Enabling the Full Potential of UAS Operations through Cybersecurity Innovation

UAS Mission Challenges

Unmanned Aerial Systems (UASs) have become a critical component of modern military operations. The datasets that they capture and share are critical to mission success, so it is imperative that they are sufficiently protected. The evolving complexity in system design, operational utilisation, and technological advancements like swarming necessitates a departure from traditional security approaches, which are no longer adequate or scalable to meet present and future demands.

UASs confront diverse cybersecurity threats targeting communication protocols, sensors, and flight control systems. Maximising operational effectiveness while maintaining flexibility is pivotal for successful UAS operations. Consequently, supporting technologies must facilitate operations without imposing restrictions, limitations, or increased risk. As UAS operations expand in scale and diversity, solutions should enhance efficiencies, reduce operational and capital expenditures (Opex and Capex), and minimally impact UAS design. Moreover, these solutions should not only address current threats but also remain adaptable to future challenges and UAS design requirements.

The prevalent use of Pre-shared Symmetric Keys (PSKs), although offering proven security at the highest levels, poses significant implementation and management costs, as well as Size, Weight & Power (SWaP) concerns. Additionally, PSKs lack scalability and dynamic adaptability essential for modern operations. Conversely, scalable solutions based on Public Key Infrastructure (PKI) alleviate logistical burdens but fail to provide adequate security for mission-critical UASs, leaving them vulnerable to various attack vectors, including “harvest now, decrypt later”.

Current PSK-based networks offer significant challenges for UAS missions

1. Reliance on group keys in mesh data networks create a single point of failure and necessitate recall of all devices for re-keying and re-deployment upon compromise.
2. SWaP issues introduced by Type 1 and 2 cryptographic hardware, impacting operational flight time and payload capacity, while also incurring significant Opex and Capex due to their bespoke nature and security requirements.
3. Inability to perform regular device authentication upon deployment, leaving systems vulnerable to spoofing attacks and unauthorised network access.
4. Difficulty in achieving dynamic tactical handover of assets, requiring extensive pre-planning and group key usage, thus restricting operational flexibility.
5. Requirement for pre-deployment of keys to deployed units, exposing systems to various security risks and adding to Opex, Capex, and operational restrictions.
6. Inability to ratchet pre-loaded PSKs without physical redeployment, leading to prolonged use of unchanged keys and poor forward secrecy.
7. Transmission of C2 and sensor data within a single tunnel using a single encryption key per device, limiting data delayering capabilities and creating a single point of failure.

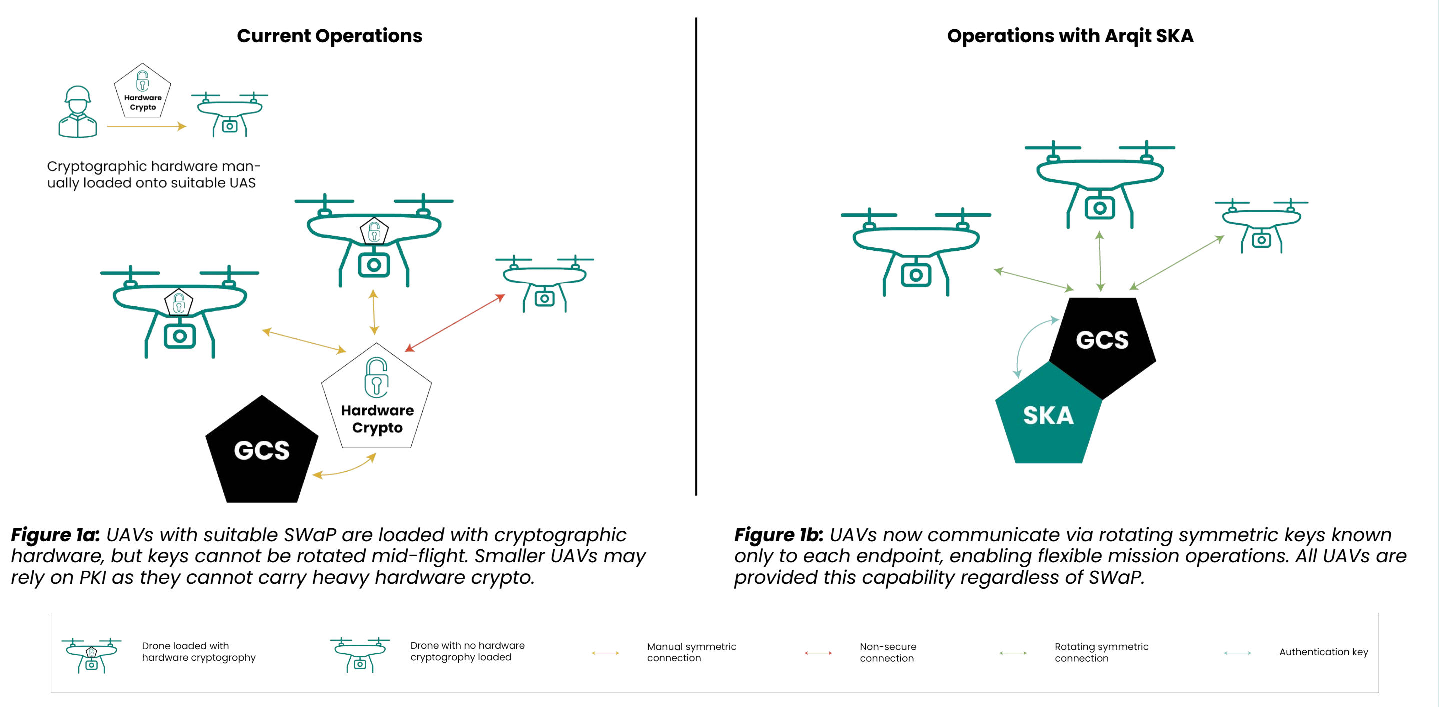
Current Operations
Hardware Crypto
Cryptographic hardware manually loaded onto suitable UAS
Hardware Crypto
GCS
Operations with Arqit SKA
GCS
SKA
Drone loaded with hardware cryptography
Drone with no hardware cryptography loaded
Manual symmetric connection
Non-secure connection
Rotating symmetric connection
Authentication key

Figure 1a: *UAVs with suitable SWaP are loaded with cryptographic hardware, but keys cannot be rotated mid-flight. Smaller UAVs may rely on PKI as they cannot carry heavy hardware crypto.*

Figure 1b: *UAVs now communicate via rotating symmetric keys known only to each endpoint, enabling flexible mission operations. All UAVs are provided this capability regardless of SWaP.*

Despite these challenges, PSK-based networks offer a well-established and trusted approach for achieving adequate levels of data encryption across various classifications using symmetric keys (e.g., The White House National Security Memorandum[1]). However, a solution integrating the security of PSKs with the flexibility of PKI is necessary to address the security, operational, and logistical concerns faced by UASs today.

Using Arqit's Symmetric Key Agreement (SKA) platform to eliminate UAS mission restrictions

Arqit's SKA platform offers a solution to eliminate UAS mission restrictions. By removing the risks associated with PKI and overcoming the complexities and limitations of PSKs, the SKA platform provides a cryptographically agile and Secure by Design (SBD) solution. Seamlessly integrating into existing network infrastructures, the SKA platform enables split trust and zero trust architectures while facilitating dynamic creation and proliferation of symmetric keys across trusted endpoints.

Enabling Swarming and Group Keys with Arqit SKA

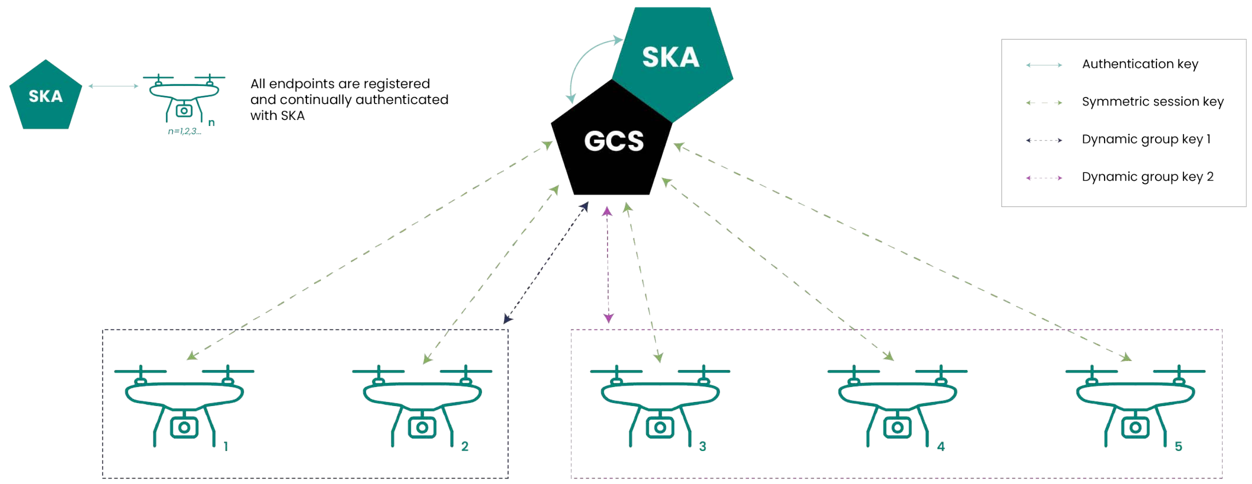

Figure 2: *A wider picture of operations with Arqit SKA. Security group controls enable segregation of responsibility. Rotating group keys for broadcast are facilitated via individual symmetric channels.*

Key features and benefits of Arqit's SKA platform

Operational Effect

- Real-time management of endpoints integrated into existing C2 systems.
- Ad hoc creation and reforming of device groupings, allowing flexible network access control.
- Rotation and removal of device authentication keys to mitigate the impact of lost assets.
- Data delayering achieved with multiple rotating symmetric keys, enabling exploitation of individual datasets and facilitating data sharing across user groups.
- Support for dynamic tactical handover of assets and scalability without hardware changes .
- Bearer agnostic solution, enabling operational flexibility, redundancy and concurrent communication channels.

Economics

- Elimination of expensive cryptographic hardware and associated SWaP restrictions.
- Reduction of manual key distribution, storage, and management costs.
- Compatibility with current encryption algorithms and industry standards, reducing integration costs.

Security

- Dynamic generation and forward rotation of symmetric keys enhance forward secrecy and eliminate manual key management errors.
- Anti-spoofing capability supported by forward-rotating individual device authentication keys.
- Support for various operational deployment models with individual session and dynamic group keys.
- Implementation model supporting split trust / zero trust SBD architectures.

Future Proofing

- Compliance with NIST[2] and Whitehouse guidelines[1], NSA CSfC[3] and FIPS 140-2[4] standards, ensuring readiness for future cybersecurity standards.
- Independence from encryption algorithms and network protocols, ensuring compatibility with emerging standards.
- Adaptability to increasing key sizes without impacting speed and performance.

Arqit's SKA platform serves as a central pillar in architecting UAS networks, enabling the full potential of UAS operations while outperforming existing cybersecurity solutions. By combining the security strengths of PSKs with the flexibility of PKI, Arqit's solution addresses the evolving challenges and requirements of UAS operations, ensuring mission success and operational superiority over adversaries.

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[2] https://www.csrc.nist.gov/pubs/sp/800/71/ipd
[3] https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/Symmetric%20Key%20Management%20Requirements%20v2_1.pdf?ver=PR0QdeiD8nnH14MbA2HnHQ%3d%3d
[4] https://csrc.nist.gov/pubs/fips/140-2/upd2/final