Challenges in Securing the Future of Air Travel

Kenneth Freeman
NASA Ames Research Center

NASA Aeronautics Research

Convergence of Disparate Technologies

- Aerodynamics
- Vertical Lift
- Software
- Batteries
- GPS
- Communications
- Computer Imaging

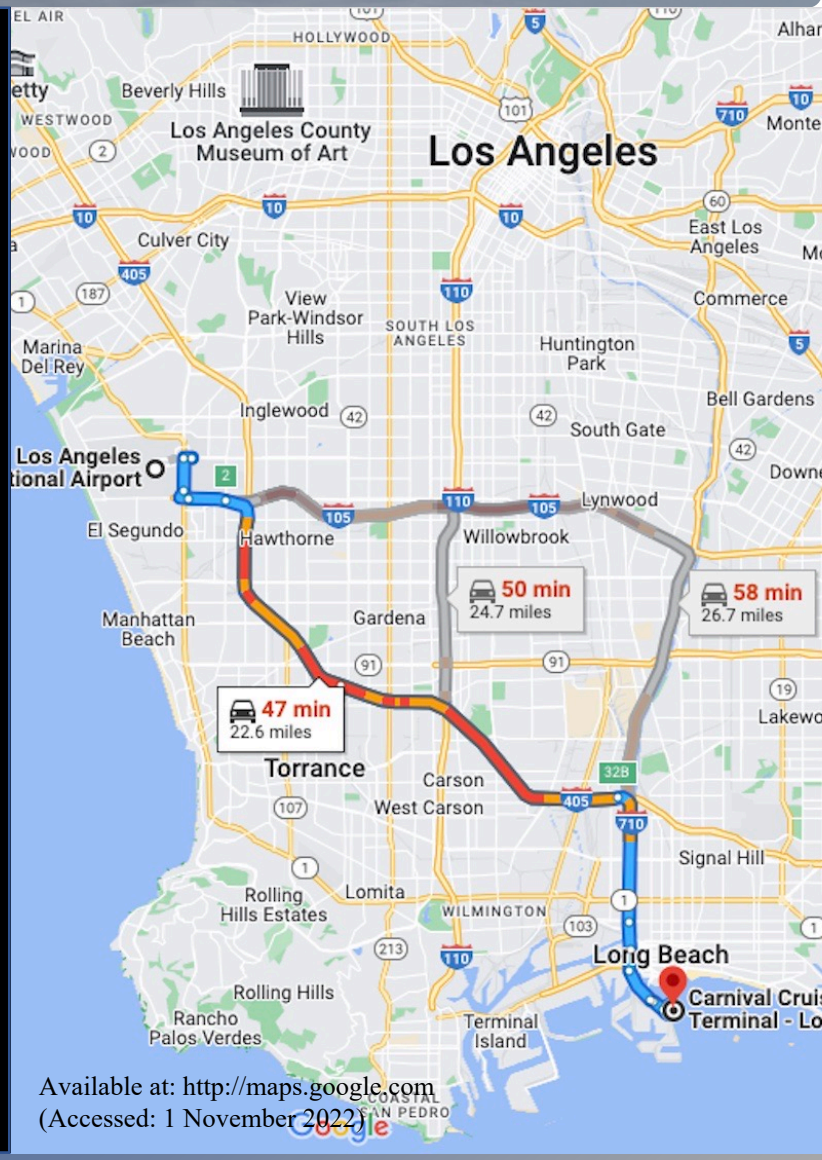
Urban Air Mobility

- Urban air mobility (UAM) is a concept that proposes to develop short-range, point-to-point transportation systems in metropolitan areas using vertical takeoff and landing (VTOL) aircraft to overcome increasing surface congestion

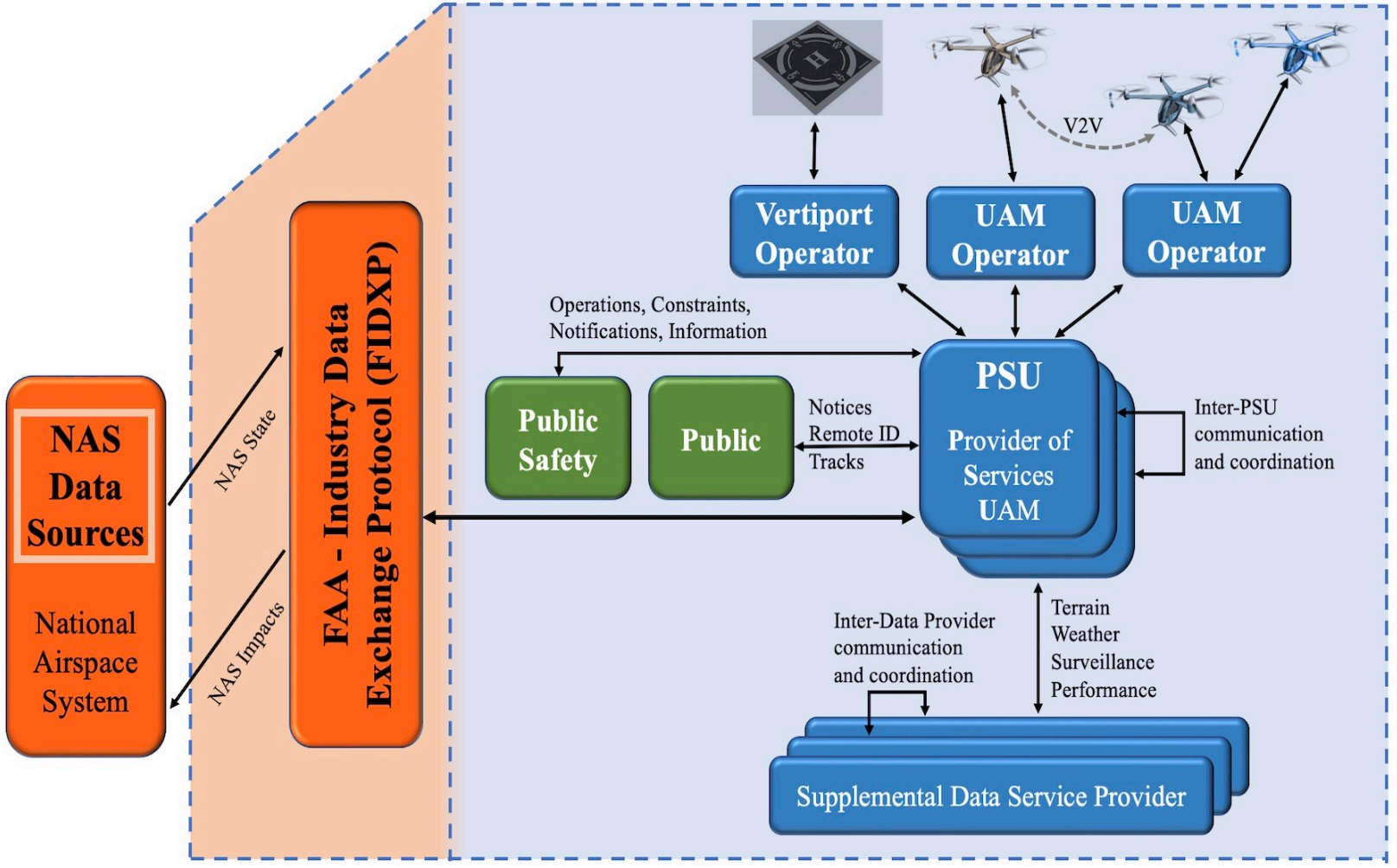
  - To realize the potential of UAM, an assurance of cybersecurity is critical for public acceptance.
  - Cybersecurity has come to the forefront highlighting the need to protect these networks and systems from cyberattacks.
  - The growth in the development of UAM systems, and the associated data exchange and service interactions will be at risk due to numerous types of cybersecurity attacks.
  - As these threats evolve, the UAM cybersecurity capabilities must adapt to these changes as well.

Case Study: UAM Flight from LAX to Long Beach

- Vehicle plans to fly from LAX to Long Beach, CA
  - Need to plan flight path
  - Need coordination with LAX, and other local airport air traffic control
- In-route
  - Need to communicate position, during flight
  - Need contingency plan, in case of problem
- Landing
  - Need coordination with landing site



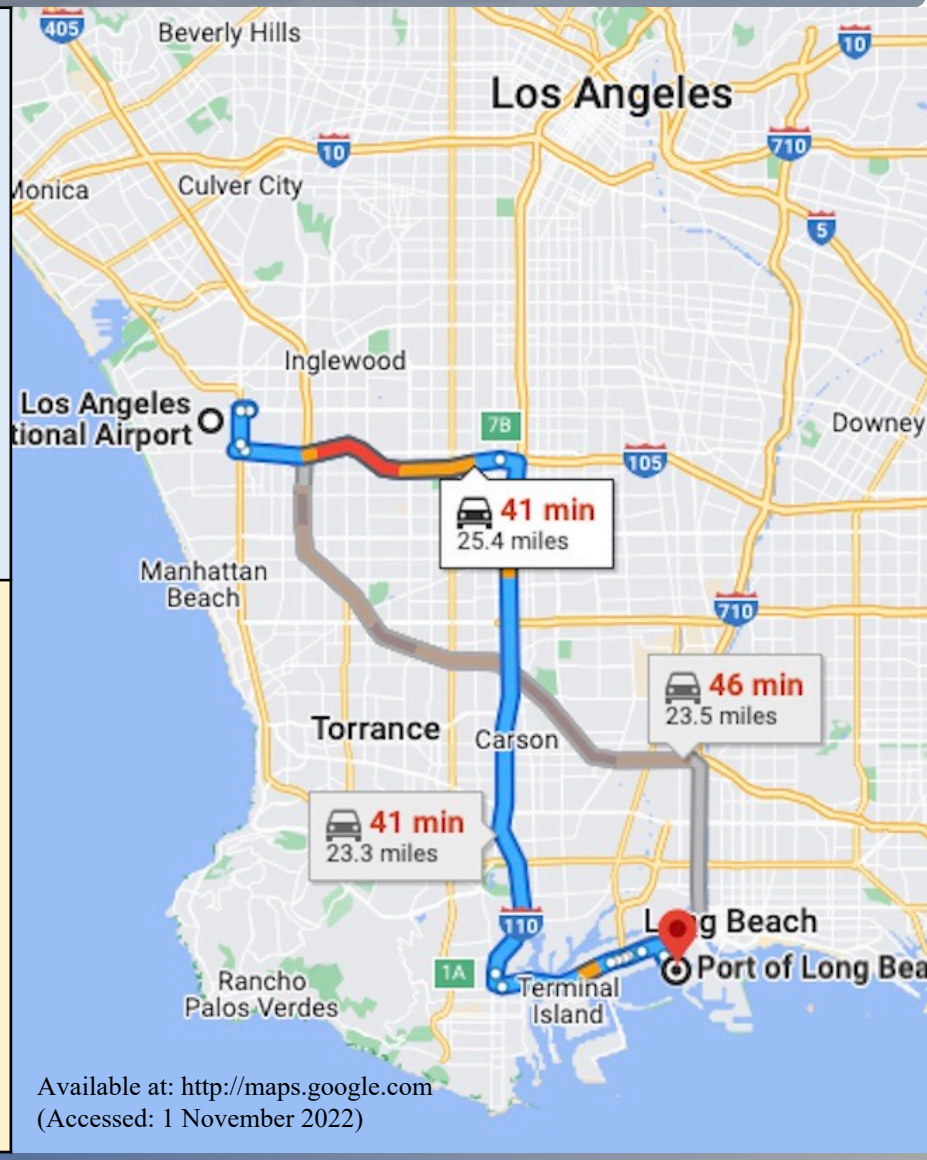
UAM Environment



- 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 operators, vertiport operators, services and the FAA are supported by local computing and cloud services, which are interconnected across various networks

Challenge: Decentralized UAM Operations

Governance	• Will need to determine the overall cybersecurity governance policy across decentralized UAM environments o Will there be common guidance for vulnerability management? o Will cyber attacks and compromises be shared across the UAM ecosystems? o Will there be coordinated incident response plans
Operations	• A trust model needs to be established across the UAM operators and service providers • Need to determine how identities for people and systems will be managed across a decentralized UAM operations

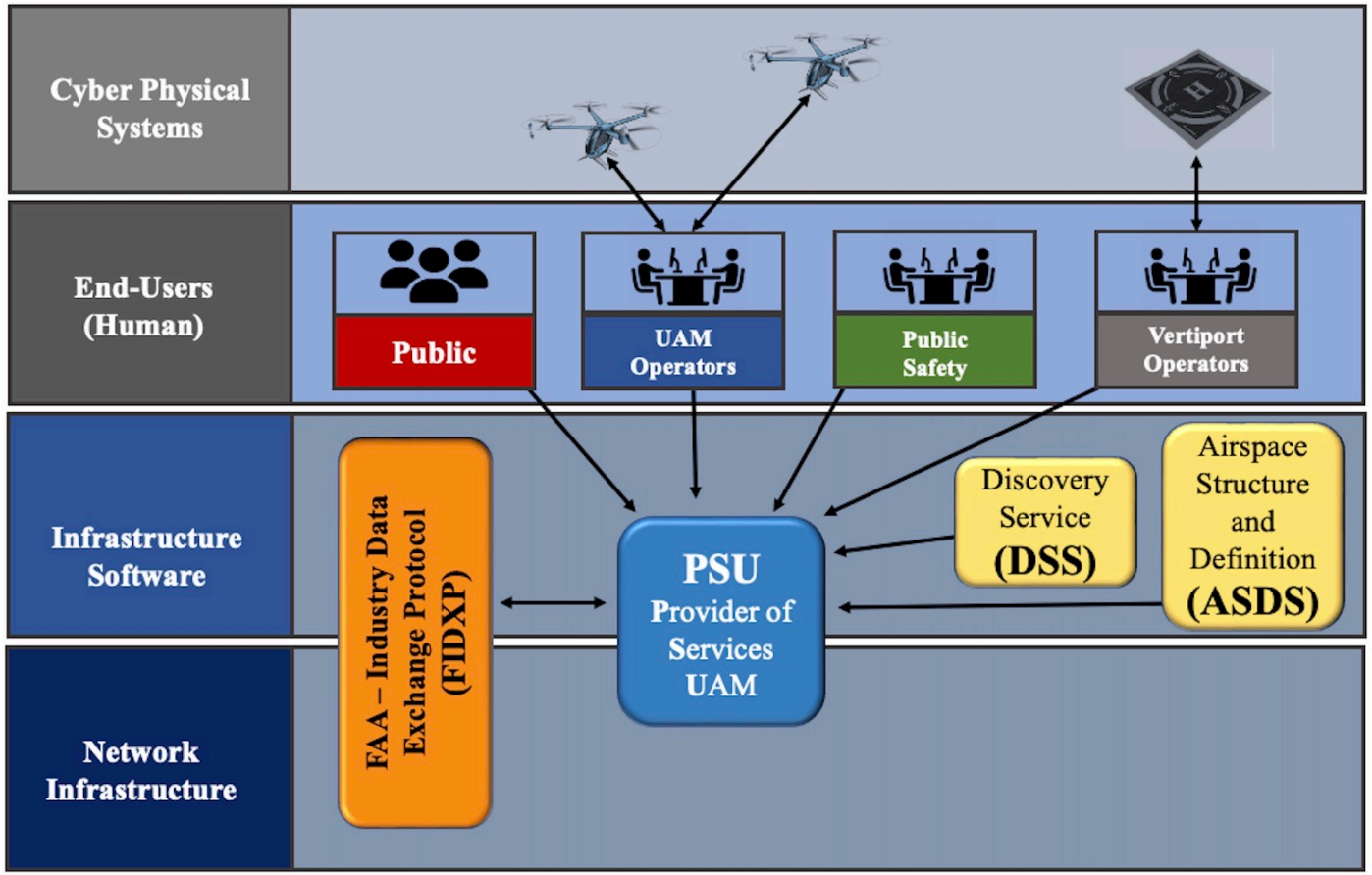


Available at: http://maps.google.com
(Accessed: 1 November 2022)

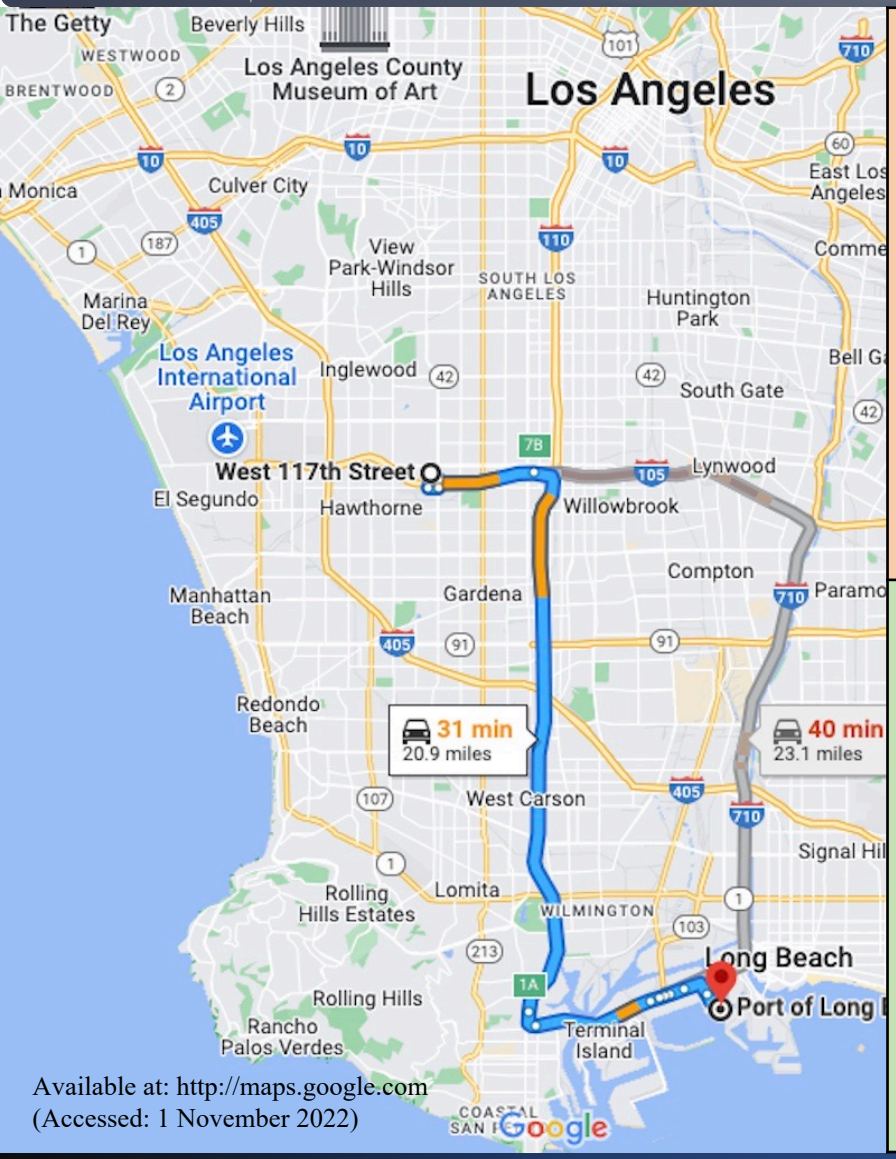
UAM Environment

UAM environments will consist of a wide range of diverse systems supporting flight missions

- The UAM environment can be viewed from the perspective of four significant high-level components, cyber-physical systems, end-users, infrastructure software and network infrastructure.
- Threats, vulnerabilities, weaknesses, and security controls for the UAM environment, are studied from these four components' perspective.
- The applicable threats, vulnerabilities, and weaknesses of the UAM environment's four component areas will differ due to the cyber-physical, cloud, and on-premise architectures.



Challenge: Protecting Cyber Physical Systems

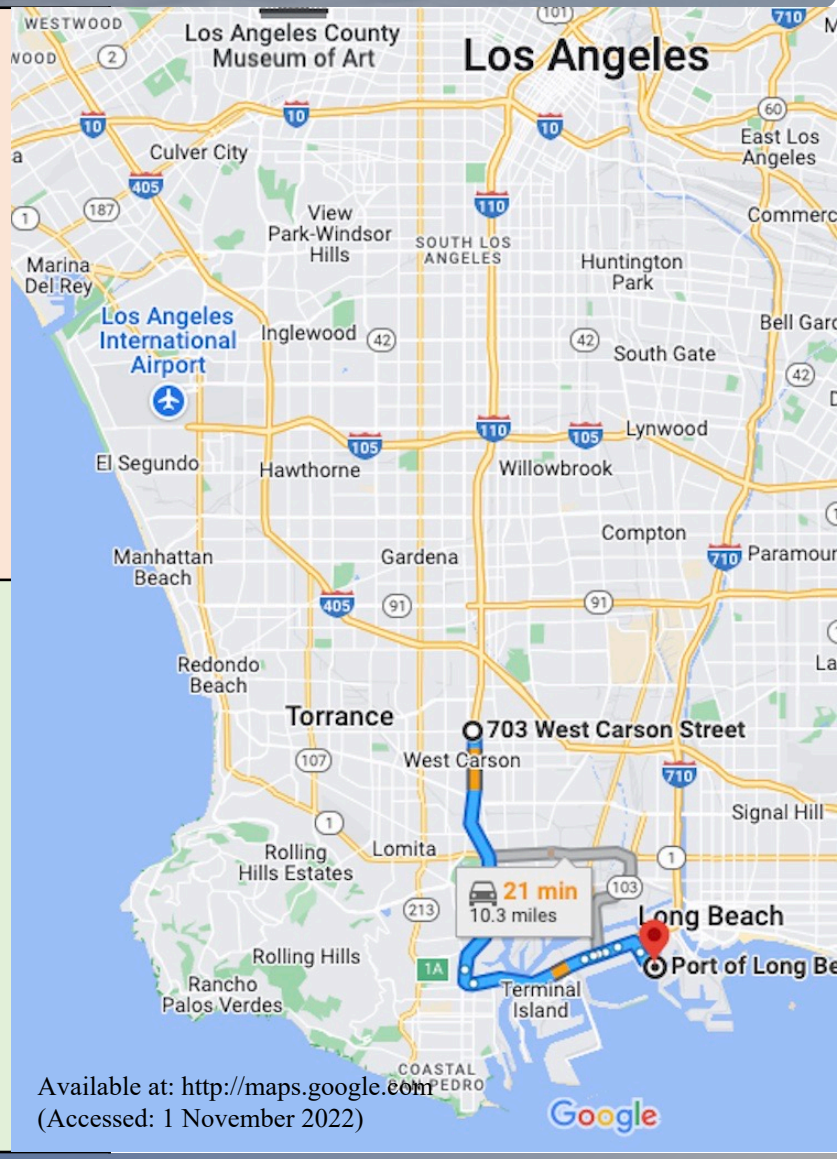


Available at: http://maps.google.com
(Accessed: 1 November 2022)

Threats	• Jamming communications signals • GPS spoofing • Denial of Service (DoS)
Mitigations	• Encrypted communications • Alternate communications options • Alternate position systems • Anomaly detection

Challenge: Human Error (Witting or Unwitting)

Threats	• Social engineering • Ransomware • Insecure design or system misconfigurations • Insider Threats
Mitigations	• Education • Zero Trust • Network segmentation • Continuous monitoring • Ransomware response and recovery planning



Available at: http://maps.google.com
(Accessed: 1 November 2022)

Challenge: Vulnerable Software or Network Infrastructure

Threats	• Broken access control • Cryptographic failures • Vulnerable and outdated components • Injection • Identity and authentication failures
Mitigations	• Construct a pre-incident strategy that includes backup, asset management and restriction of user privileges • Build post-incident response procedures • Strengthen identity proofing and identity recovery (Expand multi-factor authentication (MFA)) • Vulnerability assessments and patching

Challenges in Securing UAM Operations

Questions