Zero Trust and Identity Access Management in Support of Service-Based Urban Air Mobility Applications

Steve W. Garcia
Intrinsyx Technologies Corporation

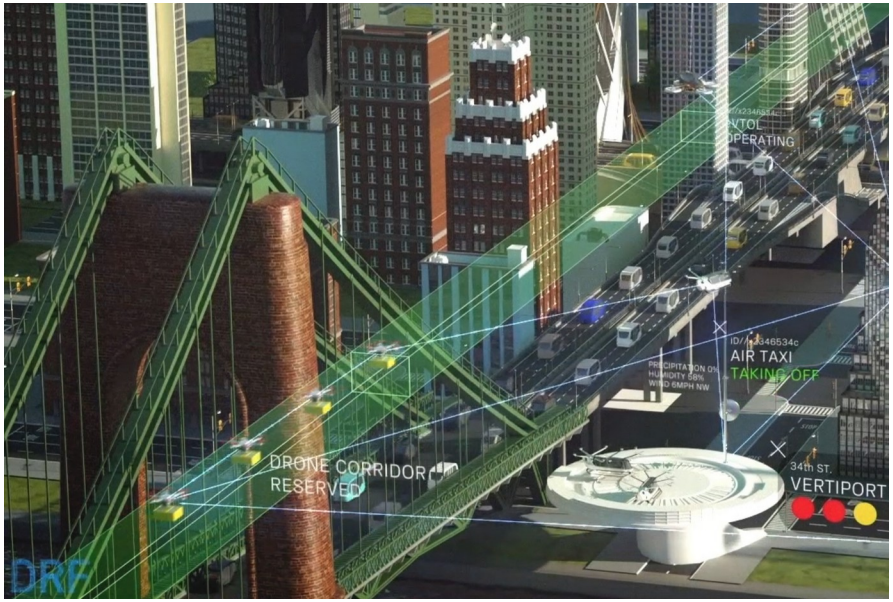
Kenneth Freeman
NASA Ames Research Center

AIAA Aviation Forum 2021
August 2 - 6

UAM Environment

The vision for Urban Air Mobility (UAM) is to enable efficient and safe air traffic operations in a metropolitan area for manned aircraft and unmanned aircraft systems.

- The UAM environment has a service-oriented architecture where UAM operators and service providers work independently to mange aerial vehicles in the urban environment.
- The UAM environment is derived from the Unmanned Traffic Management (UTM) concept of operations.
- Providers of Services, UAM operators, and Supplemental Data Service Providers provide services to support flight operations within the UAM environment.
- A method for security trust will need to be established across multiple UAM service providers.



Source: https://www.nasa.gov/feature/data-reasoning-fabric-drf

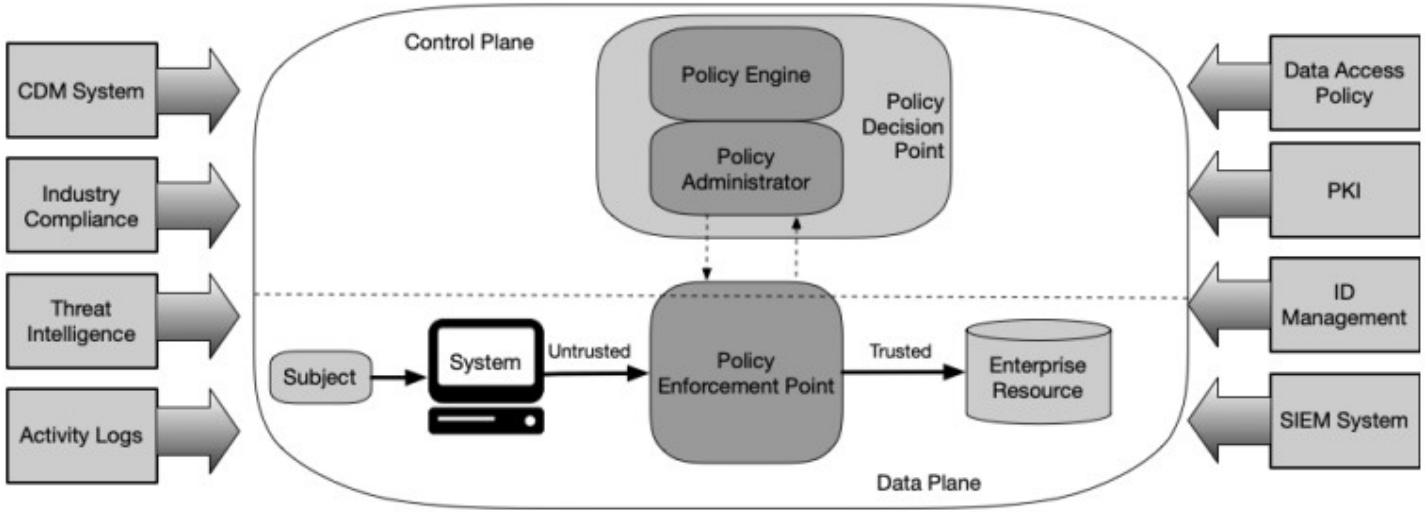
What is Zero Trust

- According to the National Institute of Standards and Technology (NIST)
  - Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.
  - A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows.
  - Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

Zero Trust View of a Network

- The entire enterprise private network is not considered an implicit trust zone.
- Devices on the network may or may not be owned or configurable by the enterprise.
- No resource is inherently trusted.
- Not all enterprise resources are on enterprise-owned infrastructure.
- Remote enterprise subjects and assets cannot fully trust their local network connection.
- Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent.

Zero Trust Logical Components



CDM – Continuous Diagnostics and Mitigation / Monitoring
PKI – Public Key Infrastructure
SIEM – Security Information and Event Management

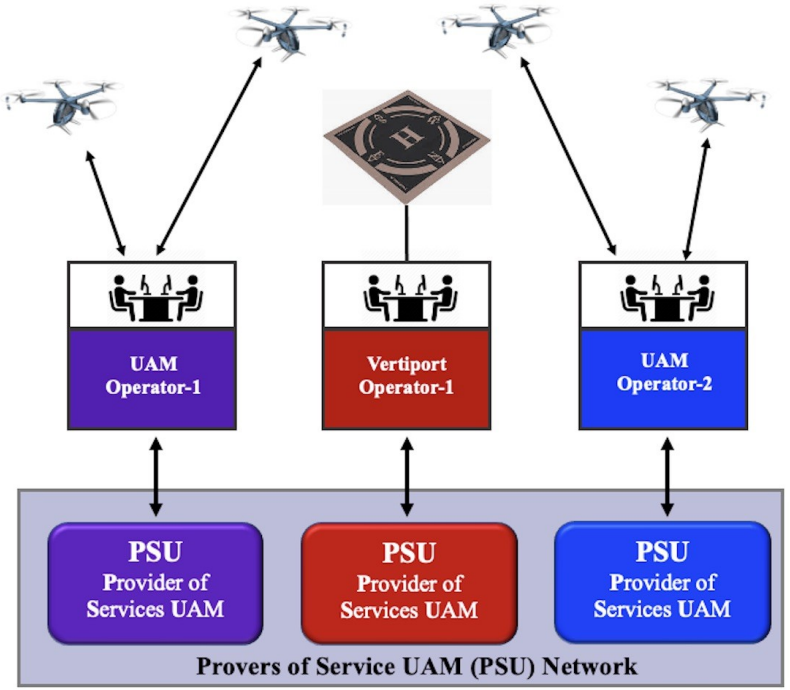
ZTA Control Plane

- Policy engine (PE): This component is responsible for the ultimate decision to grant access to a resource for a given subject.
  - The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision.
- Policy administrator (PA): This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs).
- Policy enforcement point (PEP): This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

UAM Identity and Access Management (IAM)

- Properly managing access to systems, processes, and information is central to managing cybersecurity risks and a priority for NIST's cybersecurity and privacy program.
- Digital identity is the unique representation of a subject engaged in an online transaction. The process used to verify a subject's association with their real-world identity is called identity proofing.
- Authentication establishes confidence that the claimant has possession of an authenticator(s) bound to the credential, and in some cases in the attribute values of the subscriber.
- NASA UAM will require access from outside entities. ZTA and IAM will be necessary to provide the required protection of the UAM data and system.

How Can ZTA / IAM Work in UAM



- In a UAM environment, the combination of identity and access management (IAM) coupled with ZTA policy engine and policy enforcement points will determine access to resources.
- For instance, access between resources within within a UAM Operator network are controlled by ZTA police, in addition to access from external sources.

References

Computer Security Resource Center. CSRC. (n.d.). https://csrc.nist.gov/glossary.

Grassi, P., Garcia, M., & Fenton, J. (2020, March 2). *Digital Identity Guidelines*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-63/3/final.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *Zero Trust Architecture*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-207/final.

AMERICAN INSTITUTE OF
AERONAUTICS AND ASTRONAUTICS