

Securing UTM Airspaces Through Adaptive Zero Trust Architecture

The background image shows four military helicopters, likely Apache, flying in a staggered formation across a bright, cloudy sky. Below the helicopters, a landscape is visible featuring several large, low-rise buildings with reddish-brown roofs, possibly hangars or barracks, situated in front of a dense line of green trees. The overall scene suggests a military or aviation-related context.

By: Brodie Watson, Srivanth Dhulipala, DJ Striegel, Carlos
Ortiz Callao, Nic Dmitriev

Securing UTM Airspaces Through Adaptive Zero Trust Architecture (ZTA)

UTM cannot scale unless access control decisions are dynamic, continuous context-aware, and resistant to lateral movement.

The failures:

- Static security: current RBAC/ABAC are too static to handle rapidly changing flight conditions.
- Implicit trust: trust zones enable attackers to move laterally across networks.
- Context gap: static rules cannot adapt to dynamic mission factors (weather, location, status)

The solution: ZTA is the superior and more secure approach for real-time UTM demands.

Market Crisis: National Security & Commercial Imperative

Mandate: ZTA is a necessary mandate for a safe, modern airspace, not an option.

Risk Area	Impact of Weak Security	Urgency: Why ZTA Now?
Commercial	Undermines public confidence, risks financial health. UAS Operations face operational errors.	UTM integration into airspace demands ZTA's resilience.
National Security	Exploitable systems allow surveillance and sabotage (e.g., from foreign market dominance)	Safety of the american people relies on reliable airspace control.



Future of UTM

Entities outside of national control are introducing new threats to current UTM security standards. For this reason:

- UTM market is directly affected by unsafe UTM management
- Surveillance, weaponized aircraft, uncontrolled airspaces all lead to lost money
- Stakeholders outside of UTM environments affected

Why is ZTA the best future-proof solution for stakeholders?

- Cost-effective solution for protecting privacy and enforcing security
- Scalable and applicable to all UTM environments, regardless of systems
- Adaptive response for rapidly changing tasks

Threats to UTM Functionality

Attack surfaces: Threats exist during pre-flight, flight, and post-flight stages of UAS operations. ZTA directly mitigates these risks through least privilege access, encrypted channels, and strict identity verification.

Threat Name	STRIDE Category	UTM Block Affected	ZTA Mitigation Example
Pilot Impersonation	Spoofing (Identity)	U2 Flight Authorization	Enforce ABAC and consistent mTLS communication
Manipulation of diagnostics	tampering	U3 tactical deconfliction	Implement RSA key exchanges and AES encryption
Abnormal traffic	DoS	USS service availability	Deploy firewalls with IPS; implicitly deny entrusted traffic.
Profile Pattern Recognition	linking	U-space public trust layer	Limit leaks by strictly enforcing ZTA layered protection, and threat hunting
Flight data sharing	disclosure	Remote ID/monitoring	Encrypt all data; securely store keys.

Threats to UTM Functionality

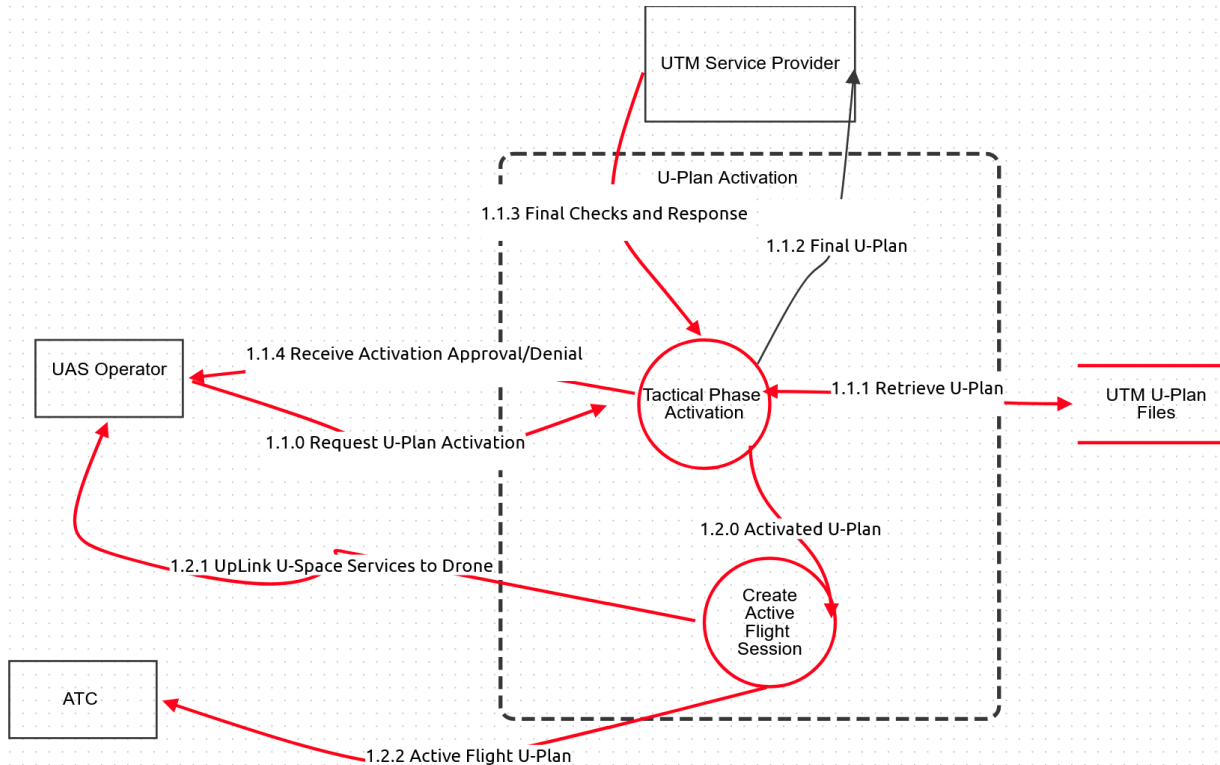
Privacy threats arise when UTM systems expose metadata, patterns, or outdated components. ZTA reduces these risks through strong encryption, minimized data exposure, and continuous enforcement of compliance requirements.

Threat Name	LINDDUN Category	Description	Proposed ZTA Mitigation
Profile Pattern Recognition	Linking	Attacker uses public-facing UTM data to build a profile on common channels, security protocols, and UAS regulations to discover more about potential vulnerabilities	Limit leaks of UTM processes by strictly enforcing ZTA methods, such as layered protection of private information and threat hunting for proactive defense
Flight Data Sharing	Disclosure	Attacker finds high-value personal data through flight plan metadata and system information transmitted during authentication events	Encrypt all data and securely store keys in a safe, private location while also implementing strict physical security involving high-profile victims
Abuse of Compliance Gaps	Non-Compliance	Attacker discovers legacy software and lack of privacy protections	Adhere to all security updates and regulations enforced by UAS administrators

Attack Tree



Proposed Solution - Initial DFD



Key weaknesses exploited by attackers:

Static authorization: non continuous checks allow attackers to preserve access or re-use compromised credentials

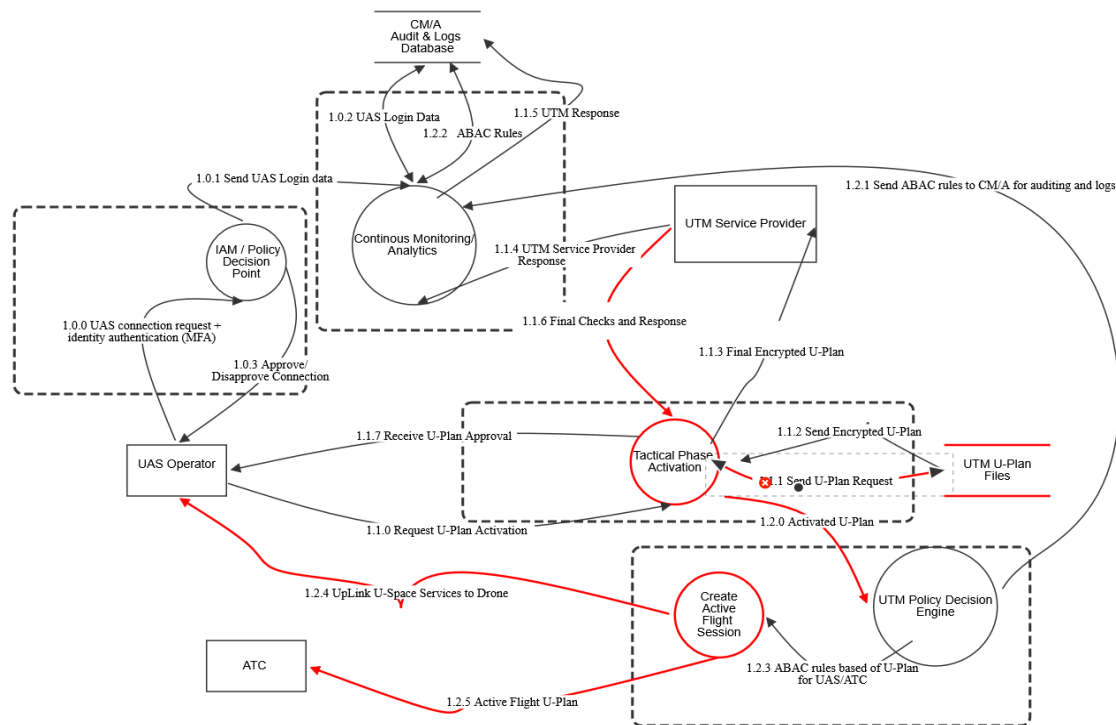
Implicit trust zones: lack of segmentation enables lateral movement

Session persistence: inadequate session revalidation gives adversaries long-lasting access.

Authentication gaps: lack of mutual authentication allows spoofing of vital functions like telemetry.

Proposed Solution - Final DFD

Focus: Applying zero trust tecture (ZTA) principles g tactical phase activation.



IAM Policy Decision Point: Verifies identity (MFA) and approves/denies UAS connections.

Continuous Monitoring (CM/A): logs UAS login data, ABAC rules, and UTM responses ABAC rules to ATC and UAS operators.

Trust Boundaries: segments critical processes (CM/A, U-plan data) to limit unauthorized lateral movement.



Good afternoon,
I'm your personal assistant

🔔 We have your next appointment set
for 10:00 AM on 10/10/2020

Book a ride

📅 10/10/2020

Book a ride

📅 10/10/2020

Book a ride

📅 10/10/2020

Book a ride

Book a ride

Book a ride

Book a ride

Book a ride

Book a ride

Book a ride

Customer Activity

Number of active customers by month



Revenue Trend

Revenue by month by quarter



Top 50 Products

Number of products by category



MANAGING RULES

MANAGING RULES

NEW RULE

EDIT RULE

Rule Name

1 2 3 4 5 6 7 8 9 10

Rule Name

1 2 3 4 5 6 7 8 9 10

Associated Business Process (Name) NEW EDIT DELETE +

Based on the following conditions, the system will:

Condition

IF Field 1 is equal to Value 1 AND Field 2 is not equal to Value 2

Then:

Update Field 3 to Value 3

and update the field to the value

OK Cancel

Associated Business Process (Name) NEW EDIT DELETE +

Based on the following conditions, the system will:

Condition

IF Field 1 is equal to Value 1 AND Field 2 is not equal to Value 2

Then:

Update Field 3 to Value 3 and Field 4 to Value 4

and update the field to the value

OK Cancel

Future Outlook



Implementation:
requires careful
planning and
phased rollout in
complex systems.



Performance: ZTA is
computationally
taxing; it requires
scalable infrastructure
for continuous, real-
time verification.



Future: focus on
continued scalability
and integration into
other critical air
traffic management
systems.



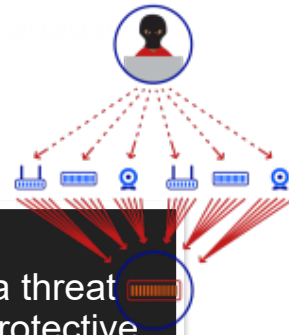
Test Case



John Doe: UAS Pilot, flying with company interface, John wants to login and get approval of his U-Plan

- Attempts to IAM service acts as a gatekeeper (IP whitelisting), attempts login, provides MFA
- Establish secure encrypted channel to host services, login data gets sent to CM/A service
- John sends a request to activate U-Plan, DB responds and sends U-plan to UTM Service Providers,
- DB response is logged, UTM Response is logged
- Activated U-Plan is sent to flight session PDE, uses custom flight algorithms
- PDE applies ABAC rules, ABAC rules are logged, ATC receives U-Plan
- U-Space Services are UpLinked to UAS

ZTA Risks



Complexity in the IAM's PDP algorithm may lead to false positives

Bottlenecks caused by PDP's data ingestion for algorithm may cause scaling issues

ZTA contains a threat actor, is not a protective barrier against all malicious activity

Intensive logging systems causes difficulties in analysis during audits, and/or forensic accounting after an attack

Vulnerable to DDoS

Difficulties integrating ZTA principles with legacy systems

Visibility, Automation, Orchestration

Zero Trust Security



Identity



Endpoints



Data



Apps



Infrastructure



Network

Conclusion

ZTA is a complex approach that involves rigorous implicit trust.

Legacy systems in current UTM environments lack ZTA's robust capabilities.

Education and implementation of ZTA is critical for UAS security.

The proposed solution supports the effectiveness of ZTA while improving efficiency.

