Formal Verification of Mixing Preshared Keys in IKEv2 Protocol Using ProVerif*

Changhyeon Woo, Bonam Kim, and Ilsun You

Kookmin University, Seoul, Republic of Korea
{crow1104, kimbona, isyou}@kookmin.ac.kr

Abstract

With the increasing importance of IP-based communication, the importance of secure key exchange mechanisms has become increasingly significant. Among these, the IKEv2 protocol serves as the core component for establishing secure channels in IPsec. However, Diffie–Hellman based key exchanges are vulnerable to quantum attacks. To mitigate this issue, RFC 8784 introduces a Post-Quantum Pre-Shared Key (PPK) extension to enhance the protocol's quantum resistance. This paper performs a formal verification of the RFC 8784–based IKEv2 protocol using ProVerif to assess its security.
Keywords: IKEv2, Formal Verification, ProVerif, Post-Quantum

1 Introduction

IPsec is a core technology for securing IP-based communications, providing confidentiality, integrity, and authentication at the network layer. It relies on the Internet Key Exchange Protocol Version 2 (IKEv2) for key exchange and management, which performs mutual authentication and generates session keys using ephermeral Diffie-Hellman (DH). However, the rise of quantum computing and Shor's algorithm poses a serious threat to DH-based exchanges, under the "Harvest Now, Decrypt Later" (HNDL) model [**?**]. To mitigate this issue, RFC 8784 [**?**] introduces a Post-Quantum Pre-Shared Key (PPK) to IKEv2 as an interim measure before full Post-Quantum Cryptography (PQC) adoption. By integrating the PPK into IKEv2's key-derivation process, the session key depends on both the Diffie–Hellman exchange and the externally distributed PPK.

This paper analyzes the IKEv2 protocol enhanced with the RFC 8784 extension, formally verifies its security properties using the ProVerif tool.Through this analysis, we seek to provide meaningful insights that contribute to strengthening the quantum resistance of key exchange mechanisms in IPsec-based communication.

2 Formal Verification of IKEv2 Based on RFC 8784

ProVerif is an automated formal verification tool based on model checking [**?**]. It formalizes cryptographic primitives and models their associated subprocess to automatically verify protocol properties such as *reachability*, *secrecy*, and *correspondence assertions*. In this work, we use ProVerif to verify the security of the two IKEv2 authentication modes (pre-shared key (PSK), certificate).

We declare private variables *secret_initiator*, *secret_responder* to verify whether confidential data are protected against the attacker. To verify the correspondence between communicating

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-59, December 16-18, 2025, Sapporo, Japan.

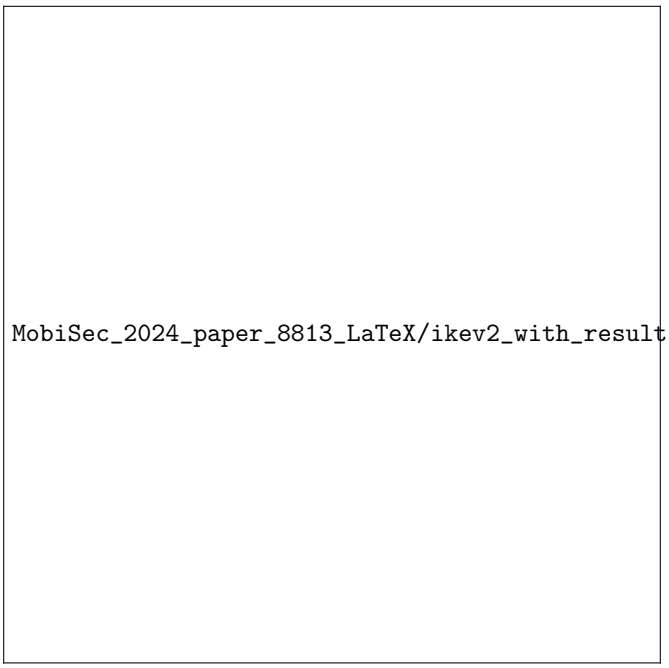

Figure 1: IKEv2 based on RFC 8784 Protocol and Verification Results

entities in the IKEv2-PPK protocol, we define *events* to represent the major steps of the protocol execution. The *injective* option is used to detect replay attacks and to confirm 1:1 mutual authentication in the communication. The *phase* option is used to declare a situation in which the long-term key is leaked and to examine whether the confidentiality of secret values is compromised as a result.

The verification results in Figure **??** show that in both IKEv2-PSK-PPK and IKEv2-CERT-PPK models, the query *inj-event(dh_init_ready(SPIi, SPIr, Ni, Nr, KEi, KEr)) → inj-event(dh_resp_ready (SPIi, SPIr, Ni, Nr, KEi, KEr)) is false* indicates that the Diffie–Hellman exchange alone cannot ensure peer agreement, allowing an attacker to deceive the initiator during the unauthenticated `IKE_SA_INIT` phase. The query *inj-event(E_AUTH_I_to_R(SPIi, SPIr, Ni, Nr, ID_init)) → inj-event(S_AUTH_I_to_R(SPIi, SPIr, Ni, Nr, ID_init)) is false* further shows that the responder may accept a forged initiator authentication, suggesting that an attacker could reuse or modify signed data to impersonate the initiator.

3 Conclusion

The verification using ProVerif reveals that in IKEv2-PSK-PPK and IKEv2-CERT-PPK models, the Diffie-Hellman exchange alone does not guarantee peer agreement, and in IKEv2-CERT-PPK model, the responder may accept a forged initiator authentication, indicating a potential impersonation risk. Since this study focuses only on the initial authentication phase of IKEv2-PPK, as future work, we plan to extent the analysis to include the Child SA creation process to comprehensively evaluate the overall security of IKEv2-PPK.

Acknowledgement: This work was supported by Institute of Information & communications

Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2022-0-00103, Development of security verification technology against vulnerabilities to assure IoT/IIoT device safety).