PQC 게이트웨이를 통한 OCI 컨테이너 서명 체계의 크립토 애질리티

권순홍[1], 손우영[1], 강남규[2], 이종혁[1]
[1]정보보호학과 & 지능형드론 융합전공, 세종대학교
[2]데이터 플랫폼 센터, 한국과학기술정보연구원
soonhong@pel.sejong.ac.kr, wooyoung@pel.sejong.ac.kr
ngkang@kisti.re.kr, jonghyouk@sejong.ac.kr

Crypto-Agility of OCI Container Signing System through a PQC Gateway

Soonhong Kwon[1], Wooyoung Son[1], Nam-Gyu Kang[2], Jong-Hyouk Lee[1]
[1]Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University
[2]Data Platform Center, Korea Institute of Science and Technology Information

요 약

소프트웨어 공급망의 복잡성이 나날이 증가하고, 이를 대상으로 한 보안위협이 점차 정교해지고 있음에 따라 컨테이너 공급망의 보안은 필수 요구사항을 자리매김되고 있다. 이와 더불어 양자 컴퓨터가 상용화되기까지의 시간이 얼마남지 않은 시점에서 기존 컨테이너 공급망에 적용되어 있는 공개키 기반 디지털 서명 체계는 더 이상 안전하지 않다는 분석이 제시되고 있다. 이에 본 논문에서는 기존 컨테이너 공급망의 워크플로우를 유지하면서 로컬 환경에서의 자원 및 호환성 문제를 회피할 수 있는 PQC (Post-Quantum Cryptography) 게이트웨이 기반 OCI (Open Container Initiative) 아티팩트 서명 프레임워크를 제안하였다. 제안된 프레임워크는 실험을 통해 PQC 서명이 OCI Referrers 기반의 다중 아티팩트 관리에 완전히 통합될 수 있음을 보임으로써 신뢰성이 보장된 공급망 환경을 구성할 수 있음을 보였다. 이와 동시에 실증을 통해 Dilithium2가 SPHINCS+에 비해 서명 시간은 약 1.94배, 검증 시간은 1.25배 더 빠른 것을 볼 수 있었으며, 서명 크기는 약 7.08배 최소화될 수 있음을 보임으로써 컨테이너 공급망 환경에 적합함을 보인다.

1. 서론

소프트웨어 공급망의 복잡성이 나날이 증가하고, 이를 대상으로 한 보안위협이 점차 정교하고 파괴적인 형태로 발전하고 있다. 특히, Log4j, 3CX 침해사고 등의 공격은 소스 코드 개발에서부터 배포에 이르기까지의 라이프사이클 전반적으로 신뢰를 보장하는 것이 얼마나 중요한지를 보여주는 주요 사례가 된 바 있다 [1].

최근 국가 기반시설의 정보 시스템과 더불어 기업의 시스템은 클라우드 네이티브 형태로 전환이 이루어지고 있는 상황이며, 금년도에는 430억원을 투자하여 7개의 기관에 대한 9개의 공공정보 시스템을 선정하고 이를 클라우드 네이티브로 전환하고자 하는 계획을 행정안전부에서 발표한 바 있다. 이에 따라 클라우드 네이티브의 구성요소인 마이크로서비스, 컨테이너, 데브옵스, CI/CD에 대한 전방향적인 보안이 요구되는 상황이다. 이는 결국 컨테이너 라이프사이클에 대한 보안이 보장되어야 함을 의미하며, 컨테이너 공급망에 대한 신뢰성이 갖추어져야 함을 의미한다. 컨테이너를 하나의 실행 파일로 보았을 때, 도커 이미지는 애플리케이션 코드, 라이브러리 등을 모두 포함하고 있음에 따라 원천 코드로 간주할 수 있다. 즉, 도커 이미지에 대한 보안이 보장되어야 컨테이너를 타겟으로 한 보안위협의 가능성을 줄일 수 있음을 알 수 있다.

이에 도커 이미지의 취약점을 스캐닝하는 연구가 다수 이루어지고 있으며, 도커 이미지와 같은 OCI (Open Container Initiative) 아티팩트의 무결성을 보장하기 위한 디지털 서명 기술이 연구/개발되고 있다. 하지만, 1995년 Shor에 의해 쇼어 알고리즘이 제시되면서 현대 암호화 체계가 무너질 가능성이 제시되었으며, 최근에는 다항시간 내에 RSA, ECDSA와 같은 공개키 암호 알고리즘이 해독되어 컨테이너 공급망에 적용되어 있는 디지털 서명이 무력화될 수 있음을 발표되고 있다. 이에 NIST에서는 Dillithium, SPHINCS+ 등과 같은 포스트 양자 암호가 표준화되고 있는 상황이며 [2][3], 이를 소프트웨어 공급망에 적용하고자 하는 노력이 이루어지고 있다.

이에 본 논문에서는 OCI 컨테이너 서명 체계의 크립토 애질리티를 제공할 수 있는 PQC 게이트웨이 기반의 프레임워크를 제안하고자 한다.

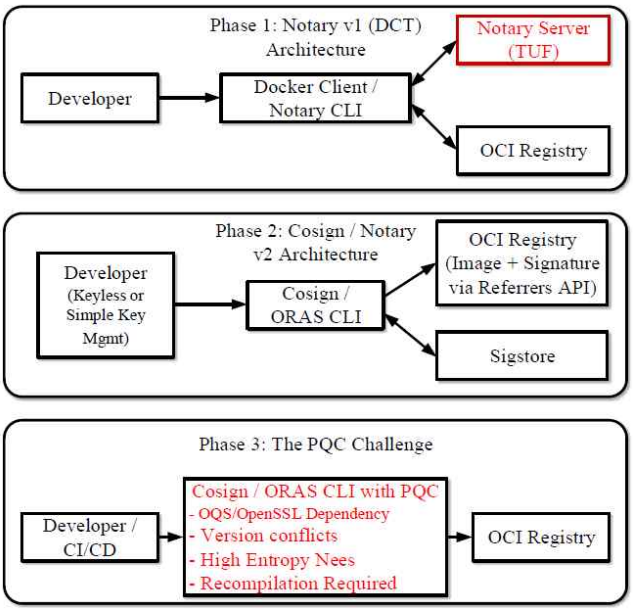
본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 OCI 아티팩트 서명 체계에 대한 분석한 내용을 설명하며, 3장에서는 도커 이미지의 무결성을 보장할 수 있는 PQC 게이트웨이 기반의 프레임워크를 제안한다. 4장에서는 제안된 프레임워크에서 활용되는 PQC 알고리즘의 성능 분석 내용을 설명하며, 5장에서 본 논문의 결론을 맺는다.

2. OCI 아티팩트 서명 체계 분석

컨테이너 공급망에서의 보안을 보장하기 위한 첫 번째 발걸음은 원천 코드의 역할을 수행하는 도커 이미지에 대한 무결성 보장이 우선시 되어야 한다. 이를 위해 OCI 아티팩트를 서명하기 위한 기술이 지속적으로 개발되었으며, 이는 TUF (The Update Framework)를 기반으로 한 Notary v1에서부터 Cosign / Notary v2로 이어지고 있다. 이에 대한 발전 흐름은 (그림 1)을 통해 확인할 수 있다.

초창기에 활용된 Notary v1에 대해 설명하기 위해서는 TUF 원칙에 대해 명확히 이해하고 있어야 한다. TUF는 분리된 역할(e.g., root, targets, snapshot, timestamp)에 대한 정의와 더불어 정의된 각 역할에 대해 서로 다른 키를 부여함으로써 키 노출에 대한 위험을 최소화하는 원칙을 의미한다. 컨테이너 공급망 환경에서는 TUF 원칙을 DCT (Docker Content Trust)에 적용하였으며, DCT의 구현체인 Notary v1을 제시하였다. Notary v1을 활용할 수 있도록 함으로써 도커 이미지의 태그([docker image name]:**tag**)와 다이제스트 간의 매핑을 안전하게 보호하도록 하였다. 이를 통해 컨테이너 공급망에 포함되어 있는 사용자는 신뢰된 사용자가 개발하여 업로드한 도커 이미지만을 사용할 수 있도록 강제함으로써 공급망의 보안을 보장하였다. 하지만, 이는 사용자 경험상의 한계를 보이게 되었으며, 기존 OCI 레지스트리와 별도로 Notary 서버를 추가 운영 및 관리해야 했음에 따라 사용자 측면에서 부담이 증가하게 되었으며, 개발자는 각 역할에 부여된 키를 직접 관리해야 하여 다양한 레지스티리로 확장할 수 있는 가능성을 저해하였다.

이와 같은 한계를 보완하기 위하여 Sigstore에서 제시한 Cosign과 CNCF에 의해 관리되는 Notary v2가 발표되었으며, 해당 기술에서는 OCI Referers API를 활용하였다는 공통점이 발견되었다. OCI Referers API의 경우, 서명과 도커 이미지를 분리된 개념으로 즉, 서로를 참조하는 개념으로 하여 아티팩트를 별도로 관리할 수 있도록 하였다.

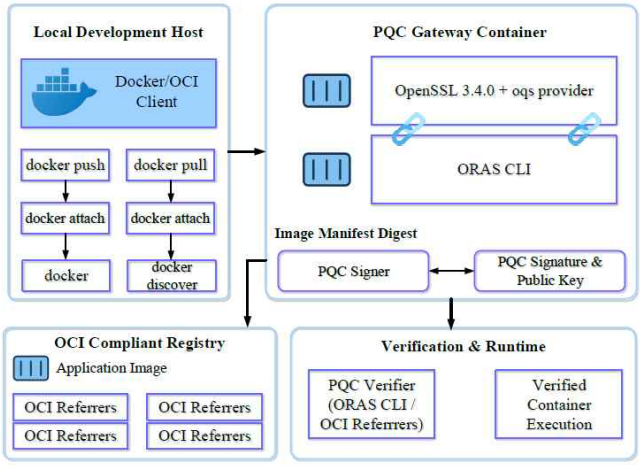


(그림 1) OCI 아티팩트 서명 체계 버전 아키텍처

즉, 기존 Notary v1에서 구성하였던 아키텍처와 달리 Notary 서버를 추가적으로 구성할 필요없이 OCI 레지스트리로만 구동할 수 있도록 하여 아키텍처를 간소화하고, 레지스트리 확장성 측면에서도 이점을 보일 수 있도록 하였다. 이와 더불어 Cosign은 OIDC (OpenID Connect)를 기반으로 한 Keyless 서명 키 관리를 제공하고 있어 Notary v1에 비해 키 관리 측면에서의 개발자 부담을 해소하였다는 장점이 있다.

그러나 현재까지의 OCI 아티팩트 서명 체계는 RSA나 ECDSA와 같은 공개키 암호 알고리즘을 통해 이루어지고 있다. 하지만, 1995년 Shor에 의해 발표된 Shor 알고리즘은 기존에 공개키가 안전하다는 이론에 의문을 품게 되었다. Shor 알고리즘은 QFT (Quantum Fourier Transform)를 기반으로 주기 찾기 문제를 해결하는 로직으로 동작한다. QFT를 통한 주기 찾기 문제 로직은 결국 특정 수의 주기를 찾는 것으로 직결되며 이는 소인수분해를 빠르게 수행할 가능성을 보임에 따라 RSA 암호 알고리즘이 무력화될 수 있음을 시사하였다. 이는 최근에 들어 양자 컴퓨터가 상용화되는 시기가 점차 가까워짐에 따라 기존 컴퓨터 연산에 의해 수십억 년이 소요될 수 있는 것을 양자 컴퓨터를 통해 다항 시간 내에 해독이 가능할 것으로 보아 PQC (Post-Quantum Cryptography)로 전환하는 것이 필수적인 상황이 되었다.

하지만, 컨테이너 공급망의 관점에서 PQC를 Cosign 혹은 Notary v2에 직접 적용하는 것은 여러 가지 측면에서 한계가 존재한다. NIST에서 표준화가 진행중인 Dillithium2나 SPHINCS+와 같은 PQC 알고리즘은



(그림 2) 제안하는 프레임워크

OQS (Open Quantum Safe)와 이를 지원하는 최신 버전의 OpenSSL 알고리즘이 요구되나, 이를 별도로 사용자 혹은 개발자의 로컬 환경에서 설치하여 적용하는 경우, 기존 운영중인 서비스와 충돌을 발생시킬 가능성이 다분하다. 이와 더불어 PQC 알고리즘들은 키를 생성하고 생성한 키를 활용하여 서명/검증하는 과정에서 높은 엔트로피를 요구함에 따라 낮은 컴퓨팅 리소스 운영 환경에서는 구동되지 않을 가능성이 존재한다. 이에 따라 실제 컨테이너 공급망을 위한 PQC 기반의 OCI 아티팩트 서명 프레임워크가 구성되기 위해서는 crypto agility와 더불어 compatibility를 확보할 수 있어야 한다.

3. 제안하는 프레임워크

최근 소프트웨어 공급망을 타겟으로 한 보안위협이 정교해지고, 고도화되고 있음에 컨테이너 라이프사이클의 시작이 되는 도커 이미지와 같은 OCI 아티팩트에 대한 무결성을 보장할 수 있는 서명 기술에 대한 중요도가 높아지고 있다. 특히, 2장에서 살펴본 바와 같이 양자 컴퓨팅의 상용화가 다가오는 상황에서 공개키 암호 기반의 디지털 서명은 더 이상 안전하지 않은 상황에 직면해 있다. 이에 따라 본 장에서는 PQC 알고리즘을 기존 OCI 아티팩트 서명 체계에 통합할 수 있도록 PQC 게이트웨이에 기반한 OCI 아티팩트 서명 프레임워크를 제안한다.

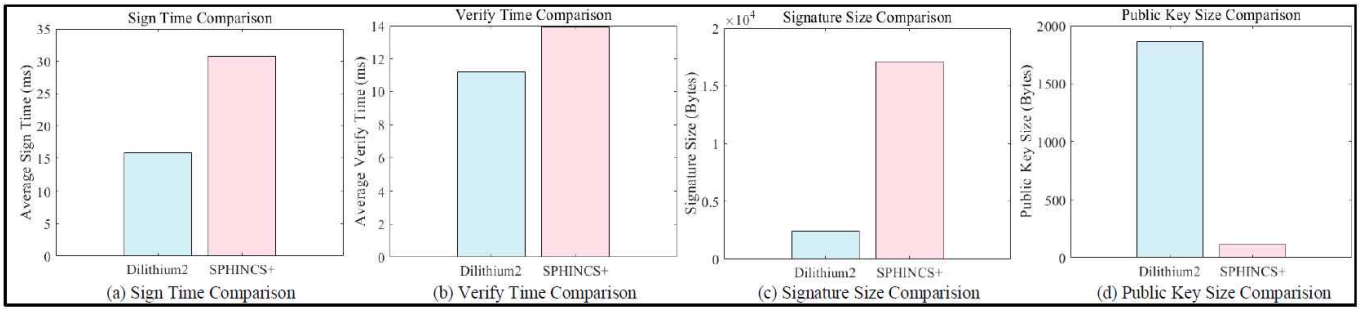
제안된 프레임워크는 (그림 2)를 통해 확인할 수 있으며, 호스트와 게이트웨이 컨테이너의 이중 구조로 구성되어 있다. 우선, 호스트 환경은 기존 OCI 아티팩트 서명 체계에서와 같이 사용자가 docker 및 ORAS CLI를 기반으로 하여 Docker Hub와 같은 도커 이미지 레포지토리에 ***push, attach, discover*** 등을 수행할 수 있도록 하였다. 이에 반면 PQC 알고리즘을 활용한 서명/검증과 같은 높은 엔트로피가 요구되는 연산에 대해서는 모두 PQC 게이트웨이 위임하여 동작할 수

(그림 3) PQC를 통한 도커 이미지 서명/검증 결과

있도록 하였다. 이를 위해서는 PQC 게이트웨이 내 OpenSSL 3.4.0과 oqs-provider가 통합되어 있으며, Dilithium2와 SPHINCS+를 비롯한 PQC를 제공할 수 있도록 구성하였다. 이와 같은 구조를 이룸으로써 호스트 환경에서는 RSA 및 ECDSA와 같은 공개키 암호 알고리즘 기반의 파이프라인을 유지할 수 있도록 하였으며, PQC 알고리즘을 외부로 확장 가능한 형태로 구성함으로써 기존 OCI 아티팩트 서명 절차를 유지할 수 있도록 하였다. 이와 더불어 PQC 알고리즘 기반 서명/검증에 대해 로컬 환경이 아닌 격리되어 있는 컨테이너 기반의 게이트웨이에 위임하여 진행될 수 있도록 하였음에 따라 로컬 환경에서 발생 가능한 라이브러리 및 OpenSSL 충돌 문제 혹은 엔트로피 부족 문제를 방지할 수 있다. (그림 2)를 통해 확인할 수 있듯이 호스트와 컨테이너는 공유 디렉토리를 설정함으로써 키, 서명, 다이제스트 파일이 교환 가능한 형태로 구성하여 확장성을 높였다.

서명 및 검증 절차와 관련하여서는 우선 호스트에서 ORAS ***menifest fetch***를 기반으로 하여 도커 이미지에 대한 manifest digest를 추출하도록 하였으며, 이를 SHA-256으로 해시하여 메시지 파일을 생성하도록 하였다. 이후, PQC 게이트웨이에서는 PQC 알고리즘(e.g., Dilithium2, SPHINCS+)에 대한 키 쌍을 생성하도록 하였으며, 해당 개인키를 기반으로 digest hash를 서명하도록 하였다. 이때, 생성된 서명과 공개키는 호스트로 전달하도록 하였으며, 호스트에서 최종적인 검증이 이루어지도록 함으로써 (그림 3)과 같이 기존 OCI 파이프라인 내에서 정상 동작하도록 하였다.

OCI 아티팩트 연동의 경우, ORAS CLI를 활용하였으며, ***attach*** 및 ***discover*** 기능을 활용함으로써 호스트에서는 PQC 서명 파일과 공개키에 대해 ***vnd.hpqc.sig*** 타입 아티팩트로 도커 이미지에 부착하였으며, 실제 ***discover***를 통해 해당 도커 이미지를 식별할 수 있어야 함에 따라 알고리즘 종류와 더불어 목적에 대해 주석으로 함께 저장될 수 있도록 하였다. 이와 같은 일련의



(그림 4) PQC 알고리즘 성능 비교

과정은 PQC 서명이 OCI Referrers 기반의 다중 아티팩트 관리 체계에 완전히 통합될 수 있음을 보임으로써 양자 컴퓨터가 상용화된 이후에도 안전한 컨테이너 공급망 환경을 구성할 수 있을 것으로 기대할 수 있다.

4. 성능 분석

본 논문에서는 양자 컴퓨터가 상용화되어 기존 OCI 아티팩트 서명에 사용된 공개키 암호 기반의 디지털 서명이 무력화될 수 있음을 확인하여 이에 대응하기 위한 PQC 게이트웨이 기반 OCI 아티팩트 서명 프레임워크를 제안하였다.

제안된 프레임워크와 관련하여 앞서 Dilithium2와 SPHINCS+ PQC 알고리즘을 활용 가능하도록 구성하였음을 제시하였다. 하지만, 해당 프레임워크는 기존 OCI 아티팩트 서명 체계에 통합될 수 있도록 설계되었음에 따라 실제 적용 가능성에 대해 확인해야 한다. 이에 따라 Dilithium2와 SPHINCS+ PQC 알고리즘에 대한 서명 시간, 검증 시간, 서명 사이즈, 공개키 사이즈를 실험을 통해 분석을 수행하였다.

Dilithium2의 경우, 서명 시간 15.820ms, 검증 시간 11.180ms, 서명 크기 2.4KB, 공개키 크기 1.8KB로 측정되었으며, SPHINCS+는 서명 시간 30.750ms, 검증 시간 13.930ms, 서명 크기 17KB, 공개키 크기 117B로 측정되어 (그림 4)와 같이 비교가 될 수 있음을 확인하였다. 즉, Dilithium2는 서명 시간 및 검증 시간을 통해 확인할 수 있듯이 SPHNICS+에 비해 빠른 응답 속도를 보이는 것을 확인할 수 있으며, 이는 실시간성을 요구하는 도커 이미지 인증에 적합한 알고리즘임을 보여주었다. 이와 더불어 서명 및 공개키 크기에 있어서는 Dilithium2가 SPHNICS+에 비해 상대적으로 전송 및 저장에 소요되는 비용을 최적화할 수 있다는 있는 반면, SPHNICS+는 공개키가 상대적으로 크게 경량화되어 있는 측면이 있음에 따라 다수의 공개키가 관리되는 환경에 적합한 측면이 존재한다. 하지만, SPHNICS+는 네트워크 전송 그리고 저장 비용이 상대적으로 증가할 수 있어 실제 컨테이너 공급망에 적용하기에는 상대적으로 한계가 존재함에 따라 Dilithium2가 OCI 아티팩트 서명 체계에 적합한 것을 확인할 수 있다.

5. 결론

컨테이너 라이프사이클의 시작이 되는 도커 이미지와 같은 OCI 아티팩트의 무결성을 보장할 수 있는 서명 기술에 대한 고도화가 요구되고 있다. 하지만, 양자 컴퓨터의 상용화가 얼마남지 않은 상황에서 기존 공개키 기반의 디지털 서명 체계는 붕괴될 가능성이 제시되고 있다. 이에 본 논문에서는 기존 OCI 아티팩트 서명 체계에 통합될 수 있음과 동시에 crypto agility와 compatbility가 보장될 수 있도록 하는 PQC 게이트웨이 기반 OCI 아티팩트 서명 프레임워크를 제안하였다. 제안된 프레임워크는 실험을 통해 PQC 서명이 OCI Referrers 기반의 다중 아티팩트 관리에 완전히 통합될 수 있음을 보임으로써 신뢰성이 보장된 공급망 환경을 구성할 수 있음을 보였다. 이와 더불어 컨테이너 공급망에 적합한 PQC 알고리즘에 대한 분석을 위해 실험을 진행하여 Dilithium2가 SPHINCS+에 비해 서명 시간은 약 1.94배, 검증 시간은 1.25배 더 빠른 것을 확인할 수 있었으며, 서명 크기는 약 7.08배 더 최소화될 수 있음을 확인하여 해당 알고리즘이 컨테이너 공급망에 적합함을 확인하였다. 향후 연구로는 하이브리드 서명 정책을 설계하여 보다 고도화된 서명 체계를 수립하고자 한다.

Acknowledgement

본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2025년도 문화기술 연구개발사업으로 수행되었음 (과제명: On-Device AI 모델 저작권 보호 및 관리를 위한 글로벌 인재양성, 과제번호: RS-2025-02221620, 기여율: 50%). 이 연구는 한국과학기술정보연구원의 지원을 받았습니다 (과제번호: (KISTI)J25JR001-25, 기여율: 50%).

참고문헌

[1] “소프트웨어 공급망 공격”, DreamSecurity, [Online]. Available: https://www.dreamsecurity.com/pr/news/1041. [Accessed: Sept. 15, 2025].

[2] J. Yang, et al., “Enhancing Cryptographic Security in Smart Consumer Electronics with a Hybrid Classical–Post-Quantum Framework”, *IEEE Transactions on Consumer Electronics*, 2025.

[3] I. Lee and Y. Back, “PQC SPHINCS+ 전자 서명 알고리즘의 효과적인 하드웨어 설계에 관한 연구”, in Proc. *Korean Information Processing Society Conf.*, vol. 30, no. 1, pp. 239-241, 2023.