Post-Quantum Secure OpenID Connect using KEMTLS.

Challenge Overview:

Current OIDC deployments depend on classical public-key cryptography (RSA, ECC), which is vulnerable to quantum attacks. Recent research on Post-Quantum OpenID Connect demonstrates how OIDC can be migrated to the post-quantum era using NISTstandard post-quantum TLS and post-quantum signature schemes. However, these implementations rely on conventional TLS handshake designs. KEMTLS is a recently proposed alternative to TLS that replaces certificate-based key exchange with Key Encapsulation Mechanisms (KEMs), making it a promising candidate for post-quantum secure communication. Despite its advantages, KEMTLS has not yet been explored or implemented in the context of OpenID Connect. This challenge focuses on implementing a Post-Quantum OpenID Connect system where all TLS communication is secured using KEMTLS, while preserving OpenID Connect protocol semantics and using standard post-quantum digital signature schemes wherever signatures are required.

Objectives

1. **Post-Quantum Transport Security**
   - Replace standard TLS or PQ-TLS with KEMTLS for all secure communication between OpenID Connect components.
   - Ensure confidentiality, authentication, and forward secrecy using KEM-based handshakes.
2. **Post-Quantum OpenID Connect Compliance**
   - Preserve OpenID Connect authentication and authorization flows.
   - Use post-quantum digital signature schemes for:
     - ID Token signing
     - JWT / JWS signing
     - Metadata and key distribution
   - Maintain protocol correctness at the application layer.
3. **Performance and Benchmarking**
   - Measure handshake latency, authentication latency, and message sizes.
   - Evaluate performance using benchmarks defined in Post-Quantum OpenID Connect research.
   - Compare results with PQ-TLS-based reference implementations where applicable.

Evaluation Criteria

1. **Protocol Correctness**
   - Correct execution of OpenID Connect authentication and authorization flows.
   - Proper separation of transport-layer security and application-layer digital signatures.
2. **Security Design**
   - Correct integration of KEMTLS.
   - Exclusive use of post-quantum cryptographic primitives.
   - No dependency on classical public-key cryptography.
3. **Performance and Benchmarking**
   - Measurement of KEMTLS handshake time.
   - Evaluation of token generation and verification overhead.
   - Comparison against reference Post-Quantum OpenID Connect benchmarks.
4. **Implementation Quality**
   - Clean and modular software architecture.
   - Reproducible experimental setup and results.
   - Clear documentation and well-justified design decisions.

Implementation Guidelines and Suggestions

General Implementation Rules

- The core protocol logic and cryptographic integration must be implemented by the project team.
- Copying complete implementations from GitHub, Kaggle, or similar platforms is strictly prohibited.
- All design choices, assumptions, and deviations must be clearly documented and justified.

Protocol and Cryptography

- OpenID Connect must remain unchanged at the application layer.
- All communication traditionally secured using TLS must instead use KEMTLS.
- NIST-standardized post-quantum digital signature schemes (e.g., Dilithium, Falcon) must be used for all signing operations.
- Full compatibility with existing JWT and JWS formats must be preserved.

Benchmarking

- Benchmarking must follow the methodology described in Post-Quantum OpenID Connect literature.
- Both cryptographic-level and protocol-level performance overheads must be measured.
- The experimental setup and evaluation environment must be clearly described to ensure reproducibility.

Deliverables

1. **Working Prototype**
   - Functional OpenID Connect system secured using KEMTLS.
   - Demonstration of an end-to-end authentication flow.
2. **Source Code**
   - Complete and well-commented source code.
   - Public or private repository link (GitHub or GitLab).
3. **Technical Documentation**
   - System architecture overview.
   - Cryptographic design choices and rationale.
   - Benchmarking methodology and performance results.
4. **Demo Video**
   - A 5–10 minute video demonstrating the authentication flow and performance evaluation.
5. **Benchmark Report**
   - Latency and protocol overhead measurements.
   - Comparison with PQ-TLS-based reference implementations.

Submission Format

- **Platform:** Submission via official college email.
- **File Structure:**
  - Source code directory
  - `README.md`
  - `TechnicalDocumentation.pdf`
  - `BenchmarkResults.pdf`
  - Demo video link (YouTube or Google Drive)

References

[1] F. Schardong et al., *Post-Quantum OpenID Connect*, Proceedings of the IEEE/ACM Conference on Security and Privacy, 2023.

[2] T. Wiggers, *KEMTLS: Building TLS with Key Encapsulation Mechanisms*, IACR Cryptology ePrint Archive, Report 2020/534, 2020.

[3] OpenID Foundation, *OpenID Connect Core 1.0 Specification*, Available at: https://openid.net/specs/openid-connect-core-1$_0$.*html*

[4] National Institute of Standards and Technology (NIST), *Post-Quantum Cryptography Standardization Project*, Available at: https://csrc.nist.gov/projects/post-quantum-cryptography