Evaluating Lightweight Certificate-based Authentication for UAV Communications

Project Description

The increasing adoption of Unmanned Aerial Vehicles (UAVs) in civilian, urban, and critical infrastructure applications has brought to the forefront the need for reliable and secure communication. UAVs often rely on lightweight communication protocols, such as MAVLink, which, by default, lack authentication and integrity mechanisms, leaving them vulnerable to spoofing, replay, and injection attacks. Although MAVLink version 2.0 introduces optional packet signing using HMAC, this feature is not enabled by default and depends on pre-shared symmetric keys, which raises scalability and key management concerns.

To address these gaps, the IETF DRIP working group proposed a Public Key Infrastructure (PKI) model through the DRIP Entity Tag (DET), enabling strong asymmetric authentication using X.509 certificates and a more compact alternative called C509, based on the CBOR (Concise Binary Object Representation) format. However, recent efforts in aviation security (e.g., LDACS systems) and Urban Air Mobility (UAM) highlight the need for adaptable and lightweight authentication methods that minimize cryptographic and communication overhead, especially over constrained links such as SATCOM or urban wireless networks.

This project aims to evaluate and compare authentication mechanisms for UAV communications—balancing cryptographic strength, efficiency, and applicability in real-world deployments. Among them, we include HMAC-based Message Authentication Codes (MACs), symmetric method, frequently used in embedded systems and offering reduced processing cost at the expense of centralized key distribution.

Objectives

1. Implement and compare five authentication mechanisms for UAV communication:
   - **X.509 certificates** (standard PKI)
   - **C509 certificates** (CBOR-encoded compact X.509)
   - **Certificate-free asymmetric signing** (public key transmitted in the clear)
   - **MAVLink v2.0 built-in message signing** (HMAC-based with pre-shared keys)
   - **Symmetric Message Authentication Codes (MAC)** using HMAC-SHA256
2. Evaluate each method in terms of:
   - Message size overhead;
   - Cryptographic processing time (signing/verification);
   - Latency and success rate under simulated conditions;
   - Compatibility with lightweight protocols (e.g., MAVLink).
3. Discuss the trade-offs in applying each method in real-world UAV scenarios, particularly in urban air mobility (UAM) contexts.

Deliverables

- Implementation of Authentication Modules: Functional code implementations for each of the specified authentication mechanisms, adaptable for UAV communication testing.
- Emulation Setup for Wireless Network: A practical emulation environment utilizing a wireless network to test authentication methods in a near-real-world scenario. This setup will integrate with QGroundControl (QGC) for ground station operations and PX4 (or a compatible flight controller software) for UAV-side communication, allowing for hands-on evaluation of the implemented authentication mechanisms.
- Performance Evaluation Report: A report detailing the comparative analysis of each authentication method based on measured metrics: message size overhead, cryptographic processing time, latency, and success rate. This report will cover both simulated and emulated results, including data visualizations and statistical analysis.
- Source Code Repository: A well-documented source code repository of all implementations, simulation scripts, and emulation configurations.

Prerequisites

Mandatory

- Proficiency in Programming: Knowledge and practical experience in a programming language suitable for network simulation and cryptographic operations (e.g., Python, C++, Java).
- Understanding of Network Protocols: Familiarity with fundamental network communication protocols, particularly UDP/TCP.
- Cryptographic Concepts: Basic to intermediate understanding of asymmetric cryptography (public/private keys), digital signatures, and certificate-based authentication (PKI).

Optional/Meriting

- Understanding of lightweight protocols like MAVLink or Crazyflie.

References and Resources

- IETF DRIP Working Group Drafts:
  - draft-ietf-drip-dki-08: Provides the foundational PKI approach for DRIP, including X.509 and C509.
  - draft-ietf-cose-cbor-encoded-cert: Relevant for understanding the development of CBOR-encoded certificates (C509).
- CBOR (Concise Binary Object Representation):
  - RFC 8949: "Concise Binary Object Representation (CBOR)." A fundamental specification for compact data encoding.
  - cbor.me: An online tool and resource for CBOR.
- MAVLink Documentation:
  - MAVLink Guide - Message Signing: Essential for understanding and implementing the MAVLink v2.0 signing mechanism.
  - MAVLink Official Documentation: General information and specifications for MAVLink protocol.
- PX4 & QGroundControl Resources:
  - PX4 Autopilot Documentation: Comprehensive documentation for the PX4 flight stack.
  - QGroundControl Documentation: User guide and developer information for QGC.
- PKI and X.509 Standards:
  - RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." The foundational standard for X.509 certificates.
- Academic Research
  - S. Khan, G. S. Gaba, A. Gurtov, N. Mäurer, T. Gräupl and C. Schmitt, "Enhancing Cybersecurity for LDACS: a Secure and Lightweight Mutual Authentication and Key

Agreement Protocol," 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC), Barcelona, Spain, 2023, pp. 1-10, doi: 10.1109/DASC58513.2023.10311307.

- Suleman Khan, Gurjot Singh Gaba, An Braeken, Pardeep Kumar, Andrei Gurtov, AKAASH: A realizable authentication, key agreement, and secure handover approach for controller-pilot data link communications, International Journal of Critical Infrastructure Protection, Volume 42, 2023, 100619, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2023.100619.