SDV OTA 백엔드 웨이브 전환 경쟁 조건과 계층적 안전 전환 프로토콜

엄 경 문#1).박 건 호#2).강 보 근2).이 훈 희3).조 병 용3)

동국대학교 정보통신공학과1).국민대학교 자동차IT융합학과2).㈜락코리아3)

Race Conditions and Safe Transition Protocol in SDV OTA Wave Switching

Kyeongmun Eom#1)·Kunho Park#2)·Bogeun Kang2)·Celia Lee3)·Brandon Jo3)

Information and communication engineering, Dongguk University, Seoul 04620, Korea1),
Department of Automobile and IT Convergence, Kookmin University, Seoul 02707, Korea2),
ROCK KOREA, Seoul 05022, Korea3)

Key words : Software-Defined Vehicle(소프트웨어 정의 차량), OTA Update Security(OTA 업데이트 보안), Race Condition(경쟁 조건), Safe Transition Protocol(안전 전환 프로토콜), Kubernetes(쿠버네티스), Istio AuthorizationPolicy(Istio 인가 정책), Microsegmentation(마이크로세그먼테이션)

E-mail: 2021112042@dgu.ac.kr
# Equal contribution and first authorship

소프트웨어 정의 차량(Software-Defined Vehicle) 환경에서 OTA(Over-the-Air) 업데이트는 차량 기능의 지속적 개선뿐 아니라 보안 패치 적용, 규제 준수, 차량 가용성 유지에 직결되는 핵심 운영 메커니즘으로 자리 잡고 있다. 주요 OEM의 OTA 플랫폼은 대규모 차량군(fleet)을 한번에 모두 갱신하지 않고, 차량을 여러 집단으로 나누어 순차적으로 배포하는 웨이브 단위 업데이트를 수행하기 위해 클라우드 네이티브 아키텍처를 도입하고 있으며 [1),2)], 이러한 환경에서 OTA 캠페인의 웨이브별 활성화 및 비활성화 과정에 연동된 동적 보안 정책과 워크로드 전환은 차량군 업데이트의 보안성과 운영 안정성을 동시에 좌우하는 핵심 요소가 된다. 그러나 OTA 웨이브 전환 과정에서 워크로드 활성화와 접근제어 정책 전파는 서로 독립적인 비동기 작업으로 수행되며, 그 실행 순서는 시스템 구조상 보장되지 않는다. 이로 인해 발생하는 시간 간극(temporal gap) 기반 경쟁 조건(race condition)은 OTA 경로의 일시적 과개방이나 정상 업데이트 요청 중단을 초래할 수 있다. 더욱이 OTA 백엔드는 차량 또는 ECU 대상 선정, 캠페인 승인, 업데이트 패키지의 무결성·진위성 검증, 웨이브 단위 배포와 결과 회수와 같이 순차적 의미를 갖는 내부 파이프라인으로 구성되므로, 웨이브 전환의 외부 안전성이 확보되더라도 단계 간 허용 경로가 엄격히 제한되지 않으면 내부 우회 및 비인가 횡적 이동을 통해 후속 배포 단계로의 비정상적 접근이 가능하다.

기존 OTA 보안 연구는 차량 단말 측에서 업데이트 패키지의 무결성과 진위성 보장에 주로 집중해 왔으며[3),4)], 클라우드 네이티브 보안 연구는 Zero Trust 아키텍처[5)], 동적 접근제어 등을 제안해 왔으나 대부분 정상 상태에서의 보안 속성에 초점을 맞출 뿐 정책 전환 과정 자체의 안전성은 충분히 다루지 않는다. 그러나 Kubernetes 환경에서 Istio AuthorizationPolicy의 전파와 Pod 준비 완료는 비동기 작업이므로 비결정적 지연이 존재하며[6),7),8)], 이로 인해 전환 과정에서 비인가 통신 허용 또는 정상 요청 중단이 발생할 수 있다. 자동차 OTA 맥락에서 이는 비대상 차량군의 업데이트 수신이나 리콜 대응 긴급 패치의 전달 실패로 이어질 수 있으며, 내부 OTA 서비스 간 통신 경로가 과도하게 허용되어 있으면 공격자는 제한된 초기 침해 권한만으로도 후속 배포 단계로 이동할 수 있다.

본 연구는 공격자가 OTA 백엔드 내 단일 최소실행단위(Pod) 또는 컨테이너 안에서 코드 실행 권한을 획득하였으나, Kubernetes API 제어 권한 및 호스트 수준 권한은 보유하지 않은 위협 모델을 가정한다. 이러한 조건에서 본 연구는 Kubernetes 기반 자동차 OTA 백엔드의 보안을 외부 웨이브 전환 계층과 내부 파이프라인 계층으로 구분하여, 두 계층 모두에서 순서 보장이 필요함을 보인다. 먼저, 웨이브 활성화 단계에서의 3가지 전환 순서, 비활성화 단계에서의 3가지 전환 순서, 그리고 이를 조합한 end-to-end 전환 수명주기 9가지 시나리오를 정의하고, 각 시나리오별 보안 홀(비인가 통신 허용 구간)의 존재 여부와 지속 시간, 가용성 장애의 발생 여부와 영향 범위를

Kubernetes + Istio 실험 환경에서 측정한다. 이어 OTA 파이프라인을 인증, 캠페인, 패키지 검증, 배포의 단계로 구조화하고, 각 단계 간 허용 통신을 최소 권한 원칙에 따라 정의한 NetworkPolicy 및 AuthorizationPolicy 규칙을 설계하여, 정책 부재 시 가능한 내부 우회 시나리오와 정책 적용 후의 차단 효과를 실험적으로 검증한다.

이를 바탕으로 본 연구는 계층적 안전 전환 프로토콜(Hierarchical Safe Transition Protocol)을 제안한다. 제안 프로토콜은 각 단계 사이에 조건 게이트(condition gate)를 두어 비동기 작업 간 순서를 강제한다. readiness probe만으로는 전환 안전성이 보장되지 않으므로, Envoy 사이드카 초기화와 AuthorizationPolicy 동기화 완료를 추가 조건으로 확인한 뒤에만 트래픽을 허용한다. 또한 내부 OTA 파이프라인에 대해서는 단계별 서비스 간 허용 경로를 명시적으로 제한하여, ECU 호환성이 확인되지 않은 패키지가 배포 큐에 진입하거나 적격성이 검증되지 않은 VIN에 캠페인이 할당되는 것을 구조적으로 차단한다. 웨이브 비활성화 시에는 기존 Pod에 대한 신규 요청 유입을 먼저 차단하고, 진행 중인 요청이 안전하게 완료되도록 drain 구간을 둔 뒤, 기존 Pod 제거와 관련 정책 차단을 순차적으로 수행함으로써 보안 노출과 서비스 중단을 최소화한다. 이 프로토콜은 Kubernetes Custom Resource(OTAWave CR)와 커스텀 컨트롤러를 통해 자동화된다.

본 연구의 기여는 다음과 같다. 첫째, Kubernetes 기반 OTA 백엔드에서 외부 웨이브 전환 과정과 내부 OTA 파이프라인 단계 간 통신을 함께 고려해야 하는 계층적 보안 문제를 정의하고, 웨이브 활성화 3가지, 비활성화 3가지, end-to-end 조합 9가지 전환 시나리오별 보안 홀과 가용성 영향을 분석한다. 둘째, readiness probe만으로는 전환 안전성을 충분히 보장할 수 없음을 보이고, Envoy 사이드카 동기화와 정책 전파 완료를 포함하는 다단계 조건 게이트 기반의 안전 전환 프로토콜을 제안한다. 셋째, 외부 전환 게이트와 내부 단계별 마이크로세그멘테이션을 결합한 계층적 안전 전환 프로토콜을 설계하고, 정상 상태의 노출도를 측정하는 공격 시간 창(Attack Window)과 전환 과정의 노출도를 측정하는 전환 위험 구간(Transition Risk Window) 세 구성을 비교 평가하는 분석 프레임워크를 제공한다. 넷째, Kubernetes + Istio 기반 OTA 파이프라인 실험 환경에서 정책 전파 지연, 보안 홀 지속 시간, 내부 우회 차단 성공률을 측정함으로써 제안 기법의 유효성을 실증적으로 검증한다.

References

1) K. Rehman et al., "A Cloud-based Development Environment using HLA and Kubernetes for the Co-simulation of a Corporate Electric Vehicle Fleet," 2019 IEEE/SICE International Symposium on System Integration (SII), Paris, France, 2019, pp. 47-54.
2) N. Nayak, D. Grewe and S. Schildt, "Automotive Container Orchestration: Requirements, Challenges and Open Directions," 2023 IEEE Vehicular Networking Conference (VNC), Istanbul, Turkiye, 2023, pp. 61-64.
3) S. Halder, A. Ghosal, M. Conti, "Secure over-the-air software updates in connected vehicles: A survey," Computer Networks, vol. 178, 107343, 2020.
4) T. K. Kuppusamy, S. Awwad, and J. Cappos, "Uptane: Security and customizability of software updates for vehicles," IEEE Vehicular Technology Magazine, vol. 13, no. 1, pp. 66-73, Mar. 2018.
5) S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST Special Publication 800-207, Aug. 2020.
6) D. A. Hahn, D. Davidson, and A. G. Bardas, "MisMesh: Security Issues and Challenges in Service Meshes," in Security and Privacy in Communication Networks (SecureComm 2020), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 335, Springer, 2020, pp. 140–151.
7) M. Fogli et al., "Performance Evaluation of Kubernetes Distributions (K8s, K3s, KubeEdge) in an Adaptive and Federated Cloud Infrastructure for Disadvantaged Tactical Networks," 2021 International Conference on Military Communication and Information Systems (ICMCIS), The Hague, Netherlands, 2021, pp. 1-7.
8) W. Li, Y. Lemieux, J. Gao, Z. Zhao, and Y. Han, "Service mesh: Challenges, state of the art, and future research opportunities," 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 2019, pp. 122-1225.