EXTENDING ZERO TRUST TO DELAY AND DISRUPTION TOLERANT NETWORKS (DTN) IN SPACE

Dr. Alberto Montilla Bravo, Alberto Montilla Ochoa

SPATIAM CORPORATION

AGENDA

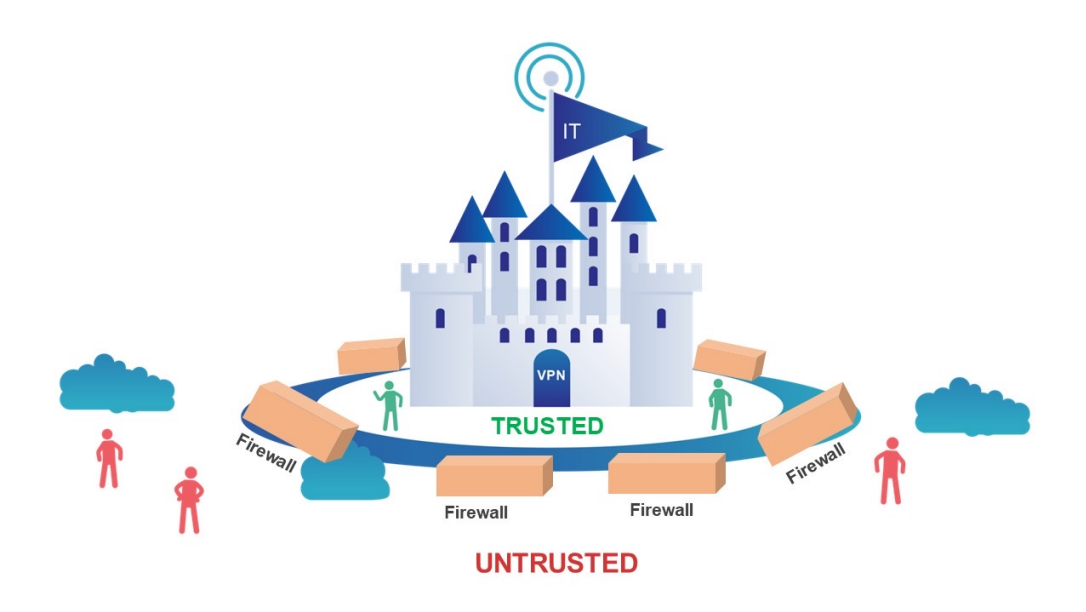
- Introduction – Challenges of “network” security.
- Concept - Extending Zero Trust to DTN (for Space)
- Considerations
- Example applications
- Conclusions and future work

“OUR ADVERSARIES ARE IN OUR NETWORKS, EXFILTRATING OUR DATA, AND EXPLOITING THE DEPARTMENT’S USERS”

DoD Zero Trust Strategy. Open Publication. US Department of Defense. 2022.

INTRODUCTION - NETWORK SECURITY

Perimeter Model (aka Castle and Moat)



- The security stack (firewalls) creates a network perimeter (Moat) around a centralized Data Center (Castle).
- Firewalls contains network protocols, configurations, and rules.
- VPNs are explicit trusted access mechanisms to extend the private network access to internet users.

INTRODUCTION - BREACH

1 Attack surface identified

- External identifiers,
- Firewalls,
- DMZ,
- VPN…

2 User compromised

- Exploiting the trust of common services
- Directly target exposed services and/or entice end users.

3 (Network) Lateral Move

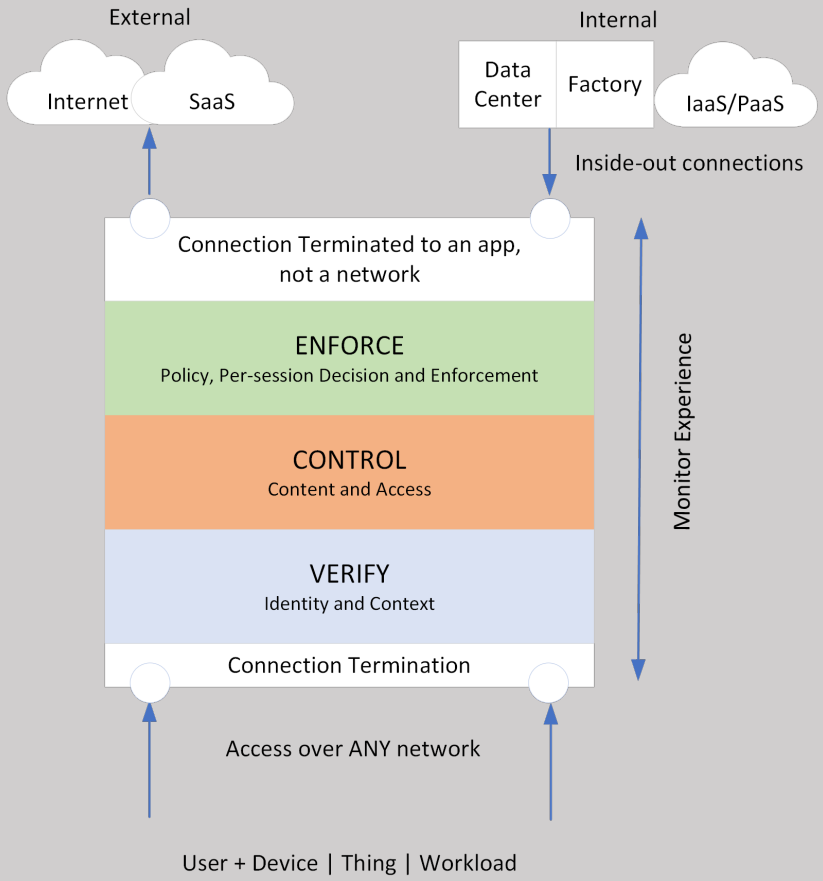
- Once in, access other applications, servers in same network.

4 Data Theft

- Leverage trusted services to set up back channels and exfiltrate data.
- Customer Data, PII, IP
- Ransomware.

ZERO TRUST
NEVER TRUST, ALWAYS VERIFY

1. What's connecting
2. What is the access context
3. Where is the connection going
4. Assess risk (adaptive control)
5. Prevent Compromise
6. Prevent Data Loss
7. Enforce Policy



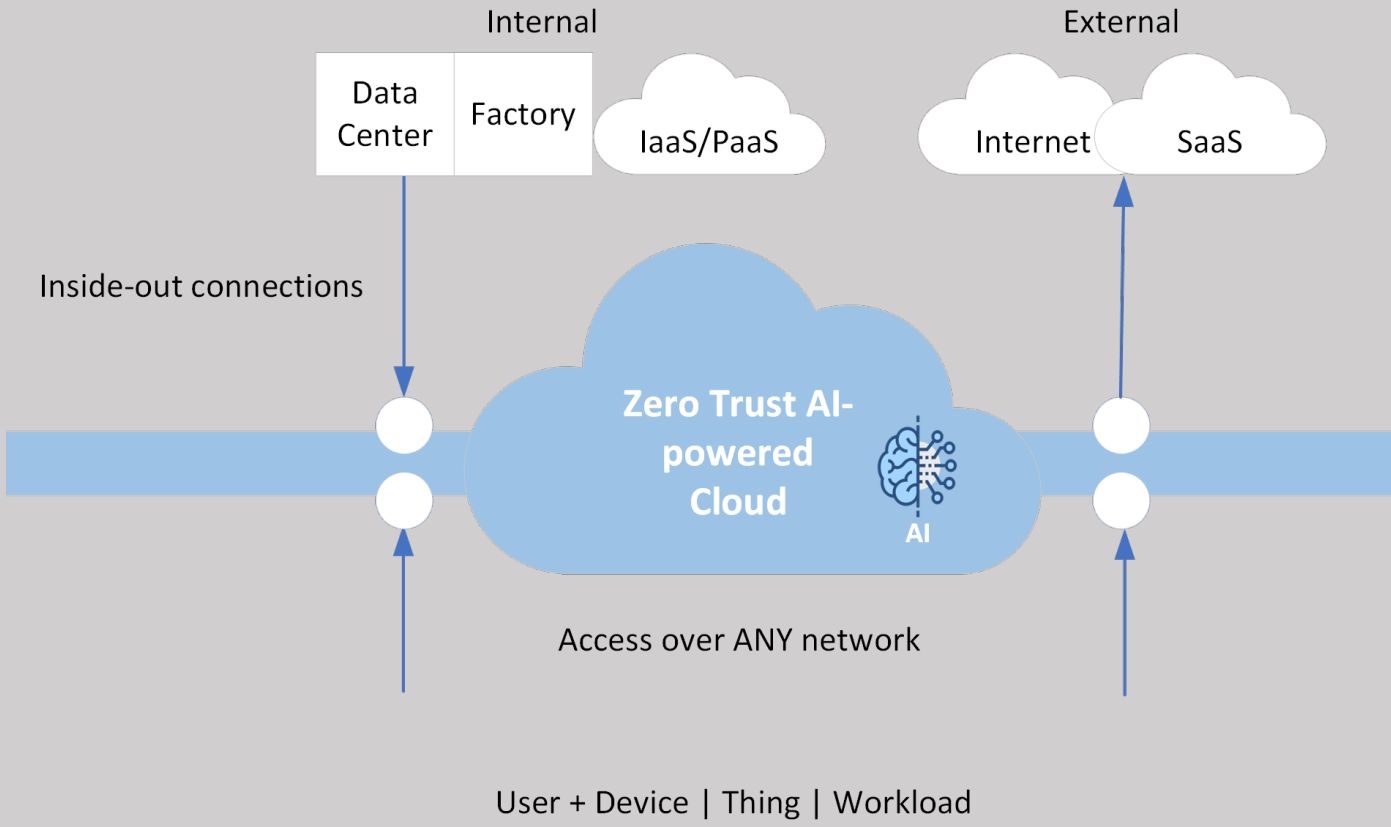
From Zscaler – Seven elements of Highly Successful Zero Trust Architecture

ZERO TRUST

AI-Powered “Cloud” Architecture

AI is used extensively inside the Zero Trust Cloud (aka Exchange) to:

- Analyze user behavior
- Assess risk and mitigation
- Threat detection
- Prevent malware by incorporating AI-powered sandboxes for Decoy



ZERO TRUST FOR DTN

Application Security Considerations

	Internet Architectures		DTN	
	Legacy Network and Security	Zero Trust	Existing Network and Security	Zero Trust for DTN considerations
Attack Surface	Firewalls/VPNs published on the Internet Can be exploited, susceptible to DDoS	Apps not exposed to the internet. You can't attack what you can't see	Contact plan is "too" open, BPSec and access lists Can be exploited, susceptible to DDoS	BIBE + application-level contact plans.
Connection	Apps access requires corporate network access Allows lateral movement of users and threats	Connects a specific, authorized user to a specific, authorized resource	Endpoint identifiers, easily guessable, subject to lateral movement. Relies on specific network security.	Challenged due to round trip time
Proxy/Pass-through	Firewall/pass-through Inspects a limited data buffer Unknown files pass through Alerts after infection	Proxy Full content inspection, including TLS/SSL Hold and inspect unknown files before reaching the endpoint	No content inspection defined (of any type) as of today.	Does not rely ONLY on centralized cloud architecture - Key infrastructure - Centralized AI for protection
Tenancy	VMs of single-tenant appliances in a public cloud	Cloud-native, multitenant design	Single tenant appliances today	Multi-tenant and air-gapped networks are orthogonal

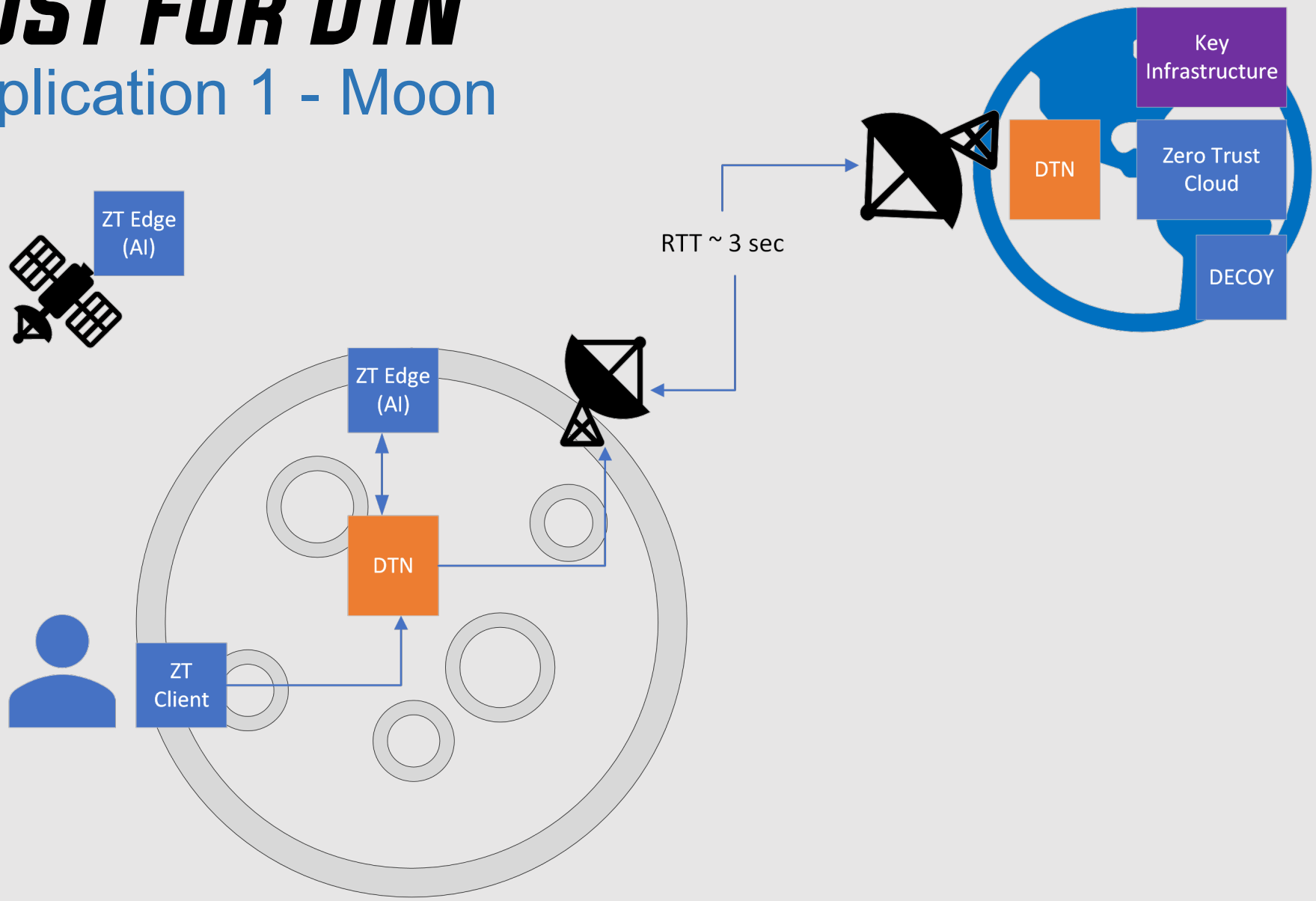
ZERO TRUST FOR DTN

Architectural Considerations

		DTN	
	Zero Trust (as of today)	Existing Network and Security	Zero Trust for DTN considerations
Tenancy	Cloud-native, multitenant design	Single tenant appliances today	Multi-tenant Note: Air-gapped networks are orthogonal to multi-tenancy
Cloud	Use of centralized and distributed cloud infrastructure.	Does not rely on cloud infrastructure but distributed nodes.	Hybrid networks (distributed with “processing” centers).
AI use	Centralized on public cloud	Does not rely on AI for basic security.	Edge and core AI is needed depending on planetary distances and settlement size.
Key infrastructure	PKI-like infrastructure	PKI or Distributed Key Architecture	PKI and Distributed Key Architecture.
Application Profiling	Extensive profiling of public cloud applications.	There are not existing profiles for standard applications (e.g. CFDP)	

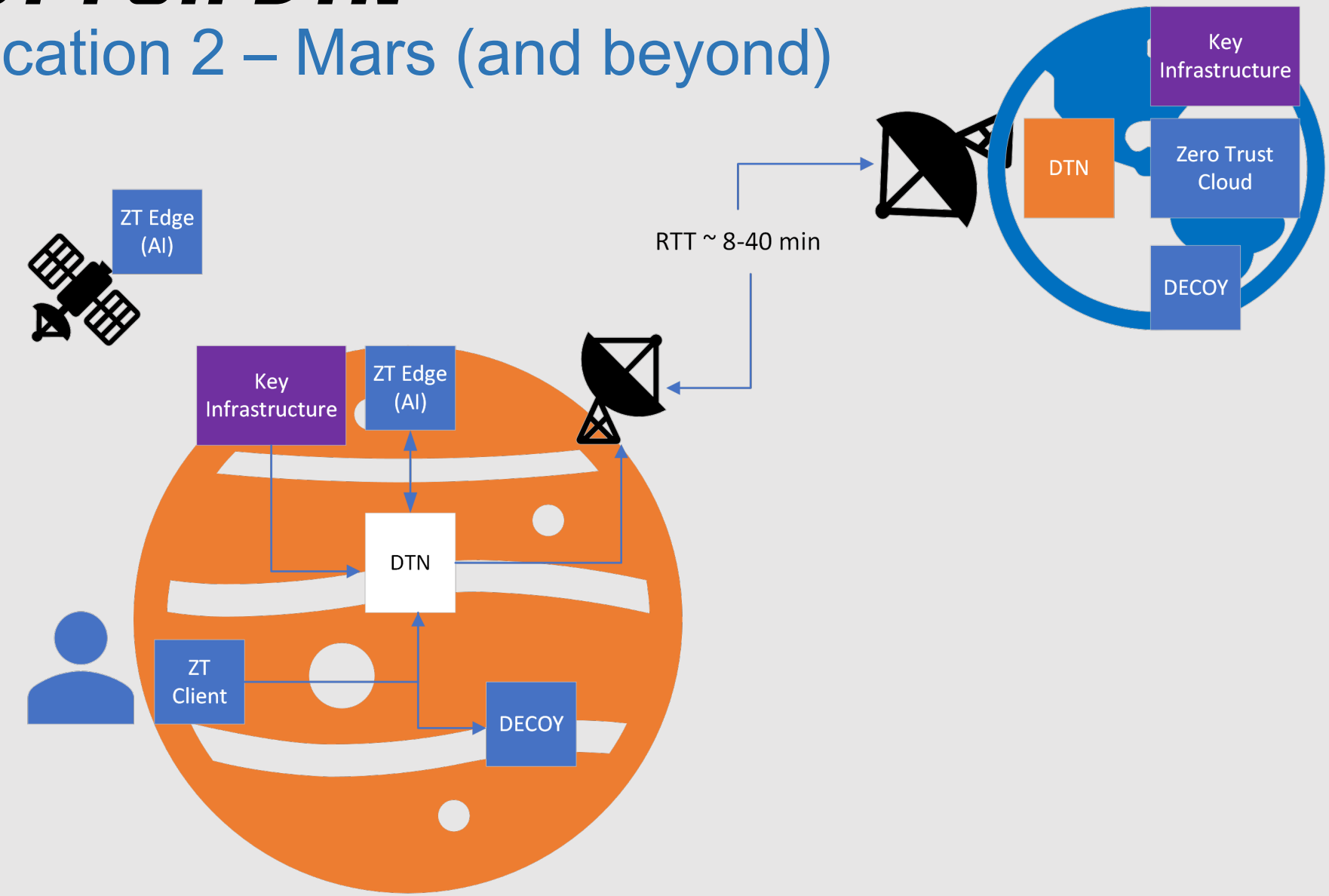
ZERO TRUST FOR DTN

Example application 1 - Moon



ZERO TRUST FOR DTN

Example application 2 – Mars (and beyond)



ZERO TRUST FOR DTN

Conclusions and future work

- DTN network and application security must be analyzed in context of the modern internet threats
- Zero Trust architecture is a current effective architecture that must be adapted to DTN Networks in space.
- Further work is required to experiment and validate ZT-DTN
  - Distributed AI (Edge + Centralized) to profiling and detect attacks to DTN Nodes and Endpoints.
  - Distributed Key Architecture is required for longer delays where round trip makes a centralized ZT Cloud (on Earth) impractical.
  - Decoys may be distributed in longer delay (Mars) scenarios.
  - Bibe and Exit nodes may not be sufficient to hide the path between two BP Endpoints.

THANK YOU!

EXTENDING ZERO TRUST TO DELAY AND DISRUPTION TOLERANT NETWORKS (DTN) IN SPACE

Dr. Alberto Montilla Bravo, Alberto Montilla Ochoa

SPATIAM CORPORATION

ABSTRACT

Zero Trust is an application security architecture for the terrestrial internet. It is anchored in five main assertions: (1) a hostile network, (2) both internal and external threats are always present in the network always, (3) network locality in not sufficient in deciding trust, (4) every device, user, and network flow is authenticated and authorized, and (5) policies must be dynamic and calculated from as many sources of data as possible. Artificial Intelligence is used extensively in the Zero Trust architecture given the massive amounts of data features to consider when analyzing every user, application, and network. Use cases of AI application on Zero Trust Networks include risk-based security strategies, dynamic security policies and dynamic authentication factors.

In this presentation, we explored the adaptation of this architecture in Delay and Disruption Tolerant Networks for deep space, analyzing key considerations, including the need for autonomy, and the limitations of centralized networking in deep space. We elaborate on specific security use cases that could be delivered with this adapted architecture. Last, we describe further areas of exploration that must be addressed.