown in Figure 2, supports identity management, access control, and authentication functionality for LDs. The two major components within their proposed architecture are the Legacy Interface Function (LIF) and the Legacy Encapsulating Gateway (LEG). The LEG is integrated into the ZTA and manages identification, authentication, and fine-grained access control mechanisms with respect to one or more LIFs connected to it. Commands and requests to LDs are facilitated through individual connections with the LIF. The LIF will also be responsible for performing data validation functions for the LDs connected to it. The LEG performs the identification and access control mechanisms for any requests or commands directed at LDs. Policies are enforced at the LEG and commands are forwarded to devices through the LIF.

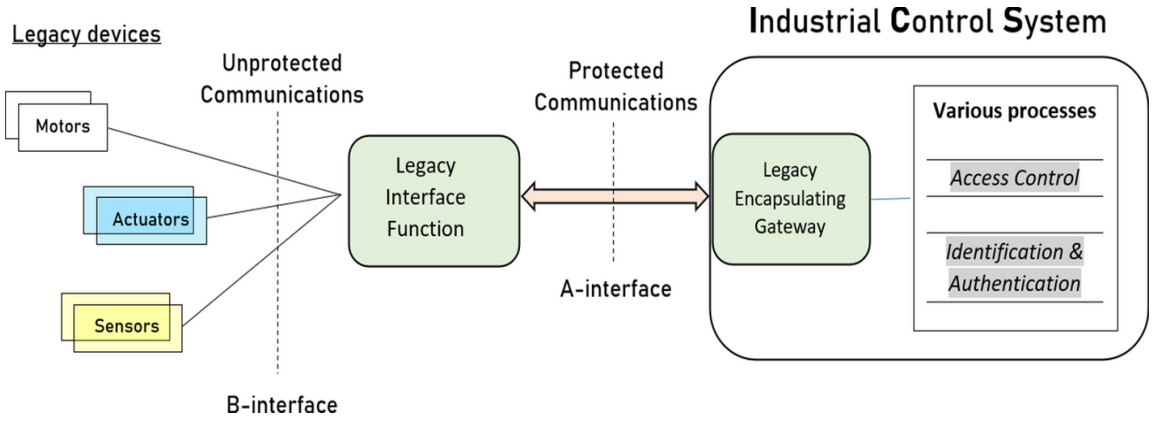

Figure 2. Køien's Legacy Component Architecture. Source: [35].

One way to improve upon Køien's architecture is to collapse the LEG and LIF into one device that can interface with both the TZTA and untrusted legacy domain. Combining the two reduces the requirement to develop a separate "A-interface" between the LEG and LIF. One method to combine them would be to implement a Trusted Execution Environment (TEE) solution that employs a separation kernel between untrusted and trusted communication. Sabt et al. described a separation kernel as the primary facilitator of concurrent operations with varying security requirements on a single platform [36]. The host system is divided into several secure partitions with a carefully managed interface for inter-partition communications. In addition to data requested and instructions to a LD that pass through the separation kernel, logs should be forwarded as well to the PA. One of these partitions would be responsible for establishing connections with the LD while the other partition is responsible for access control and authentication procedures. Logging information can provide valuable contextual information useful to providing LD attestation of trust. The Legacy Gateway is essentially a specialized PEP with a separation kernel facilitating communication with LDs. It will still receive policy guidance from the local PA. This tactical implementation is displayed in Figure 3.

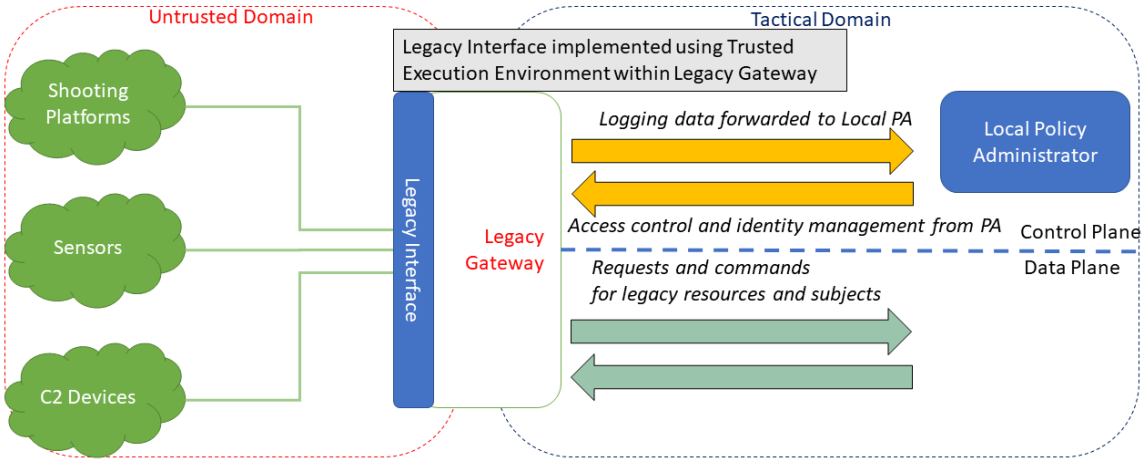

Figure 3. Legacy Component Architecture for the Tactical Environment

Collapsing the LEG and the LIF reduces the footprint required to support a TZTA; instead of using two devices to incorporate LD within the TZTA, only one device is needed. This smaller footprint decreases the physical signature of the architecture, reducing overall power consumption within a node, and ultimately benefiting operators at the tactical edge.

2. Enterprise Gateway

The enterprise gateway sits on the boundary of the EZTA and is responsible for interfacing with tactical gateways specific to each deployable TZTA. The enterprise gateway pulls relevant logging data from tactical PEs to inform policy development for enterprise agents that interact with tactical subjects and resources. The enterprise gateway will also provide updates to threat intelligence within the tactical architecture. Enterprise subjects and resources that interact with TZTAs need to satisfy policies that both the enterprise and tactical PEs generate. An example of this is if a trusted enterprise user is attempting to pull aircraft maintenance data that is stored on a database on a tactical network, that user will first have to be recognized as a trusted user from the enterprise PEP to access data stored on the tactical network. Rather than requiring the tactical PEP to authenticate enterprise users for access to tactical resources, the enterprise user will only need to authenticate with the enterprise PEP. Once authenticated, the enterprise gateway

will inform the tactical PE that the user meets authentication requirements to access tactical resources.

One method of communicating this trust between the enterprise and the tactical environment is through a token-based scheme that incorporates blockchain methods as prescribed by Hu [24]. The enterprise gateway is largely responsible for consolidating policies between tactical networks and the enterprise, ensuring the respective network logical components only evaluate trust for their subjects and resources.

3. Tactical Gateway

The tactical gateway is responsible for managing external connections from the TZTA to other TZTAs in an ad-hoc network setting and to its respective EZTA. The gateway serves as an intermediary proxy before requests are sent to the EZTA. If a local subject at the tactical edge does not possess adequate trust to access an enterprise resource, the tactical gateway can deny packets from leaving the external network, rather than submitting them to an EZTA PEP. The tactical gateway will function in a similar manner as a local Domain Name System (DNS) server, resolving policies for external requests within the architecture. The tactical gateway will have a caching function of policies from communication with the enterprise gateway. This will be especially useful in a degraded network environment, where the bandwidth available for external communication is severely limited.

The tactical gateway also houses the software defined network (SDN) controller for the tactical network. An SDN controller promotes maximum flexibility and scalability available to operators at the tactical edge. The SDN controller can dynamically allocate network resources respective to both entities within its prescribed network but also be able to handle mobile ad-hoc network establishment. This concept is explored by Poularakis et al. [37] in their discussion on SDN placement as close to the tactical edge as possible. Incorporating an SDN controller in the tactical gateway reduces latency in which policy updates are promulgated throughout network devices. This allows the network to adapt to a dynamic trust environment, where network devices could become compromised. In a disconnected environment, network operators or intelligent software will still have the

ability to adjust the network pathways without requiring a persistent connection to the enterprise controller. The responsiveness and flexibility within an SDN will also provide an ad-hoc capability to the tactical framework. A TZTA can dynamically adjust network pathways to reflect those currently available in a given operational environment. Should the primary connection between the TZTA and EZTA become compromised, network administrators at the tactical edge will have the ability to reconfigure network connections without significant downtime. The SDN controller within the tactical gateway provides a singular point of focus within the architecture where operators can manage the network infrastructure to tailor mission requirements.

An analogous architectural paradigm to the tactical environment is the security framework that governs Industry 4.0. Several components are shared between the two architectures, as referenced by Federici et al. [38], that include the vertical integration of a heterogenous mix of edge devices with corporate network infrastructure, and horizontal integration of third party service providers. A tactical architecture hosts a complex web of sensors, shooting platforms and other devices integrated into the enterprise that comprise the modern joint force kill-chain. In addition to dealing with third party service providers, a tactical network also needs to operate within a coalition environment with mission partners. The framework introduced in this thesis resembles components proposed by Federici et al., yet addresses the tactical considerations posed by the operational requirements previously listed. This framework satisfies the three security requirements by maintaining local PE/PA/PEP logical components that extend the ZTA at the tactical edge. Subjects residing in the tactical environment do not need to achieve authorization from the enterprise in order to access resources within the TZTA. If external network connections become denied or degraded, the tactical network will maintain its ability to enforce policies and have local means to authenticate and authorize, protecting resources and subjects at the edge. The inclusion of legacy PEPs at the tactical edge that complement authentication and authorization of legacy systems satisfies the second security requirement, in that it facilitates granular access control through the use of continuous multifactor authentication (MFA) mechanisms, ensuring subjects can access resources only after receiving explicit authorization to do so. All devices at the tactical edge feature robust logging components

in addition to setting up logging forwarding for LDs through the tactical gateway back to the local PE. The inclusion of the SDN controller in the tactical gateway provides operators with the means to establish ad-hoc networks with other TZTAs.

4. Chapter Summary

This chapter introduced the key security and operational requirements necessary for a ZTA implementation at the tactical edge. The security requirements were generated using the STRIDE methodology for model-based risk assessments. The security requirements address resource availability, access control, authentication mechanisms, and logging in a tactical environment. Operational requirements focus on incorporation of legacy battlefield systems and other partners such as adjacent units of coalition forces within the combat network to meet mission requirements. Both sets of requirements complement each other by ensuring that the framework provides a list of functional capabilities.

Incorporation of legacy systems within a ZTA protects legacy resources and enables other subjects and resources within the ZTA to interact with them in a secure manner. Inclusion of an SDN controller at the tactical gateway enables ad-hoc connections to other tactical SDNs, increasing overall resilience of the network in addition to providing additional pathways to communicate. The incorporation of the enterprise gateway, tactical gateway, and legacy gateway satisfies the framework requirements specified earlier. The proposed framework addresses all the requirements discussed in this chapter, and the next chapter will evaluate how well the framework can deliver on those requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS OF ZTA TACTICAL EDGE FRAMEWORK

This chapter explores how the proposed ZTA tactical edge framework interacts with users, devices, weapon systems, applications, and security services within the tactical environment. Understanding these interactions provides a comprehensive analysis of the effectiveness of the framework. Users are more mobile in a tactical environment versus an enterprise environment. Operations at the tactical edge will require user identity federation between disparate domains in joint and coalition operations. Today's battlefield is filled with networked devices, ranging from traditional personal computers to mobile devices, sensors, vehicles, and unmanned vehicles. An important subset of these networked devices is the variety of shooting platforms, such as the Switchblade loitering munition, Navy Marine Expeditionary Ship Interdiction System, or the M142 High Mobility Artillery Rocket System. Shooting platforms require additional levels of authentication through a separate targeting and fires process. Information flows are associated with the multitude of services available at the tactical edge. Security services that host intrusion detection systems are also deployed within ZTAs. These services form the basis of a unit's tactical cloud and should be available despite operating in a denied, degraded, intermittent and/or latent (DDIL) environment. Analyzing issues between users, devices, weapon systems, and information flows in such tactical environments illustrates how the framework could affect operational reliability and lethality of battlefield networks.

A. USERS AT THE TACTICAL EDGE

Implementation of the framework requires addressing challenges associated with user mobility and identity federation. These issues play a key role in shaping the effectiveness and efficiency of the framework within a tactical setting. These issues pertain to identity management within a mobile user base and establishment of an identity federation solution among disparate architectures. Identity management encompasses tasks such as: creation, identity proofing, provisioning, maintenance, identity aggregation, and deactivation of identities [39]. Although most of these functionalities are accomplished

through enterprise solutions, the tactical environment introduces several new considerations that need to be resolved.

Identity federation at the tactical edge leverages interoperability of information systems between mission partners in a joint or coalition environment. Mission partners from different federal agencies or from a multinational coalition may need to access and use resources from within a tactical network in order to accomplish mission objectives. Adversaries might have access to a mission partner's network, for instance, through a compromise in their supply chain[40]. An identity federation solution at the tactical edge should mitigate risks from partner federation to the maximum extent possible within a TZTA.

1. Mobile User Identity Management

A key difference between the tactical environment and enterprise environment is the lack of availability of enterprise resources for users at the tactical edge. User identities are created, proofed, and issued credentials in a controlled, enterprise environment from a credential service provider (CSP) [41]. These credentials are typically stored on a Common Access Card (CAC) or other token with an embedded certificate [41]. In a tactical environment, however, identity management services are limited to maintenance of identities, to include association of identities with certain access control policies. Applications deployed in the tactical environment should rely on MFA solutions to the maximum extent possible based on operational conditions [41], such as using a personal identifiable number (PIN) with a CAC. If a CAC is physically lost or a user forgets their PIN or associated password, administrators could reset authentication mechanisms using usernames and passwords in accordance with current guidelines listed in [41]. This weak form of authentication incurs several security risks to the tactical network. User names and passwords are the least secure form of authentication and are subject to adversarial compromise, as compared to other forms of authentication, as discussed in Jaspher et al. survey of user authentication schemes [42]. Therefore, a TZTA must implement strong multifactor continuous authentication schemes that can enroll users in a disconnected network environment.

A robust suite of biometric, behavioral, and physical authentication measures within the local policy engine can serve to bolster weaker authentication procedures, such as a username and password. Jin et al. proposed strengthening a username and password scheme with fingerprint data to encrypt passwords [43]. Capturing fingerprint data in a tactical environment has been prototyped by Das et al. [44], where they used wireless short range hubs to communicate with biometric sensors on an individual's body and then transmitted the biometric data via long range radios to communicate with authentication servers elsewhere. Incorporating these technologies within the local policy engine provides a resilient and responsive framework for managing a mobile user base regardless of connectivity to enterprise identity management infrastructure.

2. Identity Federation at the Tactical Edge

An identity federation scheme must be implemented within a TZTA to be interoperable with a mission partner environment (MPE). The MPE is the primary information sharing network between the DOD, other U.S. government agencies, and allied partners [40]. This federated network environment is applicable to tactical networks across the spectrum of military operations from low threat environments to major conflict. The joint task force that responded to the 2010 Haiti Earthquake served as the central information hub between various U.S. and international agencies, highlighting the importance of deploying a tactical network with the capability to share information rapidly between and among mission partners [45]. A critical component of the MPE is the implementation of an identity federation solution that permits users from various agencies and partners to access relevant data to the mission.

Incorporating a ZTA within the MPE presents a significant paradox between the two architectures. Whereas the MPE strives to maximize secure data interoperability among various partners and agencies through the federation of trusted domains, ZTAs strive to eliminate the concept of trusted domains. Strandell et al. highlights the increased attack surfaces of a ZTA when incorporated within a MPE network [46]. As more partners and agencies are incorporated within the MPE, the number of attack vectors increase as well. Their analysis showed that these risks undermine the benefits of ZTA federation,

since the overall security posture of the network can easily be compromised by the weakest partner within the MPE. Despite the seemingly contradictory tenets that guide ZTA and MPE, Hatakeyama et al. [47] suggested sharing contextual information derived from users, such as biometric, behavioral, or physical methods, to provide a means to verify user identities. The crux of incorporating identity federation within a TZTA is the development of a means to quantify trust between disparate domains.

Identity federation within the proposed TZTA framework is implemented within the tactical gateway, which is the main interface between one TZTA and other TZTAs. One way to improve upon Hatakeyama et al. ZT federation framework is to introduce an expanded trust evaluation, $\boldsymbol{T}$, based on a function of partner criticality, $\boldsymbol{C}$, historical reputation, $\boldsymbol{H}$, shared contextual metrics, $\boldsymbol{S}$, and cybersecurity posture, $\boldsymbol{P}$.

$$\boldsymbol{T = f(C, H, S, P)}$$

Each of these variables is adapted from the political, operational, economic, and technical factors used to develop the accessibility metric that Calhoun et al. used to analyze coalition information sharing environments [48]. Each of these variables can be understood as:

- Partner Criticality ($\boldsymbol{C}$) is a function of the operational impact of a partner for mission accomplishment, and sensitivity of information required for partner's respective mission accomplishment.

- Historical Reputation ($\boldsymbol{H}$) is a function of information sharing agreements, existing standard operating procedures for information sharing, and status of diplomatic relationship.

- Shared Contextual Metrics ($\boldsymbol{S}$) is a function of the number of shared user contextual metrics that are used for authentication.

- Cybersecurity Posture ($\boldsymbol{P}$) is a function of partner's known system vulnerabilities, patch and update frequency, information assurance requirements, and strength of authentication scheme.

The main objective of the function is to maximize trust between partners. The amount of trust a partner has in another determines the amount of trust implicitly given to external partners attempting to access a partner's protected resources. Trust between domains is subject to:

- $\boldsymbol{C} \leq$ criticality of a partner in order to accomplish mission
- $\boldsymbol{H} \geq$ historical reputation between partners
- $\boldsymbol{S} \geq$ shared user contextual metrics between partners
- $\boldsymbol{P} \geq$ cybersecurity posture of the partner's TZTA

Partner criticality, ***C***, refers to the operational impact of the partner as determined by the mission commander. An important aspect of this criticality is the sensitivity of information processed by the mission partner. Ensuring that partner criticality is determined by mission commanders establishes a hierarchical structure of mission partners, eliminating potential cyclic relationships between partners. Establishing clear roles of supporting and supported relationships between partners prevents confusion when determining which unit is more critical to mission accomplishment. Uniform data tagging and shared classification are necessary to determine how sensitive information is handled between each partner. Partner criticality acts as a weighted value to the three other variables of the trust evaluation ***T***. Criticality is an extension of the ZT principle of least privilege at the macro level, where the resources available to partners should be minimized as much as possible, in order to maximize trust between partners.

The historical reputation between partners, ***H***, considers existing information sharing agreements between partners, to include standard operating procedures for combined operations, and the state of diplomatic relations between the partners. Previous experiences in working with a partner can serve to build a positive or negative reputation, where system operators are familiar with capabilities and limitations of adjacent partner identity management procedures. Units from different services that routinely deploy and exercise with each other will have a higher historical reputation score than units that do not regularly train together. For example, U.S. Army units that routinely train and exercise

with the U.S. Marine Corps units will have a higher historical reputation score between them rather than an Army unit that does not have regular interactions with Marine Corps formations. A longer history of successful joint exercises and operations between DOD or coalition partners can result in an increased historical reputation score, as discussed in Calhoun et al. analysis of identity management in a joint and coalition information-sharing environment[48]. Higher historical reputation between partners increases the level of trust (***T***) between them.

An important parameter that captures the level of trust between partners is the shared user contextual metrics, ***S***, between them. Technological capabilities and privacy concerns can dictate the number of user contextual metrics used for authentication. Some partners may have privacy concerns when it comes to deploying keystroke analysis tools on their network [13], [49], [50]. Increasing the amount of shared user contextual metrics between partners increases the trust between them. Similar methodologies that capture user contextual actions enable partners' local policy engines to analyze user contextual information on their respective networks. For example, if one unit uses fingerprint biometrics, passwords, and X.509 certificates for authentication, while another unit uses X.509 certificates, keystroke analysis, and passwords; then the number of shared user contextual metrics between them are two. Each unit's tactical gateways can advertise their respective modes of user contextual information used for authentication within their TZTA, allowing other TZTAs to determine the level of trust required for federated users to access internal resources. Depending on the level of trust, a local PE may require a partner to enroll in additional authentication schemes or increase the frequency of authentication.

The cybersecurity posture, ***P***, is the final parameter used to evaluate trust between partners. A cumulative function adapted from Choi et al. proposed function that assigned vulnerability scores of critical infrastructure can be used to provide an objective determination of overall TZTA cybersecurity posture [51]. The cybersecurity posture could be evaluated from the number of known vulnerable services operating on a TZTA, the strength of authentication methods employed, physical and logical locations of a TZTA, and level of supply chain control of hardware and software deployed. Other critical components that dictate the cybersecurity posture include the frequency of system

patching, competency of the cybersecurity workforce, and information assurance requirements associated with the TZTA. Maximizing the cybersecurity posture of each TZTA maximizes the level of trust between two partners.

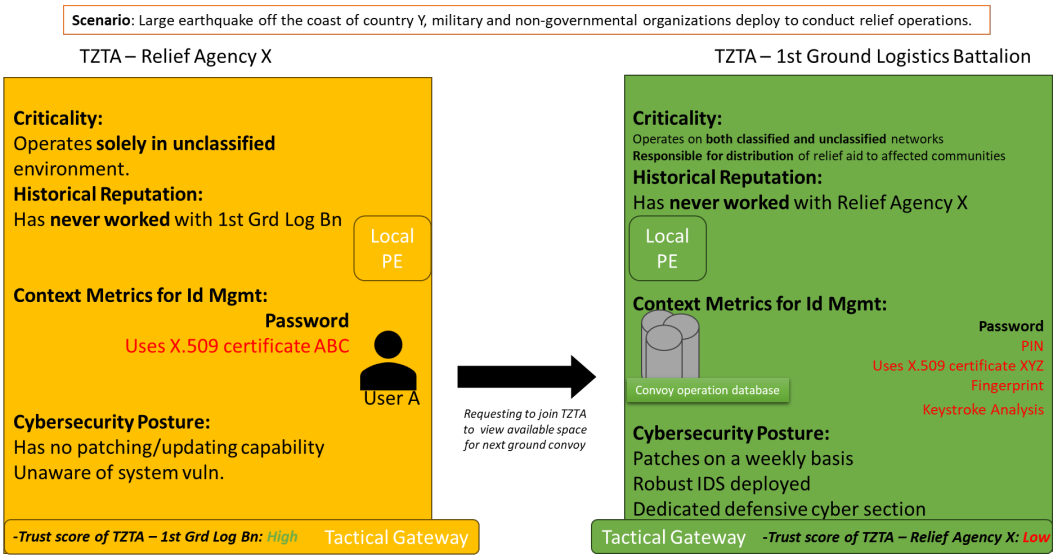

Figure 4. User Federation across Separate Tactical Zero Trust Architectures

Figure 4 demonstrates the process of evaluating trust in a scenario where federated users seek access to system resources across different TZTAs. The tactical gateways determine trust scores of adjacent TZTAs using the trust evaluation function. From the perspective of 1st Ground Logistics Battalion (1GLB), Relief Agency X (RAX) has a lower criticality score because 1GLB networks handle more sensitive data and support higher mission critical functions. Neither organization has worked with the other previously, resulting in a low historical reputation score. RAX shares a password contextual metric with 1GLB, but uses a different repository for certificates (ABC versus XYZ). Therefore, the shared user contextual metrics between the two organizations are one, which is low. The cybersecurity posture of 1GLB is significantly higher than that of RAX, which makes the cybersecurity posture of RAX lower than 1GLB. The resultant evaluation of 1GLBs trust score of RAX would be:

$$T(\text{RAX}) = f(C(low), H(low), S(low), P(low)$$

$$T(RAX) = low$$

Since the 1st Ground Logistics Battalion has a low trust score for Relief Agency X, its local policy engine may require that federated users from Relief Agency X authenticate more frequently when accessing the convoy operation database. Additionally, RAX User A might need to enroll in additional authentication mechanisms such as fingerprint or keystroke analysis. Ensuring that User A only has access to the convoy operation database necessary to see available space of convoys reduces the risk of User A abusing access and potentially compromising to 1st Ground Logistics Battalion's TZTA.

Focusing on a systematic approach to quantifying trust between TZTAs provides a dynamic and flexible framework for identity federation in a tactical environment. This systematic approach is just one method for identity federation management. Strandell et al. suggest a lightweight blockchain solution could be used to verify identities between two ZTAs. One proposed dynamic identity federation management scheme that uses blockchain is proposed by Alom et al. in their proposed architecture [52]. Although their proposed solution is optimized for security based on STRIDE threat modeling, Alom et al. did not compute storage or bandwidth requirements for a scaled deployment of their blockchain. A survey of blockchain identity management by Avellaneda et al. highlighted that all blockchain based identity federation solutions require a singular identity provider maintain connection to the blockchain network [53]. The necessity for a constant connection renders a blockchain solution unsuitable for a TZTA. The trust evaluation scheme is not specific to a singular identity provider and can operate in a disconnected environment. The proposed trust evaluation framework frees up storage, processing, and communication bandwidth resources for mission accomplishment rather than for identity federation.

B. DEVICES AT THE TACTICAL EDGE

The TZTA must accommodate the proliferation of networked devices at the tactical edge, ranging from personal computers, mobile devices, vehicles, unmanned vehicles, and

sensors [54]. Collectively, these interconnected devices are known as the internet-of-battlefield-things (IoBTs) [55], [56]. IoBTs assist with the execution of several warfighting functions such as: command and control, maneuver, logistics, intelligence, fires, force protection, and information [57] . Although their benefits are numerous, IoBTs expose a substantial attack surface that adversaries could potentially exploit to gain access to sensitive information and resources. Since IoBTs can be deployed from the rear, close, and deep battle areas [58], some nodes are very susceptible to being compromised by adversarial forces. Hartung et al. reported on the susceptibility of nodes to tampering by adversaries [59]. After physically obtaining the device or exploiting a vulnerability of the device, an adversary could potentially extract critical security information and gain access into the IoBT. Considering these risks, it is important for a TZTA to maximize the integrity of IoBT devices through device attestation, which is the process of devices authentication with their own identity to establish and maintain trust within a TZTA.

1. Device Attestation at the Tactical Edge

Device attestation can be accomplished through three different methods: hardware-based, software-based, or a combination of both [60], [61]. A hardware-based solution is generally the most secure solution, but is not applicable to legacy devices without certain components. For example, Johnston et al. recommended that bootstrapped device settings and configurations should be encrypted and signed by a private key contained by the trusted platform module (TPM) and verified by an authentication service using its respective public key [62]. A software-based scheme is the most flexible method of device attestation, but does not address hardware vulnerabilities that may be present on devices [63]. An example of a software attestation method was proposed by Seshadri et al., using a challenge-response mechanism [63]. Their method uses timing to determine the integrity of a device. This challenge-response scheme was improved by Schelleken et al. in their hybrid device attestation approach, where the TPM is used to time the checksum operation, and to validate hardware integrity of the device [64]. The primary limitation of this scheme is its lack of scalability. As more devices are added to the network, additional communication and processing overhead is incurred for device attestation. The increased overhead is not suitable for a tactical environment, which is defined by its tight

communication and processing constraints. Although a centralized solution provides a simpler framework to guarantee device integrity, a decentralized solution is better suited to a tactical environment.

2. Decentralized Device Attestation

Decentralized device attestation solutions are largely based on the Ibrahim et al. model for Unattended Scalable Attestation of IoT Devices (US-AID) [65]. In this model, devices perform collective attestation functions on each other in order to maintain awareness of how trustworthy a neighbor's hardware/software is. Although the model demonstrated scalability by accommodating a static network of 1,000,000 devices with linear energy consumption, increasing the number of mobile devices resulted in a quadratic growth of attestation messages [65]. The most promising solution thus far has been the Continuous Remote Attestation Framework for IoT (CRAFT) introduced by Moreau et al. [60], where devices are classified either as secure or partially-secure based on operator-assigned security parameters that determine the time interval of attestation messages required by each device. Therefore, CRAFT reduces the communication overhead within a large mobile network by adjusting the attestation message frequency based on the security status of devices, minimizing unnecessary transmissions. Implementation of CRAFT resulted in a 66% reduction in communication data overhead in a head-to-head comparison of CRAFT versus US-AID [60].

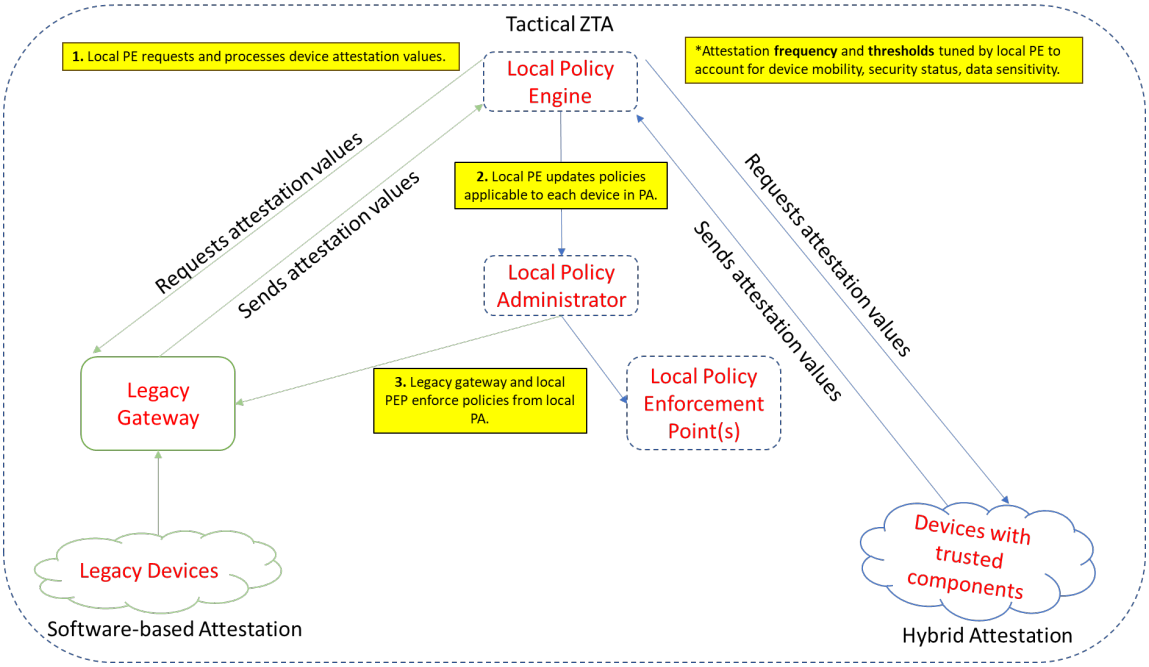

Figure 5. Device Attestation in a TZTA

Figure 5 illustrates deployment of a device attestation framework in a TZTA. Local policy engines (PE) and legacy gateways are primarily responsible for deploying this framework. Devices with appropriate TPM components perform comprehensive attestation with each other as orchestrated by the local PE, whereas legacy devices (LDs) without trusted modules use a software attestation method implemented by the legacy gateway. Attestation data gathered from the legacy gateways are sent to the local PE to evaluate integrity of each LD. This integrity score is then used by the local policy administrator to map appropriate access control rules for each LD. Access to system resources from or by LDs are then enforced by legacy gateways. Local policy enforcement points dictate access to and from system resources by devices as determined by integrity scores assigned by the local policy administrator.

Some degree of centralization is necessary in a TZTA for device attestation. The local PE orchestrates the push and pull of attestation data from devices on the tactical network. Devices capable of collective hybrid attestation manage attestation values for themselves and their neighbors. Devices are classified based on attributes such as: location from adversarial influence, degree of mobility within network, additional security

measures ensuring integrity, or sensitivity of data collected, stored, and transmitted by devices. For example, an unmanned acoustic sensor near adversarial forces is more likely to be compromised versus a fueling sensor located within a secure forward operating base. The acoustic sensor would therefore require more frequent attestation compared to the fuel sensor. These attributes are adjusted by operators in the local PE to reflect any changes stemming from mission requirements. A fuel sensor may require additional attestation if the fuel pump is placed outside of the forward operating base to be more accessible to coalition forces.

Device attestation is a difficult task to accomplish in a TZTA due to energy, storage, and bandwidth constraints. The IoBT is a complex and heterogenous mix of devices that vary in functionality, capability for implementing trust, and purpose in the tactical environment. Using a combination of decentralized and centralized frameworks to manage different groups of devices based on certain attributes provides the necessary flexibility for the local PE to perform device attestation in a tactical environment.

C. WEAPON SYSTEMS EMPLOYMENT AT THE TACTICAL EDGE

Weapons employment within the TZTA is a tightly controlled evolution regulated by rules of engagement, facilitated by commanders' intent, and supported by numerous command and control applications. The processes by which units employ their firing systems at the tactical edge are dictated by the effects rendered from those fires. Effects from weapon system employment can be tactical, operational, and strategic level effects [66]. Fires may be prosecuted at the tactical edge either through the joint targeting cycle or the decide, detect, deliver, and assess (D3A) methodology [67]. The following analysis will focus on the latter.

1. Targeting in a Tactical Zero Trust Architecture

Users at the tactical edge need to navigate through several problems in the D3A model using the TZTA framework. This section offers a thorough analysis of the potential challenges facing targeting cycles at the tactical edge. The decide step will focus on enabling users from different TZTAs to coordinate and plan. The detect phase focuses on

processing relevant targeting information across TZTAs boundaries. In the deliver phase, procedures to authenticate weapon employment require additional features within a TZTA. Finally, the assess step requires users from different TZTAs to rapidly coordinate to assess effects on targets. The policies that dictate resource accessibility for targeting and execution of fires provide the framework for information flow between decision-makers, planners, analysts, and operators.

a. Decide

The first step of D3A could require that a cross-functional team of planners from different TZTAs perform coordination and planning. The operational planning team would determine the following: which targets, when the target will be attacked, location of targets, desired effect, by what capability and how results will be assessed [67]. Today, coordination is achieved over command and control (C2) applications and chat applications. For these disparate applications to communicate between different TZTAs, federation between applications is required. A scheme like the identity federation trust evaluation could be adapted to federate applications across TZTAs. For example, if a user sends a message to another user in a different TZTA, the chat application must be federated between the two TZTAs. Next, the user would request access from the local policy enforcement point (PEP) that manages access to the chat application. Following that, the local PEP would either grant or deny access to the user, based on authentication information available to the local policy engine (PE). The message would then be sent through the tactical gateway to the other TZTA where the designated application is located. This example highlights the importance of application federation between TZTAs to enable coordination for decision making.

b. Detect

The next step of D3A involves the validation of target location, and transferring of this sensitive information to decision-makers and operators prior to delivery [67]. This step could require sensitive targeting information to be transferred across TZTAs. An intelligence sensor in a TZTA located near a target might not be in the same TZTA where the shooting platform is located. The primary way for sensitive targeting information to

traverse between the TZTAs is through federated applications on the same enclave of data classification. Since the data is collected from a ZTA, the users accessing the information, devices collecting, storing, and transmitting the information, and applications processing the information have all been validated and authenticated by their respective local policy engines before that data is transferred out of that TZTA. As that information is received at its destination TZTA, those users, devices, applications, and shooting platforms must have a quantifiable measure of how trustworthy that information is prior to the prosecution of a target.

c. Deliver

In the deliver phase of D3A, weapon platforms are fired either manually or remotely controlled by human operators. Shooting platforms capable of gathering and processing contextual information to authenticate users could potentially be used to unlock and lock these weapon systems. This operating capability is discussed in Castiglione et al. on incorporating context-aware biometrics or MFA solutions in the IoBT [68]. For example, the U.S. Navy successfully incorporated biometric systems on the advanced Tomahawk weapons control system in 2003 [69]. Incorporation of MFA on weapon systems strengthens the overall security of the weapon system from adversarial threats. If an adversary captures a weapon system that needs to be unlocked by an MFA scheme, they would be unable to operate it without developing a mechanism to defeat authentication measures. Another benefit of incorporating MFA on weapon systems is that employment of a weapon system is directly correlated with a user, promoting non-repudiation of the system.

A heterogenous mix of weapon systems with varying capabilities to implement MFA will need to be addressed in a TZTA. Indirect fire weapons such as maritime missile platforms or ground-based rocket artillery assets offer a more robust MFA user authentication scheme. These larger platforms boast enhanced communication, storage, and processing capabilities in comparison to smaller direct fire weapons such as rifles or man-portable rocket systems. This diverse range of capabilities reflects the overall composition of devices within the IoBT. Attestation of these weapon systems share a

similar scheme to the one presented in the TZTA device attestation framework introduced earlier in Chapter 4.B.2. The only additional step is the incorporation of user authentication to allow or deny weapon employment, and logging of user activity associated with the weapon system. Therefore, the local PEP and legacy gateways are responsible for facilitating user access to weapon systems within the ZTA.

Continuous MFA schemes should be employed to the maximum extent possible on weapon systems to mitigate the threats associated with MFA. As discussed in the STRIDE threat model that informed the security requirements of the TZTA framework, spoofing and DoS attacks are the most prevalent threats against MFA at the tactical edge. Increasing the number of authentication mechanisms that need to be defeated increases the level of difficulty and workload required for an adversary to spoof a weapon system on the network. Incorporating redundant methods of authentication in a multi-modal solution provides alternative methods for employing the weapons system should some authentication schemes become unavailable. TZTAs must possess authentication services capable of performing authentication of local weapons systems in a disconnected, degraded, intermittent and/or latent (DDIL) communication environment.

d. Assess

The final step of the fires process is the assessment phase, where the determination of effects produced by fires are synthesized from various collection methods and input from commanders. System administrators should ensure that applications are federated between TZTAs to promote smooth information flow between operators, analysts, planners, and commanders. Commander's determination of effects directly feed into establishing follow-on objectives for future D3A targeting cycles [67].

The effective employment of weapon systems in a TZTA relies on the seamless exchange of information between other TZTAs. Coordination and control of these processes are reliant on federated command and control applications and chat services. In the event of disconnection or degraded communication links between TZTAs, the coordination between units may take over alternative communication links not directly tied

into the TZTA, such as secure voice radio. Furthermore, the local PE should retain its ability to authorize weapon systems in a disconnected or degraded tactical environment.

D. SERVICES AND SECURITY AT THE TACTICAL EDGE

The TZTA should leverage the rapid maturation of communication, storage, and processing capabilities at the tactical edge to expand tactical service-oriented architectures (SoA) [70]. In addition to the application services that support mission requirements, security mechanisms, such as a robust intrusion detection system (IDS) capable of securing both endpoints and the network, must also be implemented in the TZTA. Although nodes may have more local resources available than in the past, the same tactical considerations of operating in a DDIL network environment persist [71].

1. Services in a Tactical Zero Trust Architecture

Each TZTA should be capable of executing mission requirements using locally hosted services in the event that their connection to enterprise, higher-level, or adjacent units are compromised. The chat services and command and control applications within a tactical SoA should be inherent to every TZTA respective to each tactical formation's mission requirements. A commander should be able to operate on applications deployed in their TZTA to command and control their forces in a DDIL environment with units they are connected to. This independent information ecosystem can be characterized as a *data puddle* that gradually establishes connections to other data puddles via federation. These data puddles eventually connect to the larger enterprise-level *data lake*.

An important requirement for data puddles to form linkages with other data puddles is the seamless federation of services across TZTAs. An example of links between tactical SoAs are proposed by Suri et al. in their policy-based control over information exchange model [72]. Additionally, this model's design complements the proposed TZTA framework. Each application hosted in their tactical SoA used a gateway server to facilitate communications across domains between applications. In a TZTA, each server gateway would be included in the tactical gateway to facilitate communication between applications from different TZTAs. Alternative methods of service federation can be accomplished

through middleware proxies such as the Agile Computing Middleware NetProxy [73], [74]. These proxies could be incorporated within the local PEPs and report contextual information to the local PE to gain additional insight for trust evaluation.

Ensuring a secure federation channel between applications operating across TZTAs solves only part of the problem. Application services are vulnerable to adversarial compromise, as emphasized in Sterle et al. report on the SolarWinds Orion security breach [75]. Application federation schemes must therefore follow a similar approach to quantitatively determine trust between application services operating on disparate TZTAs. Application service attestation could leverage middleware proxies that capture contextual information. Then the local PE can use this information to validate application integrity. Alternative methods of determining application integrity periodically compare actual hashes of the application code base or configurations to expected hashes calculated previously. Any discrepancies would lead to further investigation by operators to determine if malicious code or settings were inserted. Trust values could then be calculated and included in an encapsulated message at tactical gateway servers. The receiving gateway servers would then pass the trust values from these encapsulated messages to their local PE. The receiving local PE could then determine if application traffic is trustworthy. If not, further investigation by system operators would be required. Administrative traffic, including messages between federated applications are treated as system resources and are managed by the local PE. Any user seeking access to the application and its contents would need to follow the same steps to access any other authorized resource on the system.

2. Intrusion Detection Systems in a Tactical Zero Trust Architecture

An important subset of the security services hosted within each TZTA are the IDSs deployed. There are two types of IDS that detect intrusion within a TZTA: host-based IDSs used to detect intrusion on each endpoint, and network-based IDSs responsible for monitoring network traffic [76].

A promising solution for deploying endpoint IDSs within a ZTA is the SysFlow framework proposed by Hong et al. [77]. Their framework deploys an IDS on each host to generate events based on kernel calls to system resources. Since each event is generated

from the kernel level, it is difficult for an adversary to bypass the IDS on the host [77]. These events are sorted into flows which are then collected into flow tables stored on each host. Flows are sent to the centralized controller located in the PE to be analyzed. Flow analysis of each host serves to inform the PE on trustworthiness of an endpoint in addition to other trust information gathered from multi factor continuous authentication schemes. SysFlow distributes the storage and processing requirements to the edge to the maximum extent possible. Reducing the volume of data required by the controller from endpoints reduces the overall communication overhead for this protocol [77]. The lightweight and complementary nature of SysFlow make it an ideal candidate for incorporation into a TZTA. The only modification required for implementation in a tactical environment would be to develop an extension of SysFlow to capture flows from legacy devices. A SysFlow agent would be deployed within the legacy gateway, where each flow would correspond to a legacy device operating within the TZTA. Since the legacy gateway captures all interactions between legacy endpoints and system resources, all endpoints are tracked by an IDS.

The network-based IDS proposed by Alalmaie et al. is the most suitable for TZTA deployment [78]. Their model analyzes network traces in near real time to detect anomalous network traffic by using a multi-view approach. A multi-view approach expands the feature set derived from network flow information to include both IP addresses and port numbers. This comprehensive feature set is partitioned using multiple key vectors. These partitions are then encoded to extract principal features before being analyzed through a convolutional neural network that classifies benign or malicious network traffic.

Massive communication overhead is an issue with deployment of a network IDS in a tactical environment. Network devices sending large packet traces to the network IDS reduce available bandwidth for mission requirements. Instead, all network devices within the TZTA should have a processing capability that performs trace analysis of their own flows, and reports abnormal traffic to the local PE. The local PE would then alert network operators of anomalous traffic on endpoint devices. Network administrators could then investigate further and adjust firewall policies as necessary to block potentially harmful traffic.

Achieving mission objectives and upholding the security posture of the architecture in a TZTA relies on the successful deployment of application services and IDSs. Effective deployment of application services within TZTAs must address the issue of federation. IDSs will need to be deployed within the network and at endpoints to ensure complete and consistent coverage within the TZTA.

E. CHAPTER SUMMARY

This chapter explored how the proposed TZTA framework may interact with users, devices, weapon systems, application, and security services in a tactical environment. Increasing the number of multi-modal continuous authentication mechanisms within a TZTA mitigates risks of non-compatible authentication measures for mobile users. It also introduced a framework to quantify trust between TZTAs that facilitates user federation.

Device attestation is a complex problem faced in a heterogeneous IoBT environment. Not all models for device attestation provide the same level of security. Some models need to be augmented with increased device attestation frequency and smaller thresholds to account for a variety of attributes for each device. Device mobility, security status, and data sensitivity are examples of such attributes. Weapon system employment in a tactical network relies on the exchange of information between TZTAs for coordination and prosecution of targets. Finally, mission accomplishment is closely coupled with effectiveness of system application federation and deployment of IDS within the TZTA.

The next chapter summarizes the thesis, discusses the conclusions from the research, and identifies areas of future work to extend this work.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

A. SUMMARY

The goal of this thesis was to propose a ZTA for the tactical edge, and analyze how it may interact with users, devices, weapon systems, applications, and security services. Requirements for the architecture at the tactical edge were developed using the STRIDE threat-based model. Resource availability, access control, authentication mechanisms, and IDS deployment were addressed in the security requirements for the architecture. Incorporation of legacy battlefield systems and operating among joint or coalition partners are included in the operational requirements. These requirements complement each other, ensuring a secure, resilient, and mission effective framework.

From these requirements, a tactical ZTA (TZTA) framework was proposed. The thesis then analyzed how the architecture interacts with various entities, processes, and applications. This analysis revealed that federation, attestation, and security need to be addressed in the proposed architecture. Issues with identity and services federation were explored, and attestation of a heterogenous mix of devices at the tactical edge was investigated. Identifying the scheme for endpoint and network IDS throughout the TZTA aligned with tactical considerations of limited storage, processing, and power in these environments.

B. CONCLUSIONS

This research identified the necessary components of a ZTA suitable for the tactical edge. Features that enable federation, attestation, and security at the tactical edge were identified as well.

Two research questions were addressed by this research:

1. What are the key components of a ZTA suitable for the tactical edge?

The proposed TZTA incorporates similar components from an enterprise ZTA solution, with a policy engine, policy administrator, and policy enforcement points. An enterprise gateway, tactical gateway, and legacy gateway are added to support the

requirements of a tactical environment. The enterprise gateway serves as the primary conduit between the TZTA and the enterprise environment. The tactical gateway is the main interface where networking and federation services perform inter-TZTA communication. The legacy gateway separates legacy devices (LD) from the rest of the TZTA and encapsulates traffic to and from LD. This encapsulation scheme enables device attestation and access control. Together, these components provide the necessary foundation to realize ZT tenets at the tactical edge.

2. How do users, devices, weapon systems, applications, and security services interact within a ZTA implementation at the tactical edge?

A ZTA will interact poorly with users, devices, weapon systems, applications, and security services without incorporation of additional features within TZTA components. Some of these features are identity federation, device attestation, application federation, robust MFA schemes, and a comprehensive IDS solution. Identity federation at the tactical edge requires a model to determine trust quantitatively between disparate TZTAs. Local policy engines extended device attestation using software-based attestation models at legacy gateway. Incorporation of software-based attestation provided the framework to determine the integrity of legacy devices. Weapon system employment in TZTAs heavily relies on the secure exchange of information and a resilient method of execution. Features that enable these requirements are federated command and control applications and a robust MFA scheme. The successful deployment of federated application services and a comprehensive IDS in a TZTA are essential to achieving mission objectives in a secure fashion.

C. FUTURE WORK

1. Implementation and Testing

This research identified components suitable for deployment of a ZTA at the tactical edge, but the proposed architecture was not implemented. These proposed components aligned with the five ZT tenets referenced in [1], that: 1) Assume a Hostile Environment; 2) Presume Breach; 3) Never Trust, Always Verify; 4) Scrutinize Explicitly; and, 5) Apply Unified Analytics. Several models and technologies for continuous

authentication identified in this research ([9], [10], [13], [15], [16], [18], [20], [21]) require a method to consolidate and evaluate these authentication mechanisms within a local policy engine. Future work should develop a local policy engine model capable of consolidating the numerous authentication schemes to quantitatively determine trust across a diverse mix of users, devices, and services. Further analysis and testing of identity federation solutions such as [44], [47], [48], [51], [52] that work across TZTAs would enable interoperability with mission partners. Future research could develop and test device attestation models that encompasses legacy and conventional devices such as those found in [60]–[65]. Development and implementation of these models and solutions will enable further detailed analysis of suitability within a tactical environment.

2. Detailed Analysis of ZTA Working in MPE

The MPE introduced in Chapter IV is a federated information-sharing framework in development that spans across several network boundaries [80]. In addition to collaborating with U.S. military and government organizations, assessing interoperability with coalition partners needs to be addressed. Researchers familiar with coalition environments should expand on the research on TZTA federation amongst partners with varying capabilities.

3. TZTA Networking

This research did not cover solutions for network segmentation across TZTAs. Additional research on tactical ad-hoc networking would help realize the second operational requirement for TZTAs. Analysis of implementing a TZTA within a 5G architecture, such as the one proposed by Manan et al., would identify further research areas [81]. Another networking scheme that could be explored is the incorporation of mobile ad-hoc networks (MANET) with a TZTA. These networks provide a resilient network suitable for the dynamic tactical environment. Unfortunately, MANETs lack security mechanisms to determine trust between nodes within the network. Research into how nodes might evaluate trust between nodes would also bring TZTA closer to actual deployment.

4. Blockchain in a Tactical Environment

In this research, several blockchain solutions were discussed as solutions for authentication, federation, and attestation within a TZTA [24], [52]. These solutions were dismissed because detailed analysis of storage, processing, and power requirements were not done, and frameworks required persistent connectivity between an external resource to the blockchain network. Future analysis of some of these blockchain solutions could identify alternative solutions that would make a blockchain solution suitable for the tactical environment.

LIST OF REFERENCES

[1] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, "DOD zero trust reference architecture," Washington, DC, USA, Jul. 2022. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[2] P. Griffin, "Enter the Killweb: A Concept for Drone Warfare," *U.S. Naval Institute*, vol. 149, no. 3, Mar. 29, 2023. Accessed: Sep. 06, 2023. Available: https://www.usni.org/magazines/proceedings/2023/march/enter-killweb-concept-drone-warfare

[3] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Sep. 2017, pp. 1–6. doi: 10.1109/ISGTEurope.2017.8260283.

[4] J. Kindervag and S. Balaouras, "No more chewy centers: Introducing the zero trust model of information security," *Forrester Research*, vol. 3, pp. 1–10, 2010.

[5] DOD CIO Zero Trust Portfolio Management Office, "DOD zero trust strategy," Washington, DC, USA, Nov. 2022. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DOD-ZTStrategy.pdf

[6] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, Washington, DC, USA, NIST Special Publication (SP) 800–207, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[7] N. Siddiqui, L. Pryor, and R. Dave, "User authentication schemes using machine learning methods—A review," in *Proceedings of International Conference on Communication and Computational Technologies*, S. Kumar, S. D. Purohit, S. Hiranwal, and M. Prasad, Eds., in Algorithms for Intelligent Systems. Singapore: Springer, 2021, pp. 703–723. doi: 10.1007/978-981-16-3246-4_54.

[8] D. Appelt, C. D. Nguyen, A. Panichella, and L. C. Briand, "A machine-learning-driven evolutionary approach for testing web application firewalls," *IEEE Transactions on Reliability*, vol. 67, no. 3, pp. 733–757, Sep. 2018, doi: 10.1109/TR.2018.2805763.

[9] M. Antonakakis *et al.*, "Understanding the mirai botnet," presented at the 26th USENIX Security Symposium (USENIX Security 17), 2017, pp. 1093–1110. Accessed: Dec. 01, 2022. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[10] "Single sign on concepts and protocols | SANS institute," Accessed: Nov. 30, 2022. Available: https://www.sans.org/white-papers/1352/

[11] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: reviewing the state of the art," *Cluster Comput*, vol. 19, no. 1, pp. 455–474, Mar. 2016, doi: 10.1007/s10586-015-0510-4.

[12] M. Alimomeni and R. Safavi-Naini, "How to prevent to delegate authentication," in *Security and Privacy in Communication Networks*, B. Thuraisingham, X. Wang, and V. Yegneswaran, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer International Publishing, 2015, pp. 477–499. doi: 10.1007/978-3-319-28865-9_26.

[13] S. P. Banerjee and D. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *JPRR*, vol. 7, no. 1, pp. 116–139, 2012, doi: 10.13176/11.427.

[14] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1998–2026, 2016, doi: 10.1109/COMST.2016.2537748.

[15] S. Lee, S. Lee, E. Park, I. Y. Kim, and J. Lee, "Gait-based continuous authentication using a novel sensor compensation algorithm and geometric features extracted from wearable sensors," *IEEE Access*, vol. 10, pp. 120122–120135, Nov. 2022, doi: 10.1109/ACCESS.2022.3221813.

[16] H. Alamleh and A. A. S. AlQahtani, "Architecture for continuous authentication in location-based services," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, Dec. 2020, pp. 1–4. doi: 10.1109/3ICT51146.2020.9311972.

[17] H. Alamleh and A. A. S. AlQahtani, "A cheat-proof system to validate GPS location data," in *2020 IEEE International Conference on Electro Information Technology (EIT)*, Jul. 2020, pp. 190–193. doi: 10.1109/EIT48999.2020.9208243.

[18] W. He, X. Liu, and M. Ren, "Location cheating: A security challenge to location-based social network services," in *2011 31st International Conference on Distributed Computing Systems*, Jun. 2011, pp. 740–749. doi: 10.1109/ICDCS.2011.42.

[19] R. Mason *et al.*, "Analyzing a more resilient national positioning, navigation, and timing capability," RAND Corporation, May 2021. Accessed: Jan. 04, 2023. Available: https://www.rand.org/pubs/research_reports/RR2970.html

[20] S. W. Shah, N. F. Syed, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "LCDA: Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA) | Elsevier enhanced reader," *Computers & Security*, vol. 108, p. 102351, 2021, doi: https://doi.org/10.1016/j.cose.2021.102351.

[21] B. Yu, C. Yang, and J. Ma, "Continuous authentication for the internet of things using channel state information," presented at the 2019 IEEE Global Communications Conference(GLOBECOM), Dec. 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9014276.

[22] Y.-H. Chuang, N.-W. Lo, C.-Y. Yang, and S.-W. Tang, "A lightweight continuous authentication protocol for the internet of things," *Sensors*, vol. 18, no. 4, Art. no. 4, Apr. 2018, doi: 10.3390/s18041104.

[23] M. Naveed Aman, S. Taneja, B. Sikdar, K. C. Chua, and M. Alioto, "Token-based security for the internet of things with dynamic energy-quality tradeoff," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2843–2859, Apr. 2019, doi: 10.1109/JIOT.2018.2875472.

[24] V. Hu, "Blockchain for access control systems," National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8403, May 2022. doi: 10.6028/NIST.IR.8403.

[25] M. Rocchetto, A. Ferrari, and V. Senni, "Challenges and opportunities for model-based-security risk assessment of cyber-physical systems," in *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction*, F. Flammini, Ed., in Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2019, pp. 25–47. doi: 10.1007/978-3-319-95597-1_2.

[26] N. Shevchencko, T. Chick, P. O'Riordan, T. Scanlon, and C. Woody, "Threat modeling: A summary of available methods," Carnegie Mellon University Software Engineering Institute, Pittsburgh, PA, USA, Jul. 2018. Accessed: Mar. 31, 2023. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=524448

[27] L. Kohnfelder and P. Garg, "The threats to our products," Microsoft Corporation, Redmond, WA, USA, Technical Report Vol 33, Apr. 1999.

[28] Administrator, "CNSS instructions," Accessed: Mar. 31, 2023. Available: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[29] "Committee on national security systems (CNSS) glossary, CNSS instruction 4009–2022," *Committee on National Security Systems*, 2022.

[30] B. Tripathi, "What is repudiation in cyber security?," *Medium*, Jan. 2023, Accessed: Sep. 01, 2023. Available: https://medium.com/@brajagopal.tripathi/what-is-repudiation-in-cyber-security-2eb98a75510d

[31] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "An introduction to information security," National Institute of Standards and Technology, Washington, DC, USA, 800–12 rev 1, Jun. 2017.

[32] MITRE ATT&CK, "Privilege escalation, tactic TA0004 – enterprise | MITRE ATT&CK®," Jan. 06, 2021. https://attack.mitre.org/tactics/TA0004/ (accessed Sep. 01, 2023).

[33] E. S. Hosney, I. T. A. Halim, and A. H. Yousef, "An artificial intelligence approach for deploying zero trust architecture (ZTA)," in *2022 5th International Conference on Computing and Informatics (ICCI)*, Mar. 2022, pp. 343–350. doi: 10.1109/ICCI54321.2022.9756117.

[34] Defense Information Systems Agency (DISA), "Department of defense cloud computing security requirments guide," Washington, DC, USA, Mar. 2017.

[35] G. Køien, "Zero-trust principles for legacy components," *Wireless Personal Communications*, vol. 121, pp. 1–18, Nov. 2021, doi: 10.1007/s11277-021-09055-1.

[36] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what It is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 57–64. doi: 10.1109/Trustcom.2015.357.

[37] K. Poularakis, G. Iosifidis, and L. Tassiulas, "SDN-enabled tactical ad hoc networks: Extending programmable control to the edge," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 132–138, Jul. 2018, doi: 10.1109/MCOM.2018.1700387.

[38] F. Federici, D. Martintoni, and V. Senni, "A zero-trust architecture for remote access in industrial IOT infrastructures," *Electronics*, vol. 12, no. 3, p. 566, 2023, doi: https://doi.org/10.3390/electronics12030566.

[39] "The federated identity, credential, and access management architecture," General Services Administration, Washington, DC, USA, Jan. 2021.

[40] K. Sullivan, "Risks to the mission partner environment: Adversarial access to host nation network infrastructure," *The Cyber Defense Review*, vol. 6, no. 3, pp. 109–118, 2021.

[41] "DOD instruction 8520.03 identity authentication for information systems," DOD CIO, Washington, DC, USA, 2023.

[42] G. Jaspher, W. Katherine, E. Kirubakaran, and P. Prakash, "Smart card based remote user authentication schemes — Survey," in *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, Jul. 2012, pp. 1–5. doi: 10.1109/ICCCNT.2012.6395882.

[43] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, Nov. 2004, doi: 10.1016/j.patcog.2004.04.011.

[44] D. Das, S. Maity, B. Chatterjee, and S. Sen, "In-field remote fingerprint authentication using human body communication and on-hub analytics," in *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Jul. 2018, pp. 5398–5401. doi: 10.1109/EMBC.2018.8513667.

[45] G. Cecchine, F. E. Morgan, M. A. Wermuth, T. Jackson, A. G. Schaefer, and M. Stafford, "The U.S. military response to the 2010 Haiti earthquake: Considerations for army leaders," RAND Corporation, Oct. 2013. Accessed: Aug. 17, 2023. Available: https://www.rand.org/pubs/research_reports/RR304.html

[46] K. Strandell and S. Mittal, "Risks to zero trust in a federated mission partner environment," arXiv, Nov. 30, 2022. https://doi.org/10.48550/arXiv.2211.17073 (accessed Aug. 17, 2023).

[47] K. Hatakeyama, D. Kotani, and Y. Okabe, "Zero trust federation: Sharing context under user control towards zero trust in identity federation," in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, Mar. 2021, pp. 514–519. doi: 10.1109/PerComWorkshops51409.2021.9431116.

[48] Z. Calhoun, P. Maribojoc, N. Selzer, L. Procopi, N. Bezzo, and C. Fleming, "Analysis of identity and access management alternatives for a multinational information-sharing environment," in *2017 Systems and Information Engineering Design Symposium (SIEDS)*, Apr. 2017, pp. 208–213. doi: 10.1109/SIEDS.2017.7937718.

[49] P. Smriti, S. Srivastava, and S. Singh, "Keyboard invariant biometric authentication," in *2018 4th International Conference on Computational Intelligence & Communication Technology (CICT)*, Feb. 2018, pp. 1–6. doi: 10.1109/CIACT.2018.8480337.

[50] T. Dee, I. Richardson, and A. Tyagi, "Continuous transparent mobile device touchscreen soft keyboard biometric authentication," in *2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)*, Jan. 2019, pp. 539–540. doi: 10.1109/VLSID.2019.00125.

[51] Y. Choi, S. Lee, and B. Choi, "Vulnerability risk score recalculation for the devices in critical infrastructure," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2022, pp. 2179–2181. doi: 10.1109/ICTC55196.2022.9952587.

[52] I. Alom *et al.*, "Dynamic management of identity federations using blockchain," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2021, pp. 1–9. doi: 10.1109/ICBC51069.2021.9461128.

[53] O. Avellaneda *et al.*, "Decentralized identity: Where did it come from and where is it going?," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, Dec. 2019, doi: 10.1109/MCOMSTD.2019.9031542.

[54] N. Suri *et al.*, "Analyzing the applicability of Internet of Things to the battlefield environment," in *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2016, pp. 1–8. doi: 10.1109/ICMCIS.2016.7496574.

[55] A. Kott, A. Swami, and B. J. West, "The internet of battle things," arXiv, Dec. 24, 2017. https://doi.org/10.48550/arXiv.1712.08980 (accessed Aug. 18, 2023).

[56] L. Zhu, S. Majumdar, and C. Ekenna "An invisible warfare with the internet of battlefield things: A literature review." *Human Behavior & Emerging Technologies*, vol. 3, no. 2, pp. 255–260, 2021. doi: 10.1002/hbe2.231.

[57] Headquaters United States Marine Corps, *Marine Corps Doctrinal Publication,* MCDP 1-0 w/ CH1-3, United States Marine Corps . Washington, DC, USA, 2019. Accessed: Sep. 04, 2023. Available: https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1323621/mcdp-1-0-w-ch1-3/https%3A%2F%2Fwww.marines.mil%2FNews%2FPublications%2FMCPEL%2FElectronic-Library-Display%2FArticle%2F1323621%2Fmcdp-1-0-w-ch1-3%2F

[58] *Doctrine for the armed forces of the United States*. in 5, no. 0. Washington, DC, 2020. Available: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/5-0-Planning-Series/

[59] R. Han, C. Hartung, and J. Balasalle, "Node compromise in sensor networks: The need for secure systems," University of Colorado at Boulder, Boulder, CO, USA, CU-CS-990-05, 2005. Available: http://id.loc.gov/vocabulary/iso639-2/eng

[60] L. Moreau, E. Conchon, and D. Sauveron, "CRAFT: A continuous remote attestation framework for IoT," *IEEE Access*, vol. 9, pp. 46430–46447, 2021, doi: 10.1109/ACCESS.2021.3067697.

[61] P.-H. Yang and S.-M. Yen, "Memory attestation of wireless sensor nodes by trusted local agents," in *2015 IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 82–89. doi: 10.1109/Trustcom.2015.360.

[62] S. J. Johnston, M. Scott, and S. J. Cox, "Recommendations for securing Internet of Things devices using commodity hardware," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Dec. 2016, pp. 307–310. doi: 10.1109/WF-IoT.2016.7845410.

[63] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: SoftWare-based attestation for embedded devices," in *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*, May 2004, pp. 272–282. doi: 10.1109/SECPRI.2004.1301329.

[64] D. Schellekens, B. Wyseur, and B. Preneel, "Remote attestation on legacy operating systems with trusted platform modules," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 1, pp. 59–72, Feb. 2008, doi: 10.1016/j.entcs.2007.10.014.

[65] A. Ibrahim, A.-R. Sadeghi, and G. Tsudik, "US-AID: Unattended scalable attestation of IoT devices," in *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)*, Oct. 2018, pp. 21–30. doi: 10.1109/SRDS.2018.00013.

[66] *Doctrine for the armed forces of the United States*. in JP-3, no. 09. Washington, DC, 2019. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf

[67] *Marine Corps Warfighting Publication,* MCWP 3-43.3, Marine Air-Ground Task Force Fires, United States Marine Corps . Washington, DC, USA, 2018. Available: http://www.marines.mil/portals/1/Publications/MCWP%203-31.pdf?ver=2018-12-13-142022-170

[68] A. Castiglione, K.-K. R. Choo, M. Nappi, and S. Ricciardi, "Context Aware Ubiquitous Biometrics in Edge of Military Things," *IEEE Cloud Computing*, vol. 4, no. 6, pp. 16–20, Nov. 2017, doi: 10.1109/MCC.2018.1081072.

[69] P. Wilson and B. Shank, "Costs and benefits of integrating biometrics with a navy tactical weapons system," in *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.*, Jun. 2003, pp. 303–304. doi: 10.1109/SMCSIA.2003.1232442.

[70] G. Benincasa *et al.*, "Extending service-oriented architectures to the tactical edge," in *MILCOM 2012 – 2012 IEEE Military Communications Conference*, Oct. 2012, pp. 1–7. doi: 10.1109/MILCOM.2012.6415741.

[71] N. Suri, "Dynamic service-oriented architectures for tactical edge networks," in *Proceedings of the 4th Workshop on Emerging Web Services Technology*, in WEWST '09. New York, NY, USA: Association for Computing Machinery, Nov. 2009, pp. 3–10. doi: 10.1145/1645406.1645408.

[72] N. Suri *et al.*, "Peer-to-peer communications for tactical environments: Observations, requirements, and experiences," *IEEE Communications Magazine*, vol. 48, no. 10, pp. 60–69, Oct. 2010, doi: 10.1109/MCOM.2010.5594678.

[73] A. Morelli, R. Kohler, C. Stefanelli, N. Suri, and M. Tortonesi, "Supporting COTS applications in tactical edge networks," in *MILCOM 2012 – 2012 IEEE Military Communications Conference*, 2012. Accessed: Aug. 27, 2023. Available: https://ieeexplore.ieee.org/document/6415762

[74] R. Lenzi *et al.*, "Interconnecting tactical service-oriented infrastructures with federation services," in *MILCOM 2013 – 2013 IEEE Military Communications Conference*, Nov. 2013, pp. 692–697. doi: 10.1109/MILCOM.2013.123.

[75] L. Sterle and S. Bhunia, "On SolarWinds Orion platform security breach," in *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, Oct. 2021, pp. 636–641. doi: 10.1109/SWC50871.2021.00094.

[76] S. Sanyal and T. Sarkar, "Survey on host and network based intrusion detection system," *International Journal of Advanced Networking and Applications*, vol. 6, pp. 2266–2269, 2014.

[77] S. Hong, L. Xu, J. Huang, H. Li, H. Hu, and G. Gu, "SysFlow: Toward a programmable zero trust framework for system security," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2794–2809, 2023, doi: 10.1109/TIFS.2023.3264152.

[78] A. Z. Alalmaie, P. Nanda, and X. He, "Zero trust-NIDSs: Extended multi-view approach for network trace anonymization and auto-encoder CNN for network intrusion detection," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2022, pp. 449–456. doi: 10.1109/TrustCom56396.2022.00069.

[79] S. W. Shah and S. S. Kanhere, "Recent trends in user authentication – A survey," *IEEE Access*, vol. 7, pp. 112505–112519, 2019, doi: 10.1109/ACCESS.2019.2932400.

[80] *DOD Instruction 8110.01 Mission Partner Environment Information Sharing Capability Implementation for the DOD*. Washington, DC, USA, 2021.

[81] A. Manan, Z. Min, C. Mahmoudi, and V. Formicola, "Extending 5G services with Zero Trust security pillars: a modular approach," in *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*, Dec. 2022, pp. 1–6. doi: 10.1109/AICCSA56895.2022.10017774.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE