[Arculus] Low Overhead Zero Trust Solution for the Tactical Warfighting Edge

Presenter: Prasad Calyam, PhD (MU)

Team Members: Rohit Chadha, PhD (MU), Vijay Anand, PhD (UMSL), Reshmi Mitra, PhD (SEMO)

CAE IN CYBERSECURITY COMMUNITY

University of Missouri

Mizzou CERI
Center for Cyber Education, Research & Infrastructure

UMSL
University of Missouri–St. Louis

SEMO

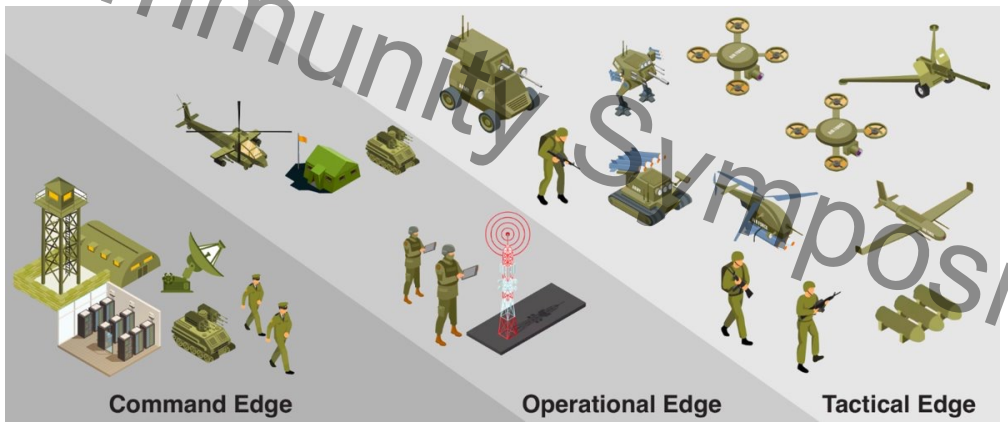
DISA

U.S. NAVAL RESEARCH LABORATORY

Implementing Zero Trust at the Tactical Warfighting Edge [TWE]

Problem Statement: The DoD is seeking innovative and actionable approaches to provide Zero Trust (ZT) functionality to warfighters operating at the tactical edge.

ZT Enterprise capabilities and activities may not be effective at the tactical edge due to operational impacts from denied, disrupted, intermittent, and limited (DDIL) environments, including limited bandwidth.



For instance, data gathering, and its processing needs to be **reliable and time efficient** for operational decision making

Figure adapted from Strayer, Tim, et al. "Content sharing with mobility in an infrastructure-less environment." Computer Networks 144 (2018): 1-16, based on CBMEN, DARPA'S peer-to-peer technology for battlefield.

Mission Tasks Carried out by TWE devices [1].

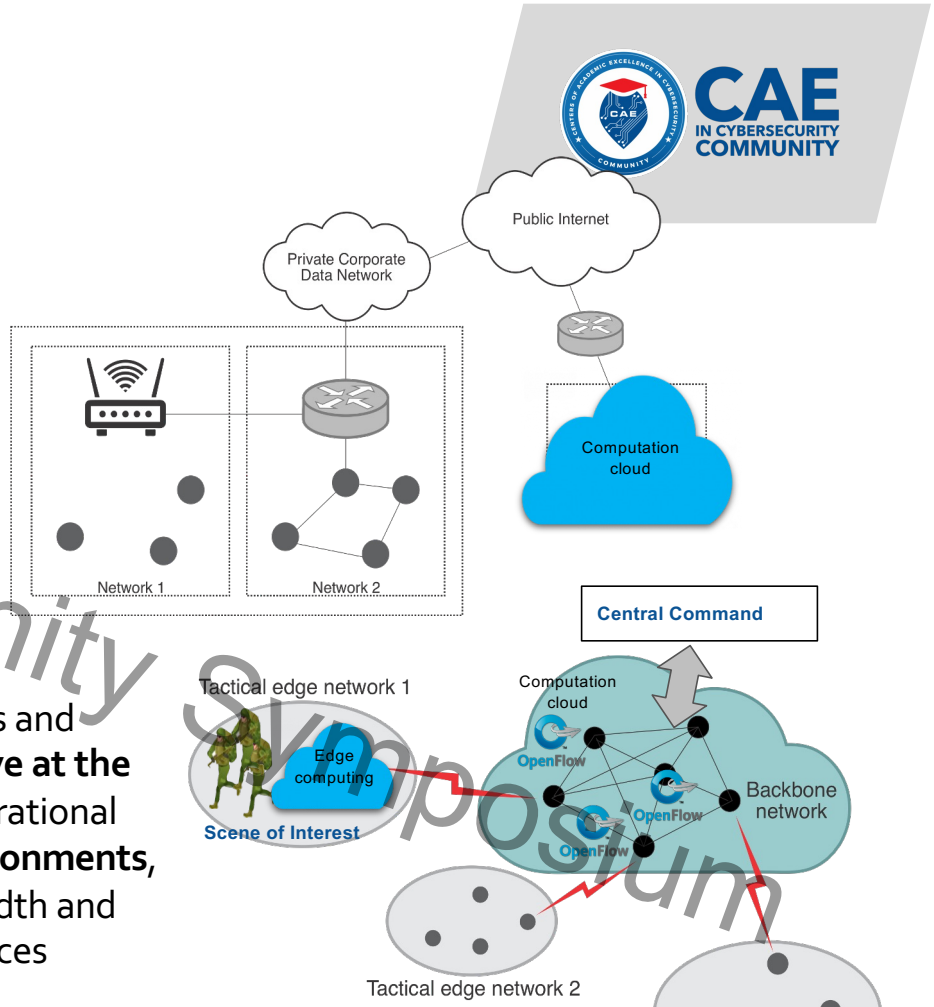
- Video data collection, transmission and processing for real-time situational awareness, decision-making, and strategic intelligence.
- Sensor data for surveillance on environmental conditions, enemy movements, and potential threats, guiding military actions, and ensuring operational success.
- Chemical, Biological, Radiological, & Nuclear (CBRN) Threat Detection to safeguard troops and civilians, prevent catastrophic incidents, and execute effective response measures in hazardous situations.
- Tracking casualties, injuries, and medical help requirement ensuring optimal resource allocation, and swiftly delivering life-saving care during missions (lower sensitive tasks).

[1] Liu, Dongxin, et al. "IoBT-OS: Optimizing the sensing-to-decision loop for the internet of battlefield things." 2022 International Conference on Computer Communications and Networks (ICCCN). IEEE, 2022. Stocchero, Jorgito Matiuzzi, et al. "Secure command and control for internet of battle things using novel network paradigms." IEEE Communications Magazine (2022).

Zero Trust paradigm is emerging in the enterprise…

Enterprise Network

- Identity Verification
- Access Control
- Resource Protection
- Policy & Orchestration
- Monitoring & Analytics
- Continuous Ops



Tactical Edge Network

- ZT Enterprise capabilities and activities are **not effective at the tactical edge** due to operational impacts from **DDIL environments**, including limited bandwidth and other constrained resources

Innovative solutions are need to apply the ZT paradigm to the warfighters' operations involving sensitive data communication or storage, as well as data processing

University of Missouri · Mizzou CERI Center for Cyber Education, Research & Infrastructure · UMSL University of Missouri–St. Louis · SEMO · DISA · U.S. Naval Research Laboratory

Motivation – Why is this important?

- **Given the Denied, Disrupted, Intermittent, and Limited Impact (DDIL)** nature of tactical edge network environments, a resource-aware security approach is essential to address edge resource constraints and enable real-time decision-making [2] .
- **The Zero Trust (ZT) security paradigm** can be used to enable mandatory access controls, continuous entity verification, and mitigation of unauthorized access, tampering, and data integrity issues.
- However, there is a need to transform ZT security principles that are typically developed for unconstrained data center environments with reliable networking and abundant computing power and are not suitable in a tactical edge network setting [3] .

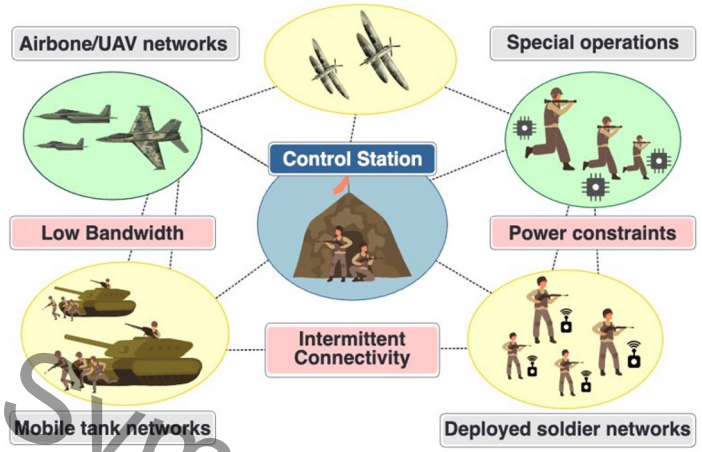


Figure 1: Tactical edge networks face several challenges, including low bandwidth, intermittent connectivity, and power constraints.

[2] Liu, Dongxin, et al. "IoBT-OS: Optimizing the sensing-to-decision loop for the internet of battlefield things." 2022 International Conference on Computer Communications and Networks (ICCCN). IEEE, 2022.
[3] Saketh Poduvu, Sayed M. Saghaian N. E., Ekincan Ufuktepe, Alicia Esquivel Morel, and Prasad Calyam. "Risk-based Zero Trust Scale for Tactical Edge Network Environments." 2023IEEE/ACM symposium on edge computing (SEC). IEEE, 2023.

ZT Architecture Fundamentals

"Never Trust, Always Verify"

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

1. Different cybersecurity strategies need to be evolved in Tactile Edge Network (DDIL) environments
2. ZT implementation needs to move defense strategies focus on users, assets and resources
3. ZT policies need to be based on data flows, user roles on a "need to know" or "least privilege" basis
4. Access control needs to be monitored and adapted to a changing environment continuously
5. Segment networks as granular as possible so that attack impact can be contained during failure
6. ZT implementation needs to comply with standards such as the NIST Zero Trust Models SP 800-207 and 800-201

Addressing the challenges of implementing a ZT architecture

- Which zero trust based defense mechanisms can help with dynamic access control and sustained resilience of the tactical edge network?

Reference **Architecture for ZT** implementation that can **move defense strategies away from static network perimeters**, and focus on users, assets and resources at the tactical warfighting edge.

Dynamic, comprehensive, adaptable and holistic ZT solution approach that can be applicable to mainly Collaborative Drone Systems (CDS), extendable to other applications involving smart devices, cameras, sensors, or radars.

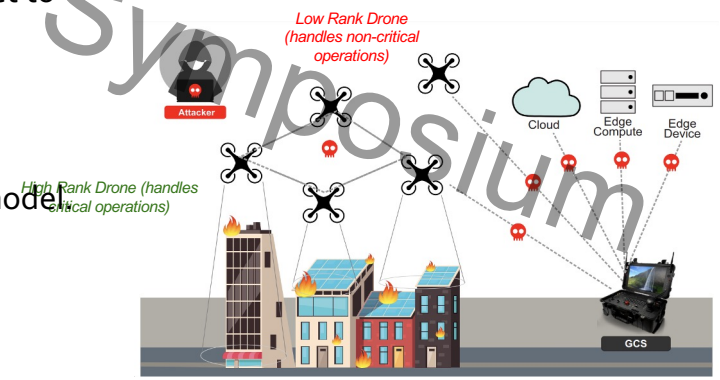
Suite of **risk quantification methods** for secure edge computing/networking systems, to implement ZT-based active defense in a tactical warfighting edge.

Helping DoD in solving a challenging problem:

- How can the Low Overhead Zero Trust Solution [Arculus] help to implement Zero Trust at the tactical warfighting edge?

Active Defense Challenge: Securing inter-connectivity of drone devices at the network edge and coordination with ground control station / central command with zero trust security that addresses edge resource overhead constraints.

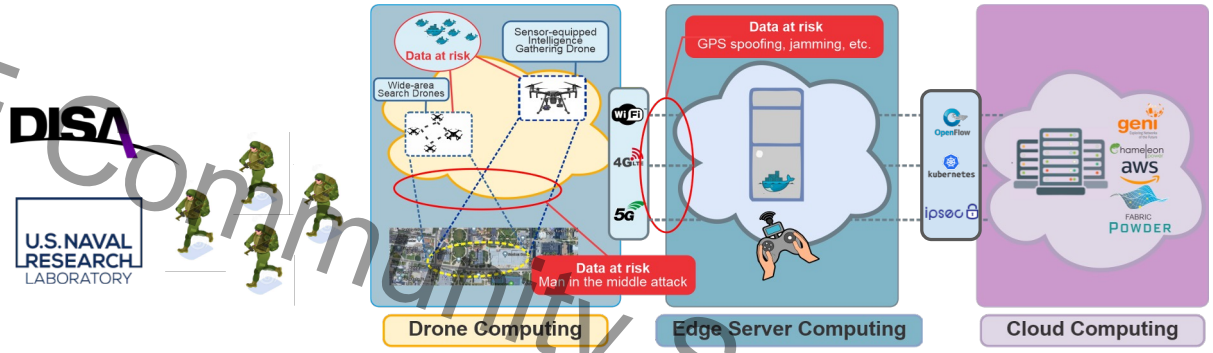
- **Risk quantification** aids in continuous evaluation/ranking of assets in a Collaborative Drone System [CDS] starting from adding a drone node or any other asset to a mission swarm to edge routing.
- **Detection of malicious/fraudulent behavior** of threat agents by the risk quantification via calculation of risk scores by using a Bayesian Network [BN] model.
- **Risk-based access control** involving action with logging + notification + commander approval (as suited).



CDS and its integration with edge/cloud infrastructures accomplishing missions, which engenders cyber-attacks that target drone's flight, communication, or reliability in data processing tasks

Challenges in the network-edge and computation security

Drone Video Analytics use-case | Preliminary study and published work [4] .

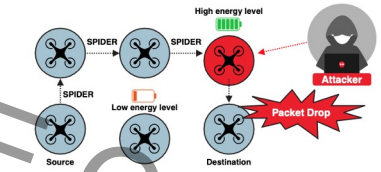


- Drone operations in FANETS are inherently insecure but need to aid warfighters in scenes of interest.
- Limited resources on UAVs brings additional constraints on any security scheme that can be applied to the common protocols in the UAV systems.
- Malicious communications, jams or spoofs in Ground Control Station (GCS) signals, or Denial of Service (DoS) attacks or malware that corrupts containerized data collection/processing

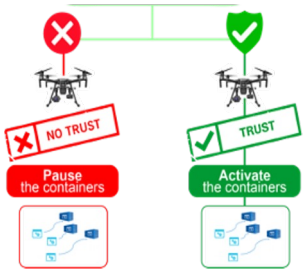
[4] C. Qu, F. Sorbelli, R. Singh, **P. Calyam**, **S. Das**, "Environmentally-Aware and Energy-Efficient Multi-Drone Coordination and Networking for Disaster Response", IEEE Transactions on Network and Service Management (TNSM), 2023

Preliminary study and published work [6, 7]

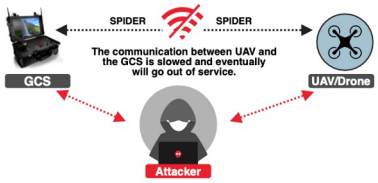
Network-edge and computation security



Faker Node Attack



Corrupted Container



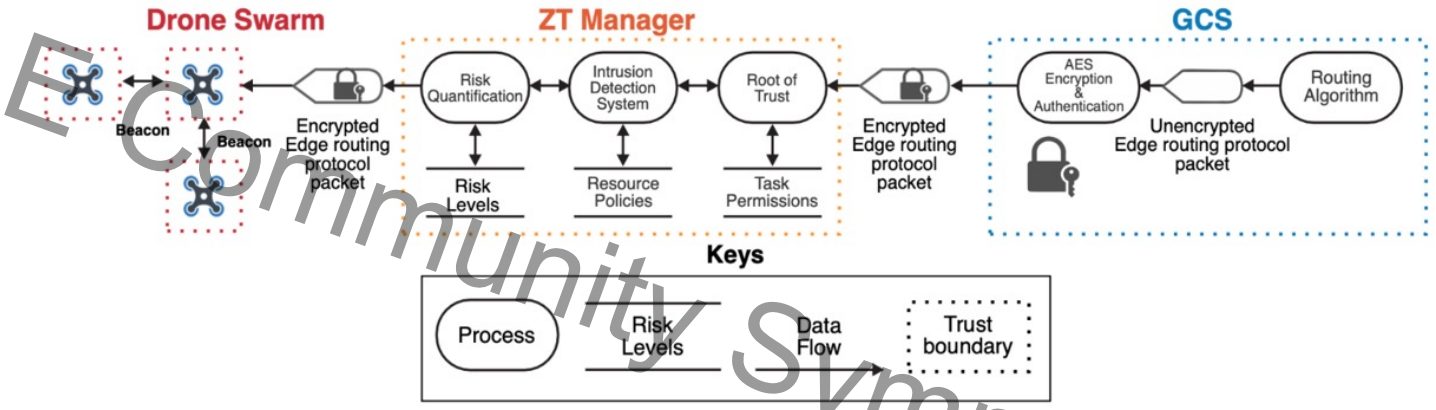
Flooder Node Attack

- **Secure messaging scheme** with custom packet design enforcing data privacy and data integrity, **securing the messaging** in between drone-to-drone and drone-to-edge servers providing a secure protocol over MAVLink.
- A **machine learning based anomaly/fraud detection**, control and countermeasure scheme with constant monitoring for **computation container security**, which can be updated dynamically to improve the security.
- **A realistic testbed** in NSF POWDER infrastructure was used in experimentation of schemes to improve network-edge connectivity and computation security for multi-UAV systems.

[6] A. Esquivel Morel, P. Calyam, D. Kavzak Ufuktepe, R. Ignatowicz, A. Riddle, C. Qu, K. Palaniappan, "Enhancing Network-edge Connectivity and Computation Security in Drone Video Analytics", *IEEE Applied Imagery Pattern Recognition (AIPR) Workshop*, 2020.
[7] A. Esquivel Morel, E. Ufuktepe, C. Grant, S. Elfrink, C. Qu, P. Calyam, K. Palaniappan, "Trust Quantification in a Collaborative Drone System with Intelligence-driven Edge Routing", IEEE/IFIP Network Operations and Management Symposium (NOMS), 2023.

ZT-based Network-edge and computation security

Data flow diagram to show micro-segmentation of risk within CDS components



- Enforcing "law of least privilege" access such that any device/service with a certain role or responsibility in the mission, as well as commanders/soldiers have regulated/time-constrained access privileges.
- Investigate strategies for data classification, encryption, data/file activity management, key management.
- Creating a "separation of duties" where multiple/diverse entities establish trust in a transaction (versus a single trusted entity) and verify the reason for access.

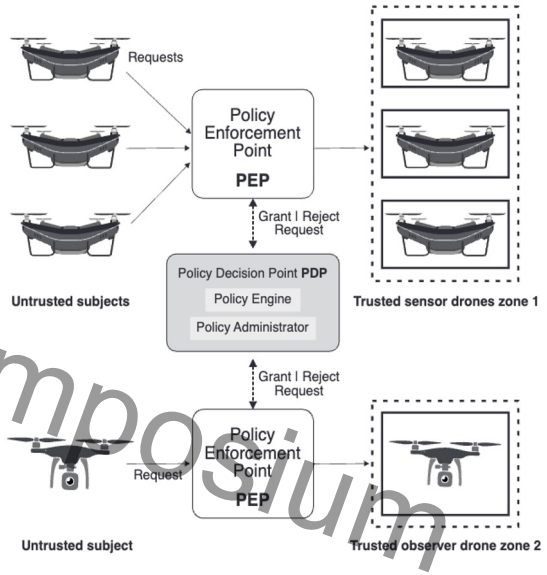
Arculus framework design and architecture

ZT Manager managing a hierarchical drone swarm system

NIST ZT model guidelines (i.e., SP 800-207 and SP 800-201) as well as the state-of-the-art in the Enterprise setting

Authentication and Authorization ⇔ Data Collection and Management ⇔ Policy Attributes

Hierarchical drone swarm systems feature a number of **sensor drones** (that are relatively cheaper and are used for surveillance) working with a more capable **observer drone** (that has high-end sensor equipment that is used for intelligence collection at a scene-of-interest)

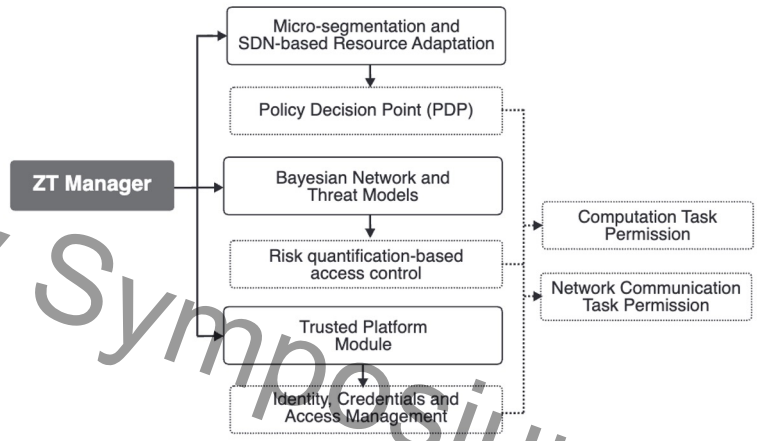


Arculus framework design and architecture

Zero Trust Management components design

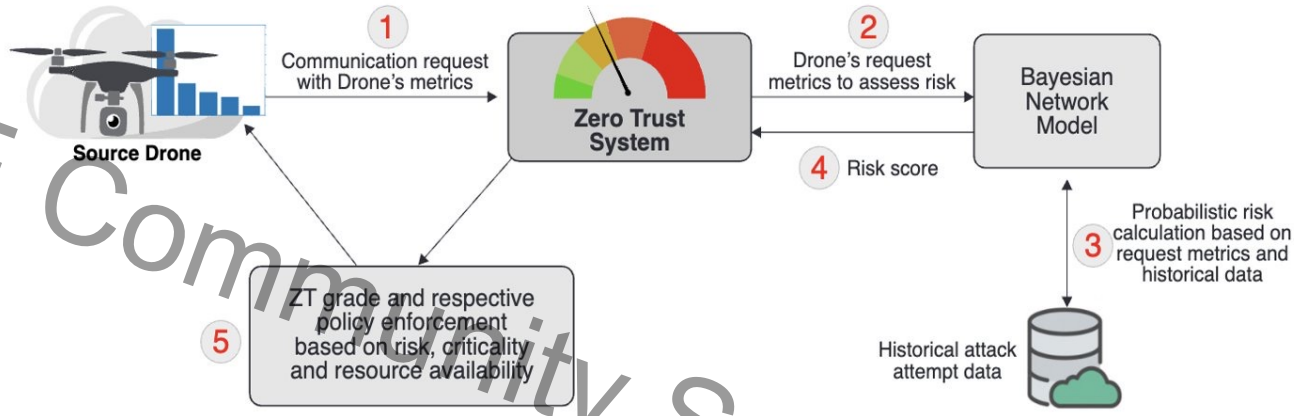
- **The ZT Manager** uses a centralized policy management strategy to **apply automated and/or manual policies** for **multi-layered micro-segmentation** and **SDN-based resource adaptation** to improve security at the container, cluster and network communication layers with a minimal performance impact.

- **Micro-segmentation**, which will be the foundational property of the architecture prevents lateral movement of threats and is achieved by employing a **Function-based Access Control strategy**.



ZT Manager components that provide secure network communication and computation through centralized policy management

Risk-based Zero Trust Scale for Tactical Edge Networks



- A source drone communicates with the ZT system, which retrieves and sends information from the BN model respectively. This BN model at the same time, collects and checks probabilistic risk calculation requests, including historical data.
- The historical data is saved in a dataset. The ZT system interacts with the drone by updating a grade and a respective policy enforcement base on risk, criticality, and resource availability

[8] S. Poduvu, S. Saghaian N. E., E. Ufuktepe, A. Esquivel Morel, P. Calyam, "Risk-based Zero Trust Scale for Tactical Edge Network Environments", *ACM Trustworthy Edge Computing Workshop, 2023.*

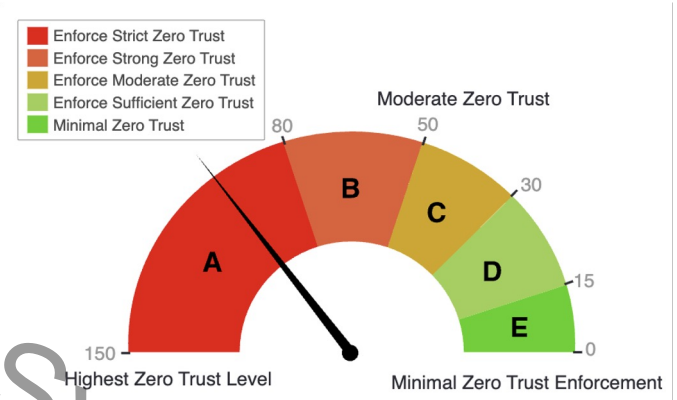
Sliding-scale Zero Trust Method

Based on Risk Quantification and Threat Detection

Coupling the "risk score" with the five grades (i.e., A to E) of "ZT Scale" of security controls thus provides a TWE environment-resource-aware method to apply necessary security controls to protecting users and assets, their interactions, workflows, and ultimately their risk levels

	Value
Use of passwords for software/hardware/user with or without multi factor	+20
Trust in CA	+10
Use of default timeouts for V&V of certificates	+20
Each software module allowed access to infrastructure files	+5
Excessive white listing, per occurrence, in excess of 3	+5
Each software module allowed access to private key of server or HSM	+20
Use of SSO	+20
Each breakage of end-to-end encryption	+20
Each identity proxy	+20
Any unencrypted traffic flow	+20
Any modification of traffic content	+20
Any segmentation above micro-segmentation	+20
Every other instance of explicit trust	+20
Server-side authentication only	+20
Multi-factor authentication of software	-5
Multi-factor authentication of servers	-10

Zero trust factors table



Risk-based ZT Scale with Grade Categorization. Highest Zero Trust Levels, Moderate Zero Trust and Minimal Zero Trust Enforcement.

Different values are given to different ZT factors and corresponding security controls

It can be observed that the **use of passwords for software/hardware/user with or without multifactor has a value of +20,** which given our sliding-scale ZT meter, **would correspond to a strong ZT scale**

Sliding-scale Zero Trust Method

Performance Evaluation Experiments

Evaluation of the BN's performance based on metrics such as packet transmission rate, distance from the control station, and energy levels of drones.

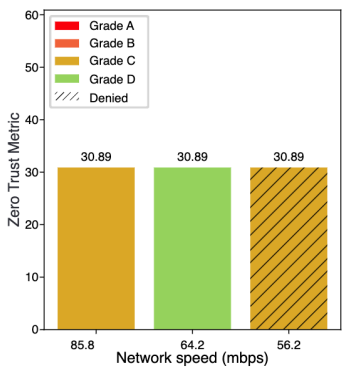
We also analyze the influence of key ZT parameters, namely Criticality, Compute Easer, and MSP, on security execution.

Experiment scenarios showing:

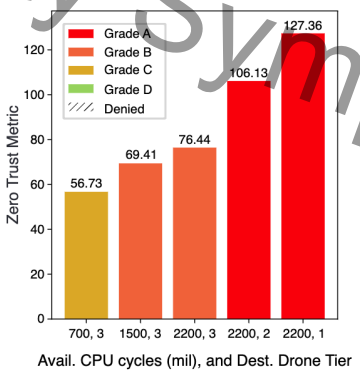
(a) Effects when ZT security policies are enforced fully or partially or denied

(b) Effects of the Available CPU Resources on the ZT Metric and corresponding ZT grades

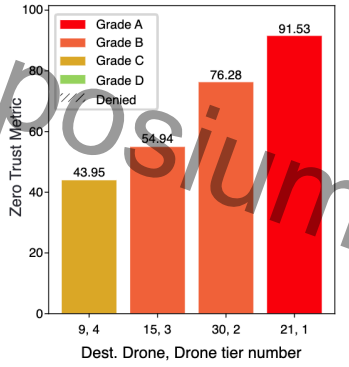
(c) Effects of the Criticality parameter on the ZT Score and corresponding ZT grades



(a)



(b)

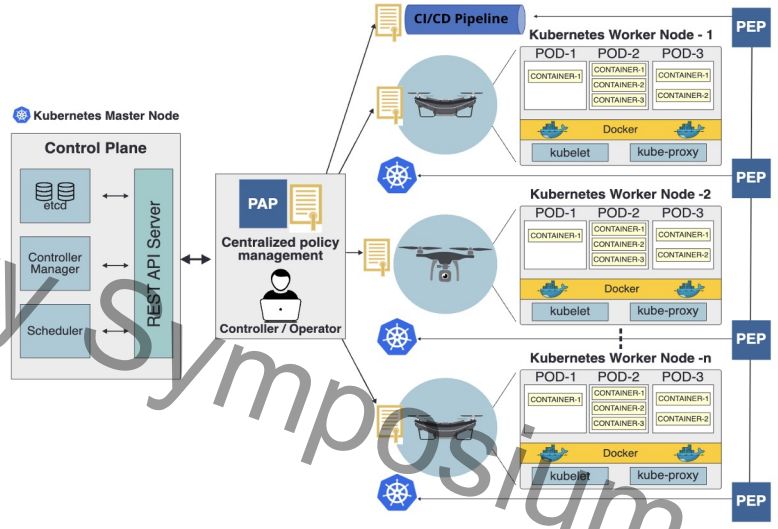


(c)

Towards implementation for automation of control policies

Arculus Demo Testbed

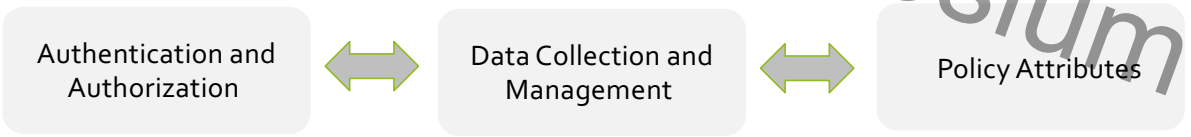
- **Monitoring methodologies** can be adapted for programmable network services deployment and their management, including credentials/commands used on edge devices (e.g., Raspberry Pi).
- **Enforcing security controls** by applying e.g., attribute-based user access control, network micro-segmentation using Kubernetes (k3s).
- **Defense by Pretense methodologies** can be integrated with distributed honeypots that can report intrusion attempts, or verify legitimate or misconfiguration actions; threat intelligence sharing of script downloads, privilege escalation, etc.



[Arculus] Low Overhead Zero Trust Solution for the Tactical Warfighting Edge

Conclusions

- We are developing a resource-aware security approach to address edge resource constraints and enable real-time decision-making.
- Our risk-based ZT scale approach tailors security measures to scenario-associated risk levels, while having low resource overheads.
- We devised a Bayesian Network (BN) model to evaluate communication request risk based on metrics indicating possible attacks.



Thank you!

POC: Prof. Prasad Calyam
(calyamp@missouri.edu)

Department of Electrical Engineering and Computer Science,
University of Missouri-Columbia