Title: Towards a formal verification of secure vehicle software updates

Authors: Martin S. Hagen, Emil Lundqvist, Alex Phu, **Yenan Wang**, Kim Strandberg, Elad M. Schiller

Abstract:

With the rise of software-defined vehicles (SDVs), where software governs most vehicle functions alongside enhanced connectivity, the need for secure software updates has become increasingly critical. Software vulnerabilities can severely impact safety, the economy, and society. In response to this challenge, Strandberg et al. [escar Europe, 2021] introduced the Unified Software Update Framework (UniSUF), designed to provide a secure update framework that integrates seamlessly with existing vehicular infrastructures. Although UniSUF has previously been evaluated regarding cybersecurity, these assessments have not employed formal verification methods. To bridge this gap, we perform a formal security analysis of UniSUF. We model UniSUF's architecture and assumptions to reflect real-world automotive systems and develop a ProVerif-based framework that formally verifies UniSUF's compliance with essential security requirements — confidentiality, integrity, authenticity, freshness, order, and liveness — demonstrating their satisfiability through symbolic execution. Our results demonstrate that UniSUF adheres to the specified security guarantees, ensuring the correctness and reliability of its security framework.

Link to paper:

https://www.sciencedirect.com/science/article/pii/S0167404825004407