블록체인 기반 SBOM 무결성 보장 연구 동향 분석

조근희 [1], 김미희 [2]
[1] 한경국립대학교 컴퓨터응용수학부 학부생
[2] 한경국립대학교 컴퓨터응용수학부 (컴퓨터 시스템 연구소) 교수

rmsgml0915@hknu.ac.kr, mhkim@hknu.ac.kr(교신저자)

Analysis of SBOM Integrity Guarantee Research Trends Based on Blockchain

Geun-hee Cho[1], Mi-hui Kim[2]
School of Computer Engineering & Applied Mathematics, Han-kyong National University

요 약

최근 오픈소스를 활용한 개발의 증가와 더불어 보안이 미숙한 업데이트 서버 혹은 제조업체를 대상으로 한 소프트웨어 공급망 공격이 증가하고 있다. 이에 이 위험성을 인식하고 다양한 연구와 조치를 통해 해당 공격에 대응하고 있다. 그 중 SBOM(Software Bill of Materials)을 이용하는 방법에서 SBOM 의 무결성의 보장을 위해 블록체인을 이용한다. 이 논문에서는 블록체인을 이용하여 무결성을 보장을 연구한 논문들을 비교 분석한다. 더 나아가 블록체인을 이용한 SBOM 무결성 보증 시스템의 설계 방향을 제언한다.

1. 서론

최근에는 오픈소스를 활용하여 개발하거나 아웃소싱으로 소프트웨어를 이용하게 되는 경우가 많아지고 있다. 또한 이용하는 최종기업의 보안이 강화됨에 따라 상대적으로 보안이 미흡한 업데이트 서버 혹은 제조 납품업체를 대상으로 한 공격이 증가하고 있다. 이에 따라 세계 각국에서 SBOM(Software Bill of Materials)을 활용하고 있다. 이를 통해 소프트웨어의 구성요소를 파악하여 위협을 빠르게 파악해 공격들에 대응하고 있다.

하지만 SBOM 또한 조작이 가능하므로 SBOM 의 무결성을 보장하는 것 또한 매우 중요하다. 따라서 이를 보장하는 방법으로 블록체인을 이용하려고 한다. 본 논문에서는 블록체인을 사용하여 SBOM 의 무결성을 보장한 논문들을 비교 분석한다.

2. 소프트웨어 공급망 공격

소프트웨어 공급망 공격이란 소프트웨어의 개발, 배포, 운영 과정 중에서 공격을 받아 소프트웨어의 구성요소가 변경되어 발생하는 각종 보안 위협을 의미한다[2]. 소프트웨어 공급망 공격은 사전탐지가 어렵고 피해가 광범위하고 지속적이다는 특징을 갖고 있다[1]. 2020 년에 일어났던 솔라윈즈 공격은 공격자가 솔라윈즈의 Orion 플랫폼의 업데이트 서버에 침투하여 백도어를 삽입하였던 공격으로 솔라윈즈의 경우 많은 미국의 핵심 연방 조직들과 글로벌기업들이 이용중이었기에 많은 피해를 야기한 공격이다[2].

2.1 공급망 공격의 대응책인 SBOM 과 업계 동향

따라서 이 공격들에 대응하기 위해 국외에서는 SBOM 을 도입하고 제도화를 추진하였다. SBOM 이란 소프트웨어 구성요소 명세서로 소프트웨어의 구성요소들이 작성되어 있어 구성요소들의 의존성을 쉽게 파악할 수 있다. 따라서 취약점이 발견되었을 때에 이를 통해 빠르게 대응할 수 있다. 또한 SBOM 제출을 의무화한 EO14028 행정명령에서 SBOM 의 데이터 필드와 자동화 지원, 관행 및 프로세스의 세 영역으로 구성되는 최소요소와 필수 형식을 게시하여 SBOM 의 기능을 지원하였다[3].

3. SBOM 의 무결성 보장을 위한 블록체인 적용

하지만 만약 공격자가 SBOM 을 위변조한다면 SBOM 이 공격을 대응하는 유효한 방법이 될 수 없다. 따라서 SBOM 의 무결성을 보장하는 것이 매우 중요하다. 현재는 개발사에서 제공하는 소프트웨어의 파일에 대한 해시값과 사용자가 다운로드하여 구한 해시값의 비교를 통하여 무결성을 검증하고 있다. 하지만 공격자가 소프트웨어에 악성코드 설치 시에 해시

값도 위변조할 수 있다는 한계를 가지고 있다[3].

블록체인은 중개자 없이 원장을 공유하는 방법으로 무결성과 신뢰성을 보장하는 신기술로 스마트컨트랙트 블록체인 기술을 통해 SBOM 의 무결성과 신뢰성을 보장할 수 있다[2].

3.1 블록체인 시스템을 이용한 연구에 대한 분석 및 고찰

블록체인을 사용하여 SBOM 의 무결성을 보장한 3 가지 연구를 분석하였다.

<표 1> 블록체인으로 SBOM의 무결성을 보장한 연구 비교

	[1]	[2]	[3]
제안 방식	개발한 소프트웨어의 메타정보들을 블록체인에 저장	소프트웨어 부품 유통기록 블록을 생성 및 SBOM은 비밀데이터로 전달	스마트컨트랙트를 활용하여 SBOM생성 및 저장
사용 기술	블록체인 기반의 데이터베이스	하이퍼레저 블록체인의 채널과 비밀데이터	스마트컨트랙트 블록체인
무결성 보장 방법	납품받은 소프트웨어와 블록체인에 등록된 SBOM을 통해 소프트웨어의 형상을 비교	블록체인에 저장된 SBOM의 해시값과 전달받은 SBOM의 해시 비교	홈페이지에 공표된 해시값과 블록체인의 해시값을 비교
저장되는 블록의 이름	공급내용 블록, 소프트웨어 정보 블록	소프트웨어 유통기록 블록	SBOM
블록 구성요소	도입기관, 공급기관, 소프트웨어 이름, 버전, 블록ID, 발급기관 서명등	공급자, 피공급자, SBOM 해시값	SW공급자명, SW이름, SW버전, SW Hash
소프트웨어 구성요소 공개	참가하는 모든 참가자에 공개	하이퍼레저 블록체인을 사용하여 기밀성을 보장	스마트컨트랙트 기술을 활용하여 참가하는 모든 노드에 공개
추가 인증	공개 키 기반 디지털 서명으로 1차인증, 발급받은 인증서로 개발사 신원 2차 인증	추가 인증 없음	작성된 SBOM을 블록체인 참여자를 통해 디지털 서명 검증으로 인증

연구[1]의 경우 하청업체부터 개발업체까지 개발한 모든 소프트웨어의 정보를 블록체인에 저장하고 그것과 실제 납품 받은 소프트웨어와의 비교를 통하여 무결성을 검증한다 갖고 있다. 연구[2]의 경우 SBOM 의 해시만 블록체인에 등록하고 SBOM 은 비밀데이터로 전송하여 해시값의 비교를 통해 무결성을 검증한다. 연구[3]의 경우 개발사의 홈페이지에도 SBOM을 등록하여 그것의 해시값과 블록체인에 등록된 SBOM 의 해시값을 비교하여 무결성을 보장한다.

3.2 블록체인을 이용한 SBOM 무결성 보증 시스템 설계 방향

앞서 살펴본 연구들은 모두 블록체인을 이용하여 SBOM 의 무결성을 보장한다는 공통점을 가진다. 하지만 연구[1]의 경우 모든 소프트웨어의 정보를 블록체인에 등록하므로 블록이 너무 많아져 비효율적이고 연구[3]의 경우 또한 홈페이지와 블록체인 두 곳에 SBOM을 매번 올려야 하기에 비효율적이라 분석된다. 그에 비해 연구[2]의 경우 SBOM 을 블록체인에 올리는 것이 아닌 비밀데이터로 전송하고 SBOM 의 해시값만 올리므로 블록체인에 적은 데이터만으로도 무결성을 보장할 수 있기에 가장 효율적이라고 분석된다. 하지만 연구[2]의 경우에도 채널을 나누고 비밀데이터를 전송하는 것에 취약점이 존재 가능하다. 블록체인을 이용한 SBOM 무결성 보증 시스템을 설계하되 효율성과 보안성을 함께 고려해야 한다.

4. 결론

최근 오픈소스를 활용한 개발의 증가와 더불어 보안이 미숙한 제조업체를 대상으로 소프트웨어 공급망 공격이 증가하고 있다. 이에 따라 대한민국을 비롯한 세계 각국에서는 SBOM 을 제안하여 공격을 대응하고 있고, 본 논문에서는 SBOM 의 무결성을 보장하는 3 가지 연구에 대하여 분석하였다. 블록체인을 이용하는 방법은 효과적이나 SBOM 을 어떻게 제공하는지 그리고 무결성을 보장하는 방법에 따라 블록체인 네트워크의 효율이 달라질 수 있다. 향후 연구로서 효율성과 보안성을 강화한 블록체인 기반 SBOM 보증 시스템을 설계하고자 한다.

사사 (Acknowledgement)

이 논문은 한경국립대학교 국립대학육성사업(2025) 지원을 받아 작성되었음

참고문헌

[1] 김정우, 국경완, 류연승, “블록체인 활용 연구사례 분석을 통한 소프트웨어 공급망 보안 강화 방안 연구,” 융합보안논문지, 24(5), 2024, pp.55-61.

[2] 김광준, “블록체인 기반 소프트웨어 공급망 보증 시스템,” 한남대학교 박사학위논문,2023.

[3] 정재은, 백남균, “SBOM 의 무결성 확보를 위한 스마트컨트랙트 블록체인 활용 방안 연구,” 한국산업보안연구, 13(2), 2023, pp.105-120.