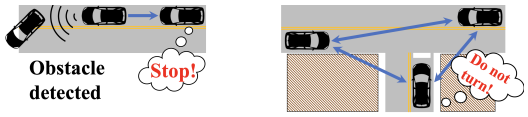
Demo: An Open-Source Hardware-in-the-Loop Testbed for Post-Quantum V2V Security Research

Geoff Twardokus and Hanif Rahbari
Rochester Institute of Technology • {geoff.twardokus,rahbari}@mail.rit.edu

***Abstract*—We showcase *PQ-V2Verifier*, the first open-source testbed for using NIST-approved post-quantum authentication algorithms in vehicle-to-vehicle (V2V) communications. With hardware in the loop for over-the-air experiments using software-defined radios and commercial V2V devices, we show the potential of *PQ-V2Verifier* for customizable experiments to evaluate V2V security protocols in safety use cases against attacks enabled by a large quantum computer, as well as novel countermeasures.**

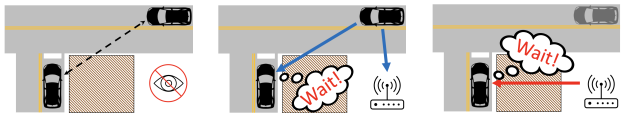
Introduction. Vehicle-to-vehicle (V2V) communication technology could significantly reduce roadway crashes and enhance transportation efficiency by facilitating cooperative vehicle maneuvering. However, the security of current V2V technology relies primarily on digital signatures. The anticipated development of large quantum computers that can break digital signatures based on classical cryptography—which may occur within 15–20 years [1]—is the impetus for agencies like the National Institute of Standards and Technology (NIST) to begin identifying and mitigating the challenges of adopting post-quantum cryptography (PQC). This is a particular challenge when considering constrained services like V2V that require significant redesign to transition from classical cryptography to PQC. Consequently, developing tools and environments to support research in this area, which requires facilitating realistic and scalable evaluations of PQC integrations with V2V, is a critical undertaking. In this demo, we showcase *PQ-V2Verifier*, our fully open-source[1], scalable, hardware-in-the-loop testbed for integration of NIST-approved PQC algorithms into the IEEE 1609.2 security standard on top of open-source implementations of V2V communication protocols.

Testbed Demo. Our testbed uses widely available software-defined radios and, optionally, leading commercial V2V devices (e.g., Cohda MK6 [2]) to incorporate over-the-air transmission of V2V signals for real-world evaluation of post-quantum solutions for V2V. Our software stack uses carefully selected implementations of NIST-approved PQC digital signatures [1] targeted at automotive processors, integrated with open-source implementations of V2V security and communication protocols for the physical through application layers [3], in compliance with relevant industry standards. We begin by demonstrating key safety use cases for V2V, such as Forward Collision Warning (FCW) and Intersection Movement Assist (IMA), to convey the life-saving potential of V2V (see Fig. 1). Vehicle movements, and the content of over-the-air V2V messages exchanged, will be rendered on our graphical interface



(a) FCW. (b) IMA.

Fig. 1: Safety use cases for V2V.



(a) Scenario. (b) Message capture. (c) Replay.

Fig. 2: Replay attack scenario enabled by quantum attacks.

(based on, e.g., OpenStreetMaps [4]) to concretely convey real-world outcomes—e.g., vehicles colliding—to the audience.

We next demonstrate multiple attacks against V2V which are mitigated under current standards but will be enabled by large quantum computers. For example, we will demonstrate the message replay attack shown in Fig. 2. In a blind corner scenario (Fig. 2(a)), an attacker captures and stores messages from vehicles (Fig. 2(b)). Later, the attacker modifies a captured message indicating the presence of a vehicle (e.g., by updating its timestamp to pass a validity period check) and forges a new, legitimate digital signature using a quantum computer. The attacker then replays the altered message, causing receivers to believe a vehicle is present when none is, and, for instance, causes traffic to stop for no reason (Fig. 2(c)). Our demo will feature larger-scale scenarios with additional virtual vehicles, and we will also demonstrate message forgery attacks, with consequences including significant traffic jams and avoidable vehicle collisions. We will demonstrate our mitigation techniques and their performance metrics from [1]. Further, an interactive portion will allow attendees to enable and disable select security features (e.g., PQC support) and observe the outcomes, reinforcing the technical and educational capabilities of our testbed regarding the safety benefits of V2V.

Acknowledgment. This material is based on work supported by the National Science Foundation (NSF) under Grant No. 2239931. Any opinions, findings, and conclusions are the author(s)' and may not reflect the views of the NSF.

References

[1] G. Twardokus, N. Bindel, H. Rahbari, and S. McCarthy, "When cryptography needs a hand: Practical post-quantum authentication for V2V communications," in *Proc. Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Feb. 2024.

[2] Cohda Wireless, "MK6–Cohda Wireless," 2023, Accessed: Nov. 12, 2023. [Online]. Available: https://bit.ly/3FSPNzU

[3] G. Twardokus and H. Rahbari, "Evaluating V2V security on an SDR testbed," in *Proc. IEEE Conf. Computer Commun. Workshops (INFOCOM WKSHPS)*, (Virtual) Vancouver, BC, Canada, May 2021.

[4] OpenStreetMap contributors, "OpenStreetMap," 2023, Accessed: Jan 3, 2024. [Online]. Available: https://www.openstreetmap.org

[1] https://github.com/twardokus/pq-v2verifier

Symposium on Vehicle Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25007
www.ndss-symposium.org