Formal Verification of the LDACS MAKE Protocol

Nils Mäurer
German Aerospace Center (DLR)

Sophia Grundner-Culemann
MNM-Team, Ludwig-Maximilians-Universität München

34th Crypto Day, June 9 and 10, 2022

Text-based in-flight-communications between aircraft and ground has been carried out over the Aircraft Communications, Reporting and Addressing System (ACARS) since 1978 [1, 3]. Only in 2007, the ACARS Message Security protocol (AMS) [1] added some much-needed security features to the de-facto standard. However, security concerns about the protocol have been voiced repeatedly since its introduction [3], and some serious flaws were identified in 2017 using symbolic model checking [ibid].

Furthermore, aeronautical communications are currently transitioning from largely analogue to digital services. This includes a shift to the Internet-Protocol as underlying networks layer. As a part of this process, the L-band Digital Aeronautical Communications System (LDACS) has been developed as a new terrestrial datalink for flight guidance and communications related to safety and regularity of flight in continental airspace. It is currently under review to be standardized by the International Civil Aviation Organization [2].

As the example of AMS shows [3], Automated Theorem Proving (ATP) is a valuable tool for finding security holes in communication protocols, however carefully crafted they might be.

In our talk, we therefore present the first formal verification of the security properties of the updated LDACS 3-pass Mutual Authentication and Key Establishment (MAKE) protocol. This protocol allows AS and GS to establish shared keys via Diffie-Hellman or a Key Encapsulation Mechanism, and to mutually authenticate communication partners in a three-way handshake. There are two variants: (1) The LDACS IKEv2 based 3-pass MAKE protocol and (2) the LDACS ISO/IEC 11770-3:2021 key agreement mechanism 7 based 3-pass MAKE protocol. The verification is done with the *Tamarin Prover* [6], which has also been used to formally verify TLS 1.3 and (post-quantum-)IKEv2, among others [4, 5]. We present our approach[1], point out security features and highlight difficulties in modelling the protocol correctly.
Our work supports the on-going design and standardization process of LDACS.

[1]The complete code is available online: https://github.com/NilsMaeurer/ldacs$_i$so − $kam7_ikev2_make_proofs$, accessed 05/30/2022

References

[1] ARINC (2007). Datalink Security Part 1 - ACARS Message Security. ARINC SPECIFICATION 823, Aeronautical Radio, Incorporated (ARINC).

[2] Miguel Angel Bellido-Manganell, Thomas Gräupl, Oliver Heirich, Nils Mäurer, Alexandra Filip-Dhaubhadel, Daniel M. Mielke, Lukas Marcel Schalk, Dennis Becker, Nicolas Schneckenburger & Michael Schnell (2021). LDACS Flight Trials: Demonstration and Performance Analysis of the Future Aeronautical Communications System. *IEEE Transactions on Aerospace and Electronic Systems* 1–19.

[3] Bruno Blanchet (2017). Symbolic and computational mechanized verification of the ARINC823 avionic protocols. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, 68–82. IEEE, Santa Barbara, CA, USA.

[4] Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott & Thyla van der Merwe (2017). A comprehensive symbolic analysis of TLS 1.3. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1773–1788. ACM.

[5] Stefan-Lukas Gazdag, Sophia Grundner-Culemann, Tobias Guggemos, Tobias Heider & Daniel Loebenberger (2021). A formal analysis of IKEv2's post-quantum extension. In *Annual Computer Security Applications Conference*, ACM Digital Library, 91–105. Association for Computing Machinery, New York,NY,United States. ISBN 9781450385794.

[6] S. Meier, B. Schmidt, C. Cremers & D. Basin (2013). The TAMARIN Prover For The Symbolic Analysis Of Security Protocols. In *25th International Conference on Computer Aided Verification (CAV)*, 696–701.