국·내외 SW공급망보안 현황 및
SBOM 도구 실증
결과보고서

2024. 12.

kisia 한국정보보호산업협회

※ 이 보고서는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 보고서임 (RS-2022-II220277, SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발 과제)

국·내외 SW공급망보안 현황 및 SBOM 도구 실증 결과보고서

1. 보고서 개요

Chapter 1

보고서 개요

1) 추진 배경

사람, 사물이 유기적으로 연결되어 소통하고 상호 작용하는 초연결사회가 도래하고 디지털 전환이 가속화됨에 따라 전 분야에서의 SW융합이 촉진되고 SW재사용에 기반한 분업화된 조립식 개발이 일상화되고 있다.

최근 SW 개발비용과 시간을 절감하기 위하여 모든 구성요소를 자체 개발하는 것이 아닌 소스코드가 공개되어 누구나 자유롭게 수정 및 배포가 가능한 오픈소스SW 또는 상용SW 등이 널리 사용됨에 따라 제3자가 개발한 SW를 활용함으로써 라이선스·보안·품질 위협이 동반되고 있다.

대표적으로 2020년의 Solarwinds, 2021년의 Log4j의 대형사고 뿐만 아니라 2023년 3CX 사태, 국내 주요기관 60여곳의 PC 210여대 해킹 사태 등 공급망 공격 사례는 계속해서 발생하고 있고 그 수와 규모도 증가하고 있다. 가트너는 2021년보다 3배 증가한 규모로써 2025년까지 전 세계 조직 45%가 소프트웨어 공급망 공격을 겪게 될 것[1] 이며 사이버시큐리티벤처스는 2025년까지 피해액이 600억 달러, 2031년 1,380억 달러에 이를 것으로 예상했다[2]. 이처럼 공급망 공격은 그 피해규모가 크고 광범위하며 지속적이라는 특징을 나타내고 있다. 이로 인해 사이버보안의 강화 필요성이 증가하고 있으며 SW공급망 투명성 확보 필요성이 제기되었고, 전세계는 방안 중 하나로 소프트웨어의 구성요소와 의존성을 기록해 나타내는 명세서인 SBOM (Software Bill of Materials)에 주목하기 시작하였다.

2) 연구의 목표 및 내용

본 보고서에서는 국내 및 미국, EU, 일본을 중심으로 한 해외 주요국의 소프트웨어 공급망 보안 정책과 최신 동향을 소개하고 SBOM의 개념과 필요성, 미국 NTIA의 도구 기능 유형과 최소구성요소를 소개한다. NTIA 도구 기능 유형, 최소구성요소 기준에 따라 국내 정보보호기업 3개 社를 대상으로, 본 연구를 통해 개발된 SBOM 자동생성 도구인 HatBOM과 취약점탐지도구 Vuddy의 실증을 진행한 결과와 SBOM 도구의 실효성 검증 및 정책적·제도적 개선사항을 기술하였다. 이를 통해 R&D 연구개발 과제의 산출물인 SBOM 자동생성 도구 및 기술의 완성도를 높임이 연구의 목표이다. 연구내용은 다음과 같다.

1) Gartner(2024.6.), “Leader’s Guide to Software Supply Chain Security”
2) Snyk, Cybersecurity Ventures(2023), “2023 Software Supply Chain Attack Report”

구 분	세부내용
국내·외 SW공급망보안 동향	- 주요국가(미국,EU,일본)별 SW공급망보안 정책 및 전략 - 국내 SW공급망보안 현황
SBOM	- SBOM 기본개념과 필요성 - SBOM 표준형식 - NTIA 기준 SBOM 도구 기능 유형 / 최소구성요소
SBOM 도구 실증 결과	- R&D연구개발 결과물 소개 - 실증개요 및 기업별 실증 세부 결과

2.
국내·외 SW 공급망 보안 동향

Chapter 2

국내·외 SW 공급망 보안 동향

1) 주요 국가별 정책 및 전략

1-1) 미국

Solarwinds 등의 대규모 SW공급망 공격이 발생하고 이에 피해가 발생함에 따라 미국 바이든 행정부는 공급망 보안의 중요성을 인식하고 2021년 5월, 「국가 사이버보안 향상에 관한 행정명령(EO 14028)」을 발표하였다. 행정명령은 위협정보 공유, 제로트러스트 아키텍처 도입 등의 내용을 담고 있으며, 그 중 4절에서 SW공급망보안을 강화하기 위한 프레임워크를 언급한다. 4절은 다음과 같은 내용을 담고 있다.[3)]

- SBOM(소프트웨어 자재 명세서)에 대한 최소 구성요소 공표
- 중요 소프트웨어 (Critical Software)에 대한 용어 정의 및 목록파악, 관련된 보안 지침 발표
- 소프트웨어 공급망 보안을 강화하는 가이드라인 발행
- 소프트웨어 소스코드에 대한 공급업체의 테스트 최소 표준 지침 발표

[표 1] Sec.4. Enhancing Software Supply Chain Security

이에 상무부는 SW 공급망보안 가이드ㅁ를 연방기관이 준수하도록 하는 메모랜덤을 발송하였다. 기존 내용을 업데이트 한 메모랜덤에서 연방정부에 SW를 납품하는 공급자에게 미국 국가기술표준원(NIST)의 '안전한 SW 개발 체계(SSDF)' 모범사례 준수를 요구하며 이를 수행했음을 선언하는 '자체증명서(Self-Attestation-Form)'을 제출하도록 하는 내용을 명시했다.

법적인 제도화 이전 미국은 실제산업(의료, 에너지 등)에서의 실증을 수행하였고 가이드배포, 조달 규정 개정, 유관 법안 발의를 통해 SBOM 확산을 위한 기반을 마련하였다. 식품의약국(FDA)은 2023년 10월, 의료기기의 인허가 시 SBOM 제출을 의무화하여 제도를 시행중이다.

미국 사이버보안 및 인프라보안국(CISA)은 2024년 3월, 메모랜덤을 보완하는 안전한 소프트웨어 개발 증명양식(Secure Software Development Attestation Form)을 확정하여 공개하였다. 이로부터 90일 후인 6월부터 연방정부 납품 Critical Software에 대한 증명 수집 시행, 180일 후인 9월부터 모든 Software에 대해 증명 수집이 확대되었다.[4)]

3) Federal Reguster(2021), "Executive Order 14028, Improving the nation's Cybersecurity"

이처럼 미국은 실증 및 제도화 단계를 거쳐 공공·민간에서의 SBOM의 상용화를 앞당기며 SW공급망보안 관리 정책 시행단계에 접어들고 있다.

1-2) 유럽(EU)

2016년 7월, 유럽의회는 EU 최초의 사이버보안 규정 'NIS(The Network and Information Security)를 채택하여 회원국에 대해 주요 기반 시설과 서비스 제공자에게 보안 조치를 요구하며 유럽 전역의 사이버보안 수준을 향상시키고자 하였다. 하지만 명확하지 않은 세부사항 및 주요 기반시설과 디지털 서비스 제공자에게만 한정된 규정의 한계를 확인하고 2022년 12월, 유럽 의회는 NIS에 대한 업데이트를 승인하여 'NIS2(Directive on Security of Network and Information Systems 2)'를 채택하였다.

NIS2는 SBOM을 명시적으로 언급하지는 않지만 공급망 보안 영역에서는 공급망 전반에 걸쳐 다양한 보안조치를 요구하고 있으며, 모든 공급업체에 통일된 보안 기준의 설정, 공급망 위험평가와 관리, 협력사 보안감사(보안 사고 발생에 따른 책임과 대응 방안 규정), 공급망 전반에 대한 실시간 모니터링과 위협탐지 시스템 구축 등을 규정하고 있다.[5)]

NIS2법안 외에도 유럽은 2023년, 네트워크 연결 장비의 최소 사이버보안 기준 도입 및 중요 품목의 인증절차 강화를 위한 법으로 사이버복원력법([6)]CRA, Cyber Resilience Act) 최종법안에 합의, 2024년 3월에 승인, 10월에 CRA의 이사회 채택이 있었다. CRA 법안은 네트워크에 대한 직·간접적인 데이터 연결을 포함하는 하드웨어 및 소프트웨어를 대상으로 하며 2027년부터 효력이 발생할 예정이다.

사이버복원력법(CRA, Cyber Resilience Act)

- 제조업체가 수명 주기 전체에 걸쳐 디지털 요소가 포함된 제품의 보안을 개선하도록 보장
  (적합성평가를 통해 CE 마크 부착 여부를 결정하는데 이때 SBOM 제출 의무화 계획)
- 일관된 사이버보안 프레임워크를 보장하여 하드웨어 및 소프트웨어 생산자의 규정 준수를 용이하게 함
- CRA의 필수 사이버 보안 요건이나 책임 의무를 준수하지 않을 시, 최대 1,500만 달러 이상의 벌금 부과

[표 2] EU 사이버복원력법

또한 EU는 IoT분야의 SW공급망보안 강화를 위해 분산형 SBOM 관리 모델을 실증하는 프로젝트로 D-SBOM (Distributed SBOM)[7)]을 추진하였다. 블록체인과 DLT를 사용하여 개발된 D-SBOM을 통해 소프트웨어를 문서화하고 알려진 소프트웨어 취약성(CVE)에 조치를 취함으로서 그 효과성을 입증한다는 계획이다. 독일의 IoT SW공급망 보안 전문 기업 asvin에서 프로젝트를 추진하였으며 개발된 결과물을 자동차 산업에 적용하여 검증할 예정이다.

4) CISA(2024.3.), "Secure Software Development Attestation Form Instructions"
5) European Union (2022.12), "Directive (EU) 2022/2555 of the European Parliament and of the Council"
6) European Parliament(2022.9.), "Regulation of the European Parliament and of the council : on horizontal cybersecurity requirements for products with digital elements and amending Regulation(EU) 2019/1020"
7) Trublo.eu "https://www.trublo.eu/d-sbom/"

1-3) 일본

일본정부는 경제산업성(METI)에 소프트웨어 Task Force (SW TF)를 설치하여 실증사업을 통해 SBOM의 모범 사례를 확인하고 활성화하고자 하였다. 전담 TF를 통해 SW 벤더 및 기업의 협력으로 자동차 안전 검증 SW 'GARDEN'을 선정하여 실증사업을 진행하였고 이를 의료·자동차·SW 분야에 확장시키는 계획을 수립하였다. 이러한 실증사업 결과를 바탕으로 SBOM 활용 사례를 담은 오픈소스 우수사례집을 발간해 SBOM 확산을 추진중에 있다.

총무성은 또한 ICT 사이버보안 종합대책 2022[8]에서 SBOM 제도화 검토 필요성을 적시해 SBOM 적용 범위를 ICT 전반으로 확대할 것을 시사하였다. 내용으로 전국 5G의 특정 기지국 개설 설계 인정 및 지역 5G 면허 시, 공급망 위협 대응을 포함한 사이버보안 대책 강구를 조건으로 요구, SW공급망 위협 대응을 위한 향후의 대처 중 하나로 SBOM 도입 가능성 검토를 제시하였다.

> "Apache Log4j와 같은 널리 사용되는 SW구성요소의 취약성에 대처하는 것이 중요해지고 있는 동안 SW제품의 구성요소를 관리하고 취약성에 신속하게 대응할 수 있는 **메커니즘인 SBOM(Software Bill of Materials)의 경우, 정보통신 분야에서의 도입가능성을 검토하는 것이 적절**하다. 또한, 널리 보급되는 통신용 어플리케이션 등에 관한 이용 상 주의 방식을 검토해 나가는 것이 적당하다" - ICT 사이버보안 종합대책 2022 中

2023년 7월, 일본 경제산업성은 '소프트웨어 관리를 위한 SBOM 도입에 관한 안내'[9]에 대한 첫 번째 버전을 공개하고 2024년 5월, 두 번째 버전을 공개하였다. SBOM 채택을 통해 소프트웨어 취약점 관리를 개선하고 기업의 개발생산성 증가, 산업계의 사이버 보안 능력 향상을 기대하고 환경 설정, SBOM 작성 및 공유, SBOM 운영 및 관리, 계약 규정 사항, SBOM 도입 효과 등 SBOM 구현을 위한 단계별 세부 절차 등 패키지 및 임베디드 소프트웨어 기업을 위한 상세 가이드를 제공한다.

2024년 7월, 총무성의 사이버보안 TF는 사이버보안 2024(サイバーセキュリティ2024)[10]를 통해 공개 SW의 급속한 확대로 통신 분야 공급망에 대한 SBOM 도입이 우선이라고 명시하며 통신 공급망보안에 주력할 것을 밝혔다. 이에 따라 수작업과 툴활용 두가지 방법으로 SBOM을 작성해 비교·검증하며 SBOM 도입에 대한 과제를 정리하고 해외사례 조사 및 전문가 회의를 통한 SBOM 도입을 검토하는 등 SBOM 실증을 위해 다양한 분야에서 노력하는 중이다.

8) 총무성(総務省, 2022) "ICT サイバーセキュリティ総合対策 2022"
9) 경제산업성(経済産業省, 2023.7.), "ソフトウェア管理に向けた SBOM(Software Bill of Materials)の導入に関する手引 Ver. 1.0"
10) NISC (サイバーセキュリティ戦略本部, 2024.7.), "サイバーセキュリティ 2024"

2) 국내 SW 공급망 보안 현황

현재 SW공급망보안에 대한 국제적인 관심에 따라, 정부 기관 및 국내 기업들 또한 SBOM의 중요성을 인식하고 도입을 위해 노력하고 있는 중이다.

정부는 'SW 공급망 보안 관리체계 적용·확산'에 25년 신규예산으로 60억원을 편성[11]하여 SW공급망에서 보안의 중요성을 인식하였음을 드러냈다.

국내 SW 공급망 보안 관련 정책은 과학기술정보통신부, 국가정보원, 디지털플랫폼정부위원회가 중심이 되어 추진하고 있다. 과학기술정보통신부, 국가정보원, 디지털플랫폼정부위원회는 합동으로 'SW 공급망 보안 가이드라인'을 발간하여 SW 공급망 공격에 대응, 공급망의 투명성을 확보해 SW 품질을 높이고, SBOM 규제에 따른 해외 무역 장벽을 극복할 수 있도록 지원하였다. 공급망보안 가이드라인은 △SW 공급망 위기 대응의 필요성과 주요국의 정책 동향 △공급망 위험관리, SW 개발·운영환경의 공급망 보안체계 구축 방안과 SBOM △SBOM 실증사례 △테스트베드, 국내 표준과 속성규격 등 활성화 지원의 내용이 담겨있다.

국가 차원의 공급망 보안 관리체계 확산 및 법 제도화 노력 외에 국내 기업·기관들도 국제적 동향에 발맞춰 SBOM을 도입하려는 노력을 이어가고 있다. 래브라도랩스는 국내 최초로 SBOM 생성솔루션을 통해 해외 시장에 진출[12], 스패로우, 쿤텍 등은 SBOM 명세서 출력을 포함한 SW공급망보안 관리 솔루션을 출시[13]함으로서 SW 생태계에 SBOM 솔루션을 공급하고 있다. 또한 기상청 등 공공기관에서 인프라 도입사업 공고 시 SBOM 제출을 요구하는 경우도 생겨나 SBOM의 수요 또한 증가한 것으로 보여진다.

이와 같이 정부 및 국내 기업에서도 SW공급망보안의 중요성과 SBOM 도입을 염두에 두고 산업에 적용하려는 움직임을 보이고 있다. SBOM을 도입하는데 있어서 부작용을 최소화하기 위해 정부 기관 차원에서 국내 실정에 맞는 제도와 그를 뒷받침하는 지원 정책의 수립하려고 지속적으로 노력하고 있으며, 산업계에서도 SBOM에 관심을 가지고 대응을 하고 있음을 알 수 있다.

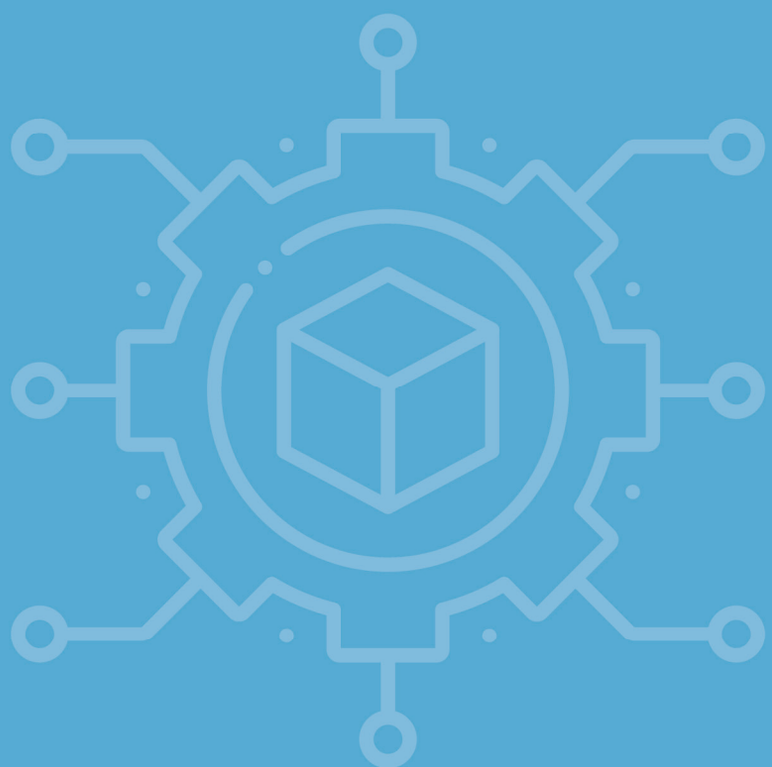
11) 과학기술정보통신부 보도자료(2024.08.) "과기정통부, 선도형 연구개발 체제 전환을 통한 미래도약 가속화"
12) 지디넷코리아, "래브라도랩스, SW공급망 자동관리플랫폼 '래브라도SCM' 출시"
13) IT Daily, "오픈소스 취약점 노린 SW공급망 보안 위협, 'SBOM'이 해결사 될까"

3) 국내·외 SW 공급망 보안 동향 요약

구 분	미국	EU	일본	국내
공급망 보안 정책 규제	- EO 14028을 통해 SBOM 구체화, SW공급망 보안 지침 정리 - 자체증명서 양식 확정 후 연방정부 납품 SW에 대한 증명 수집 - FDA, 의료기기 인허가시 SBOM 제출 의무화	- NIS2 업데이트를 통해 공급망 전반에 걸친 다양한 보안 조치 요구 - CRA 승인, 이사회 채택을 통해 디지털 요소가 포함된 제품의 보안 개선 (SBOM 의무화 계획)	- 경제산업성에 SW TF 설치하여 SBOM 사례 확인 및 가이드 배포 - ICT 사이버보안 종합대책에서 SBOM 제도화 필요성 적시 - 사이버보안 2024를 통해 통신 공급망보안에 주력할 것임을 명시	- SW공급망보안 관리체계 적용·확산에 60억의 신규 예산 편성 - SW공급망보안 가이드라인 발간 - SW공급망보안 TF 발족, 단계적 제도 시행 계획 마련 - 25.01.24 '디지털의료제품법' 시행, 의료기기 SW를 포함하여 안전성,유효성 확보의 법적기반 마련
SBOM 실증	- 헬스케어 부문, 에너지 부문에서 실증을 통해 가이드 배포, 조달규정 개정, 유관법안 발의	- IoT분야의 SW 공급망 보안 강화를 위해 블록체인, DLT를 사용하여 D-SBOM 실증 추진	- 수작업과 툴활용 두 가지 방법을 비교·검증하여 통신 SBOM 실증	- KISA SBOM 실증사업을 통해 가이드라인 기초데이터 마련

[표 3] SBOM 실증 조사 결과 요약 및 시사점

3. SBOM



Chapter 3

SBOM

1) SBOM의 기본개념과 필요성

최근 들어 SW공급망 공격은 그 피해규모가 크고 광범위하며 지속적이라는 특징을 나타내고 있다. 이로 인해 사이버 보안의 강화 필요성이 증가하고 있으며 SW공급망 투명성 확보 필요성이 제기되었고, 방안 중 하나로 SBOM (Software Bill of Materials)에 주목하기 시작하였다.

SBOM(Software Bill of Materials)은 소프트웨어 제품에 사용된 모든 구성 요소와 의존성을 기록한 목록으로 제조업에 사용되는 자재명세서(Bill of Materials, BOM)의 개념을 소프트웨어 분야에 적용한 것이다. SBOM에 대해 법적으로 정해진 규정은 없지만 일반적으로 라이브러리 등의 구성요소, 라이센스 정보, 버전 정보와 공급자 등의 내용을 표시하며 의존성을 나타내어 하나의 소프트웨어에 대해 그 구성요소들을 목록화하여 관리할 수 있도록 한다.

모든 구성요소를 자체개발하는 것이 아니라 다수의 오픈소스 또는 상용 소프트웨어를 사용하여 하나의 소프트웨어를 개발하는 오늘날의 소프트웨어 패키지에서는 이러한 구성요소 관리는 더욱 중요한 역할을 한다. 공급망 공격의 경우 변조된 업데이트가 정상 업데이트 서버로 배포되기 때문에 제3자 소프트웨어를 사용하는 사용자의 입장에서 변조된 파일임을 알아차리기 어렵다. Solarwinds 공급망 공격의 경우 18,000개 이상의 기관이 피해를 입었으며 피해를 입은 기업들은 1년이 넘게 그 취약성을 알아차리지 못했다.

SBOM 명세서를 통해 개발 소프트웨어의 구성요소를 목록화하고 파악한 후, 알려진 취약점 (CVE)을 사전에 식별하고 조치함으로서 공개 SW 활용에 따른 위험에 대응하고 피해를 최소화할 수 있다. 또한 개발·공급·운영 전반에 걸친 SW공급망보안 관리체계를 구축함으로서 SW 공급망의 투명성을 확보할 수 있으므로 SBOM의 중요성은 더욱 커지고 있다.

2) SBOM 표준 형식

현대 소프트웨어 시스템 공급망의 복잡성과 동적 특성은 투명성에 심각한 문제를 야기한다. 명확하고 일관된 형식으로 SW 구성요소를 수집하고 공유하여야 비용이 절감되고 디지털 인프라에 대한 신뢰를 확보할 수 있을 것이다. 표준 및 형식에 관한 NTIA 소프트웨어 투명성 실무 그룹(NTIA Software Transparency Working Group on Standards and Formats)은 디지털 인프라에 대한 신뢰를 높이기 위하여 SW 구성요소 관련 기존 표준 및 이니셔티브를 조사하였다. 그 과정에서 작업 그룹은 세 가지 형식이 일반적으로 사용된다는 사실을 발견하였다.

SPDX (Software Package Data Exchange)[14)]	- LINUX 재단에서 운영하는 프로젝트로서 출처, 라이선스, 보안 및 기타 관련 정보를 포함한 SBOM 정보를 전달하기 위한 개방형 표준 - ISO/IEC 5962:2021으로 채택된 국제 표준 - SPDX 프로젝트의 구성 · SPDX 사양 자체 · SPDX 라이선스 목록 · SPDX 문서 및 SPDX 라이선스 목록 작업을 위한 SPDX 도구 및 라이브러리
CycloneDX[15)]	- OWASP(Open Web Application Security Project) 커뮤니티에서 개발된 보안과 신뢰성에 중점을 둔 경량 SBOM 표준 - Ecma International에 의해 표준화되었으며 글로벌 보안 커뮤니티가 지원 - 패키지 URL, CPE, SWID, SPDX 라이선스 ID 및 표현과 같은 기존사양 포함 - 소프트웨어 구성 요소들을 XML, JSON, Protobuf 등 다양한 형식으로 표현 컴포넌트 이름, 버전, 설명, 라이선스, 제작자, 보안취약점 정보
SWID tags	- ISO에 의해 제정된 관리장치에 설치된 소프트웨어를 투명한 방식으로 추적할 수 있도록 하는 소프트웨어 식별태그 - ISO/IEC 19770-2:2015 국제 표준 - SW 제품의 특정 릴리스에 대한 정보 포함, 수명 주기를 간략히 설명 - Primary, Patch, Corpus, Supplemental(기본, 패치, 코퍼스, 추가) 4가지태그

[표 4] SBOM 표준 형식

3) NTIA SBOM Tool Classification Taxonomy

NTIA 투명성 작업그룹은 2021년, SBOM 도구에 대한 기능별 유형을 분류한 SBOM Tool Classification Taxonomy를 발표하였다. 작업 그룹은 SBOM 생성 및 소비의 다양한 사용 사례에 중요하다고 판단되는 다양한 유형의 도구를 분류하여 도구 제작자와 공급업체의 이해를 돕고자 다음과 같은 기능 유형을 제시하였다.[16)]

Category	Type	Description
생성	빌드(Build)	- SBOM은 SW 빌드의 일부로 자동 생성되며 빌드에 대한 정보를 포함한다
	분석(Analyze)	- SW 및 관련소스를 검사하는 등 소스 및 바이너리 파일을 분석하여 SBOM을 생성한다
	편집(Edit)	- 사람이 수동으로 SBOM 데이터를 입력하고 수정할 수 있도록 지원한다
소비	뷰(View)	- 사람이 읽을 수 있는 형식(그림, 표, 텍스트 등)으로 내용을 이해할 수 있어야 하며, 의사결정 및 비즈니스 프로세스를 지원하는데 사용한다
	비교(Diff)	- 다수의 SBOM 비교를 통해 차이점을 파악할 수 있다
	불러오기(Import)	- 처리, 분석을 위해 SBOM을 검색 및 시스템상으로 불러오기할 수 있다
변형	변환(Translate)	- 같은 정보를 유지하면서 다른 형식으로의 변환이 가능하다
	병합(Merge)	- 분석 및 검사 목적으로 다수의 SBOM과 데이터를 병합할 수 있다
	도구지원 (Tool Support)	- API, 객체모델, 라이브러리, 전송 또는 레퍼런스에 의한 기타 도구 사용을 지원한다

[표 5] NTIA SBOM 도구 기능 유형

14) The Linux Foundation Projects "About SPDX"
15) OWASP "CycloneDX One Pager"
16) NTIA SBOM Formats & Tooling Working Group "SBOM Tool Classification Taxonomy" (2021.03)

4) NTIA Minimum Elements for a SBOM

EO 14028 행정명령은 발표된지 60일 이내로 상무부가 NTIA와 협력하여 SBOM의 최소 구성요소를 공표하도록 지시하였다. NTIA와 상무부는 SW 생태계의 여러 전문가들을 소집하여 리소스를 도출함으로서 SW공급망에 대한 생산자, 구매자, 운영자 전반에 대한 이해를 높이고자 하였다. NTIA와 상무부는 2021년 다음과 같은 세가지 SBOM 최소 구성요소를 제시하였다.

Minimum Elements	
데이터 필드 (Data Fields)	- 추적 및 유지관리가 필요한 각 구성요소에 대한 기본정보 (Supplier name, Component name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM data, Time stamp)
자동화 지원 (Automation Support)	- SBOM은 기계판독이 가능하여야 하며 지속적인 데이터 추적을 위해 자동으로 생성될 수 있어야 한다. SBOM 데이터 형식에는 SPDX, CyCloneDX, SWID tags를 포함한다.
관행 및 프로세스 (Practices and Processes)	- SBOM 문서는 SBOM 생성 및 업데이트, 배포 및 액세스, 오류 처리에 대한 표준 관행 및 절차를 따라야한다. (Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control and Accommodation of Mistakes)

[표 6] NTIA SBOM 최소 구성 요소[17)]

SBOM의 핵심은 SW구성요소를 이해하는데 일관되고 균일한 구조를 가져야한다는 것이다. 그 중, 데이터 필드는 SBOM 명세서를 생성 했을 시 추적 및 유지 관리해야하는 SW 구성요소에 대한 기본 정보를 포함하고 있다.

Data Field	Description
공급자 이름 (Supplier Name)	- 컴포넌트를 생성, 정의, 식별하는 개인 또는 조직의 이름 (작성자, 제조업체)
컴포넌트 이름 (Component Name)	- 원래 공급자, 제조업체가 정의한 소프트웨어 요소에 할당된 이름 소프트웨어에 여러 이름과 별칭이 있는 경우 내용도 함께 표시
컴포넌트 버전 (Version of the Component)	- 이전 식별번호와 구분할 수 있도록 소프트웨어 제조업체가 지정한 식별자
기타 고유 식별자 (Other Unique Identifiers)	- 컴포넌트를 식별하거나 DB에서 구성요소를 찾기 위한 조회키로 사용되는 컴포넌트 이름 및 버전 이외의 추가 식별자
의존성 (Dependency Relationship)	- 컴포넌트가 상위 컴포넌트에 종속되어 있다는 관계에 대한 설명
SBOM 작성자 (Author of SBOM Data)	- SBOM 데이터를 생성한 개인 또는 조직의 이름
타임스탬프 (Timestamp)	- SBOM 데이터가 생성된 날짜와 시간에 대한 기록

[표 7] NTIA SBOM 최소 구성 요소

17) NTIA, Department of Commerce “The Minimum Elements For a Software Bill of Materials” (2021.07)

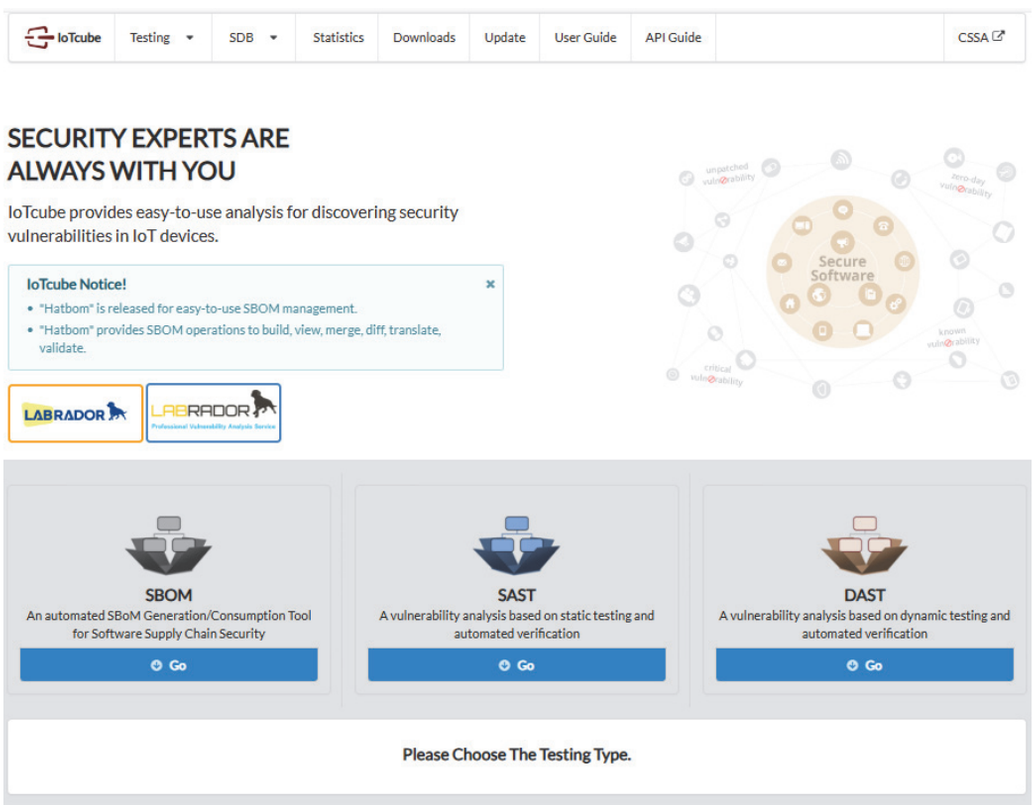
4.
SBOM 도구 실증 결과

Chapter 4

SBOM 도구 실증 결과

1) R&D 연구결과물 소개

고려대학교 소프트웨어보안연구소(CSSA)는 과학기술정보통신부 및 정보통신기획평가원이 지원하는 'SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발' 정부과제를 2022년부터 시작하여 2025년까지 진행중이며, 이에 따라 SBOM 자동생성 도구와 취약점 탐지도구를 개발하였다. 개발된 SBOM 자동생성도구 HatBOM과 취약점 탐지도구 Vuddy를 통해 SW 컴포넌트를 자동으로 관리하여 패치하고 특정 컴포넌트에 취약점·공급망공격이 발생 시 즉각적으로 업데이트함을 목표로 한다. 해당 도구들은 IoTcube 플랫폼에서 보안 전문가가 아닌 누구라도 이용할 수 있도록 개방되어 있는 도구들이다 (https://iotcube.net/)



[그림 1] SBOM 자동생성과 취약점분석기능을 이용할 수 있는 IoTcube 플랫폼

1-1) SBOM 자동생성도구 HatBOM

SBOM 자동생성도구인 HatBOM은 소스코드 기반의 소프트웨어를 분석하여 구성요소를 관리하고 분석할 수 있는 도구이다. 현재 HatBOM1(Build), HatBOM2(View, Translate), HatBOM3(Merge, Diff), HatBOM4(Validate) 4개의 기능을 제공하고 있다. hmark를 통해 소프트웨어의 해시인덱스파일(hidx)을 생성하여 드래그앤드롭 형식으로 업로드하면 SBOM을 자동으로 생성하고 종속성을 트리형태로 시각화해주는 것은 물론, 표준형식 간의 변환, 유효성 검증까지 모든 과정을 간편하게 진행할 수 있다. 해시파일 생성을 통해 구성요소와 의존성 정보를 파악함으로서 소스코드 외부 유출에 대한 우려 없이 SW공급망의 투명성 확보가 가능하다.

1-2) 취약점 탐지도구 Vuddy(Hmark)

취약한 코드 클론 탐지(VCC, Vulnerable Code Clone Detection)방식을 이용한 취약점 탐지도구이다. hmark를 통해 생성된 hidx파일을 IoTcube 플랫폼에 업로드하여 소프트웨어의 취약점을 효율적이고 정확하게 탐지할 수 있다. 발견된 취약점에 대해 그래프로 시각화하여 결과를 보여주며 알려진 취약점(CVE, Common Vulnerabillities and Exposures) 발견년도와 유형 등의 정보를 제공한다. 약 39만개가 넘는 취약함수 데이터베이스를 통해 기존 기술 대비 빠른 속도로 취약 코드 클론 탐지가 가능하며 추상화 모드를 이용해 유사한 코드 클론까지 탐지가 가능하다.

2) 실증 개요

과학기술정보통신부 및 정보통신기획평가원이 지원하는 'SW공급망보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발'연구 과제를 통해 개발된 SBOM 생성도구와 취약점 탐지 도구를 활용하여 국내 정보보호기업 3개 社를 대상으로 실증 조사를 실시하여 실효성을 검증하고자 하였다.

정보보호기업의 솔루션과 서브모듈을 가지고 1차 실증을 진행하였으나 가상환경 경로, 디렉터리 경로, 바이너리 파일 업로드 등의 문제로 인해 결과 산출이 미비하여 미비점을 보완 후 2차 실증을 진행하였다. 실증연구 전개 과정은 다음과 같다.

《실증연구 전개 과정》

기업 모집 및 선정	→	1차 실증	→	원인 분석 및 보완	→	2차 실증
- 실증기업모집 - 국내 정보보호기업 3개 社 선정		- 자사솔루션 실증 - 일부 컴포넌트 및 취약점 검출 미비		- 가상환경 경로, 디렉터리 경로, 바이너리 파일 등의 문제 확인 - 미비점 보완		- 2차 실증 진행 - 최종결과 도출

3) 기업별 실증 세부 결과

본 연구를 통해 개발된 도구를 통해 기업 솔루션의 SBOM을 추출, 취약점을 비교하여 개발한 도구의 실효성을 검증하고 정책적·기술적 애로사항 및 개선사항을 도출하는 데에 의의를 두었으며, 기업별 실증 세부 결과는 다음과 같다.

3-1) A사 실증 세부 결과

참여 배경 및 실증대상, 실증목적 및 기대성과

- 참여배경

  Log4j, 3CX 등 유명 오픈소스 소프트웨어의 치명적인 취약점 발견으로 전세계 대규모 피해 발생. 이러한 오픈소스 소프트웨어를 통한 공급망위험에 대비하기 위해 오픈소스 라이브러리와 구성요소의 목록화, 취약점 관리의 필요성을 인식

- 실증대상

  실제 개발 PC 환경에서 AI 기반 분석 보안 솔루션을 대상으로 하여 소프트웨어의 오픈소스 라이브러리 구성요소와 취약점을 식별

- 실증목적

  SBOM을 통해 각 SW의 구성 요소를 명확히 파악하고, 취약점 정보를 실시간으로 관리 할 수 있어, 향후 보안 위협에 대해 보다 빠르고 효율적으로 대응이 가능. 이를 통해 OSS를 안전하게 관리하고 보안 리스크를 최소화하는 것이 목표

- 기대성과

  AI 솔루션 개발의 높은 오픈소스 활용도에 대비한 사전 취약점 식별 및 사용중인 오픈소스 목록화를 통한 신뢰성 확보

실증 관련 주요 내용 및 결과

- 실증절차

  (1) IoTcube 홈페이지에서 Hmark(해시 인덱스 파일 생성기) 압축파일 다운로드

  (2) 소스코드에 활용된 오픈소스 목록 구조화를 위한 hidx 파일 생성

  (3) 생성된 hidx 파일을 업로드하여 컴포넌트 및 취약점 결과 분석

○ SBOM 도구에 대한 실증 주요 내용 및 결과

NTIA 명시 기능 유형	내용
F1 (빌드에 대한 정보)	패키지이름, 버전정보 나열 / 빌드환경(OS, 컴파일러 버전 등)에 대한 구체적인 정보는 제공되지 않음
F2 (소스 및 바이너리 파일 분석)	소프트웨어에 활용된 패키지 목록과 파일 개수를 나타내며 소스코드, 라이브러리 등 구성요소를 명확히 가시화
F3 (수동입력 및 편집지원)	-
F4 (사람이 읽을 수 있는 형식)	결과가 시각적으로 구조화되어 이해하기 편함
F5 (SBOM간 차이점 파악)	버전별 비교에서 글씨 색을 통해 구분이 가능함, 구별에 용이
F6 (시스템으로 불러오기)	결과가 CyCloneDX 형식으로 제공되어 호환성 보유
F7 (형식 변경)	CyCloneDX 형식에서 SPDX 형식으로 변환 가능
F8 (SBOM간 결합)	명세서 결합 기능을 제공하여 결합 결과를 확인 가능
F9 (도구지원)	-

※ 현재 지원하지 않는 F1과 F9는 상용화 시 지원 예정이며, F3은 지원하지 않음

○ SBOM 명세서에 대한 실증 주요 내용 및 결과

NTIA 최소구성요소	내용
공급자이름 (Supplier Name)	-
구성요소이름 (Component Name)	솔루션 내 컴포넌트 요소를 식별하여 표시
버전 (Version)	웹 UI 상에서 컴포넌트 이름 옆에서 버전을 확인 가능
기타 고유 식별자 (Unique Identifier)	구성요소, 이름 외 기타 고유 식별자를 표시
종속 관계 (Dependency Relationship)	Tree 형태로 가시화를 통해 솔루션, 컴포넌트간 종속관계를 표시
데이터 작성자 (Author of SBOM Data)	SBOM 명세서를 생성한 도구 표시
타임스탬프 (Timestamp)	SBOM 명세서를 생성한 시간 표시

솔루션에 대해 48개의 OSS 의존성을 확인, 대표적인 OSS는 식별되지만 OSS를 동작하기 위한 세부 오픈소스들은 일부 식별이 되지 않은 것으로 파악

※ 원인분석결과 : 식별되지 않은 OSS은 .so파일이였거나 Github star개수가 적은 OSS라 수집되지 않음. 추후 OSS수집 기준 재정립 필요

○ 취약점 분석 주요 내용 및 결과

취약점 분석결과 취약점이 1개 발견되었으나 취약점 식별 조사 결과, 현재 활용중인 패키지 버전은 이미 업데이트가 되어 문제가 해결된 버전임을 확인

○ 결과분석 및 기대성과 달성 여부

(1) 소스코드 취약점 분석결과 취약점을 발견했으나 이미 해결된 취약점임을 교차검증을 통해 확인하여 취약점 분석기능에 대한 목표를 달성

(2) 소스코드의 구성요소를 가시화하고 JSON 포맷으로 획득하여 목표를 달성

(3) 소스코드에서 활용되는 컴포넌트 수가 트리 형태로 정상적으로 가시화되는 것을 확인하여 목표 달성

실증 시 애로사항 및 개선사항

- 결과 별도 다운로드 필요

  웹 UI로 SBOM 명세서 생성시, 웹에서 데이터를 가시화시켜 파일 관리가 불편. 별도 명세서 파일 다운로드 기능의 추가 필요

- SBOM 도구 활용법 숙지의 어려움

  일반 사용자 입장에서 안내 및 매뉴얼의 어려움이 존재. 명확한 가이드 및 Best Practice가 필요

- 경로 입력시 편의성 개선

  초기 Python 기반의 exe파일로 hidx 파일을 생성시 "\"를 기반으로 경로를 입력 시 경로를 인식하지 못하고 "/"로 입력하여야 함. 편의성 개선 필요

실증결과를 통한 취약점 관리 방향

기존에는 패키지관리자 기능으로 얻은 라이브러리 목록을 한국인터넷진흥원의 CVE 통합검색을 통해 명칭 검색과 버전 식별을 하는 방법으로 솔루션 취약점 확인

이번 실증에서는 SBOM 도구를 사용하며 세부 구성요소를 확인하고 hidx 파일을 생성하여 업로드 하는 것으로 취약점 분석을 수행하여 취약점이 해결되어 있다는 점을 확인. 추후 라이브러리 버전 업데이트 및 기능 추가 등 유지보수 시 발생되는 변경점에 대해 실증도구를 활용하여 마이너 버전까지 OSS의 명세와 취약점들을 SW버전·명세버전을 묶어 관리할 계획

SBOM 관련 정책적/기술적 개선사항

- SW공급망보안 컴플라이언스에 대한 가이드라인 제공

  SBOM은 사이버 보안 및 컴플라이언스 강화를 위해 중요성이 대두되는 중으로, 기업마다 SBOM 관리를 자율적으로 수행 시 체계적인 관리가 이루어지지 않을 것으로 예상. SBOM에 대한 정의, 구성요소, 필요성, 우수 사례 등에 대한 명확한 가이드라인 필요. 추가적으로 SBOM 관리 도구 사용법과 자동화 툴에 대한 실질적인 지침 제공 필요

- SBOM 표준 준수와 인증체계 도입

  SBOM 명세서 생성 자동화 도구마다 특성과 생성하는 방식이 상이. 이에 따른 명세서 신뢰성 의문 제기 가능성 존재. SBOM 자동 생성 도구의 표준 준수 여부 검증 및 SBOM 명세서에 대한 인증 체계의 도입 필요

- Python 언어에 대한 라이브러리 식별

  패키지매니저를 통해 관리되는 Python 언어에 대한 일부 라이브러리 미식별 사례 존재

3-2) B사 실증 세부 결과

참여 배경 및 실증대상, 실증목적 및 기대성과

- 참여배경

  미국의 SW SBOM 제출 의무화, 유럽의 CRA 발의 등 국제적 트렌드에 발맞추어 한국도 SBOM 관련 정책의 도입/시행을 검토 중. B사는 자사 솔루션의 글로벌 공급 및 향후 국내 SBOM 컴플라이언스 시행에 대비하여 자체적인 내부 검토를 위해 실증 수요기업으로 참여

- 실증대상

  다양한 언어로 구성된 솔루션에서 현재 SBOM 도구가 지원하는 언어인 C++, Python으로 구성된 일부 서브모듈을 통해 실증 수행

- 실증목적

  B사 보유 S/W의 OSS 식별 관리체계를 준비하여 소프트웨어 구성요소를 투명하게 관리 및 취약점을 보완하여 글로벌 규제와 국내 컴플라이언스 발효에 대비, 산업계 입장으로서의 정책 제정에 대한 의견 제시가 목표

- 기대성과

  B사 보유 S/W의 투명성과 보안성을 향상. 취약점 발견 과정 및 대응 시간 단축을 통한 S/W 관리 업무 효율성 개선

실증 관련 주요 내용 및 결과

- 실증절차

  (1) IoTcube 홈페이지에서 Hmark(해시 인덱스 파일 생성기) 압축파일 다운로드

  (2) 자사 솔루션 패키지 중 HatBOM 분석이 가능한 C++/Python 언어기반의 서브 모듈 준비

  (3) SBOM 툴을 이용하여 프로젝트 별로 빌드를 위한 hidx 파일 생성 및 분석

○ SBOM 도구에 대한 실증 주요 내용 및 결과

NTIA 명시 기능 유형	내용
F1 (빌드에 대한 정보)	패키지이름, 버전정보 나열 / 빌드환경(OS, 컴파일러 버전 등)에 대한 구체적인 정보는 제공되지 않음
F2 (소스 및 바이너리 파일 분석)	소스코드 수준의 분석이 가능하며, File, Function, Line의 개수, 생성완료시간, 소요시간, 취약성 비율 등의 정보를 표현
F3 (수동입력 및 편집지원)	-
F4 (사람이 읽을 수 있는 형식)	소스 Tree 형태로 표시, 분석내용을 표로 요약하여 가독성이 좋음
F5 (SBOM간 차이점 파악)	두 개 이상의 SBOM 분석이 가능, 차이점을 시각화된 트리, OSS, 종속성 비교를 통해 보여줌
F6 (시스템으로 불러오기)	JSON 파일을 불러오기 가능
F7 (형식 변경)	SBOM JSON파일을 입력시 CycloneDX 및 SPDX 형식으로 변환 지원
F8 (SBOM간 결합)	SBOM 파일의 데이터 소스를 병합하여 하나의 결과로 보여줌
F9 (도구지원)	-

※ 현재 지원하지 않는 F1과 F9는 상용화 시 지원 예정이며, F3은 지원하지 않음

○ SBOM 명세서에 대한 실증 주요 내용 및 결과

NTIA 최소구성요소	내용
공급자이름 (Supplier Name)	-
구성요소이름 (Component Name)	서브모듈 내 컴포넌트 요소를 식별하여 표시
버전 (Version)	웹 UI 상에서 컴포넌트 이름 옆에서 버전을 확인 가능
기타 고유 식별자 (Unique Identifier)	구성요소, 이름 외 기타 고유 식별자를 표시
종속 관계 (Dependency Relationship)	Tree 형태로 가시화를 통해 서브모듈, 컴포넌트간 종속관계를 표시
데이터 작성자 (Author of SBOM Data)	SBOM 명세서를 생성한 도구 표시
타임스탬프 (Timestamp)	SBOM 명세서를 생성한 시간 표시

(1) C++언어로 된 서브모듈에서 2개의 OSS 의존성을 발견하여 트리생성·가시화

(2) Python언어로 된 서브모듈에서 6개의 OSS 의존성을 발견하여 트리생성·가시화

(3) Python언어로 된 서브모듈에서 1개의 OSS 의존성을 발견하여 트리생성·가시화

○ 취약점 분석 주요 내용 및 결과

(1) C++언어로 된 서브모듈에서 2가지유형, 5개 CVE 취약성 코드 발견

(2) Python언어로 된 서브모듈에서 3가지유형, 6개 CVE 취약성 코드 발견

(3) Python언어로 된 서브모듈에서 0개 CVE 취약성 코드 발견

- 결과분석 및 기대성과 달성 여부

  (1) 해시코드를 이용한 SBOM 관리방안에 대한 가능성 확인 및 소스코드 노출 없는 제3자에 의한 SBOM 관리 방안을 확인할 수 있었음

  (2) 소스코드 수준에서 패키지내부 OSS를 식별, CVE 식별자와 관련 Reference 제시를 통해 취약점에 대한 정보를 제공

실증 시 애로사항 및 개선사항

- 도구의 제한적인 언어지원

  SBOM 생성도구 및 취약점 분석도구는 현재 개발 및 업데이트 중으로, 지원 언어의 한계 존재. 실증을 위해 솔루션 중 C++, Python 언어로 구성된 일부 서브모듈만 사용하여 실제 사용중인 솔루션의 전체는 검증 불가. 지원언어의 확대 필요

- SBOM 도구 활용법 숙지의 어려움

  도구를 처음 사용해보는 입장에서 활용의 어려움 존재. hmark 압축파일 다운로드 및 사용이나 hidx 생성 시 라이브러리 포함범위 등을 이해하기 어려워 사용법 숙지에 많은 시간이 소요

실증결과를 통한 취약점 관리 방향

- SBOM 컴포넌트 관리 방안

  기존 별다른 OSS 관리를 진행하고 있지 않았으나, 실증 이후 C, C++ 등의 언어를 포함한 구성관리 식별을 일반화하여 관리

- 취약점 점검방법

  기존에는 시험기관에 취약점 점검 의뢰 및 도구를 임대하는 방식 사용. 또는 정부지원 사업에서 취약점 점검을 진행. 이번 SBOM 도구를 통해 취약점 리스트와 관련 Reference를 참고하여 패치를 진행할 예정

SBOM 관련 정책적/기술적 개선사항

- 규제 측면의 운영 회피

  현재도 정부·공공기관에 제품/서비스를 공급하기 위해서는 GS인증, 조달물품등록과 같은 규제가 존재, 여기에 SBOM 추가 시 중소기업의 부담 가중 우려. Compliance 지정 시 기업입장에서 생기는 비용적, 절차적 부담에 대한 고려 필요. SW 품질 식별성을 향상시키는 본연의 목적을 잘 살리는 동시에 부담을 최소화할 수 있는 절차 수립을 초기 제도적 정착 시기에 마련 필요

- SBOM 시행 목적 달성

  시행적인 측면에서의 효율성만 강조 시 SBOM 정책 시행 목적 달성의 어려움 존재. 기업의 보안성 강조로 인해 SW 컴포넌트 점검이 제대로 작동하지 못하는 SBOM 제도는 기술적으로 불완전한 제도가 될 것. 기술적인 완전성과 시행적인 효율성 측면을 모두 고려할 수 있는 절차와 제도 마련 필요

3-3) C사 실증 세부 결과

참여 배경 및 실증대상, 실증목적 및 기대성과

- 참여배경

  현재 단일 회사에서 소프트웨어를 모두 개발하여 공급하는 경우는 거의 없으며, 여러 오픈소스나 API 호출을 통해 제작되는 형태가 다수. 이러한 환경에서 개발자는 소프트웨어에 어떤 패키지나 라이브러리가 포함되어 있는지 정확히 알기 어려우며 신속한 대응이 힘듦. 또한 대부분 솔루션 도입 업체에서 SBOM을 요구하고 있어 자사 솔루션의 안정성 및 신뢰성 확보의 필요성 인식

- 실증대상

  자사 내 데이터 통합/수집 관리 솔루션과 보안 솔루션 대상, 분석에 필요한 소스 코드를 분류하여 실증을 진행

- 실증목적 및 기대성과

  현재 사용 중인 오픈소스들의 취약점을 개선을 통한, 보다 안정적인 S/W 경쟁력 확보가 목표

실증 관련 주요 내용 및 결과

- 실증절차

  (1) IoTcube 홈페이지에서 Hmark(해시 인덱스 파일 생성기) 압축파일 다운로드

  (2) 소스 리포지토리에서 최신 소스 다운로드, 소스코드를 제외한 빌드 결과물, 라이브러리 파일, 실행 바이너리 파일 등 삭제 후 라이브러리 및 모듈별 정리

  (3) SBOM 툴을 이용하여 프로젝트 별로 빌드를 위한 hidx 파일 생성 및 분석

SBOM 도구에 대한 실증 주요 내용 및 결과

NTIA 명시 기능 유형	내용
F1 (빌드에 대한 정보)	패키지이름, 버전정보 나열/빌드환경(OS, 컴파일러 버전 등)에 대한 구체적인 정보는 제공되지 않음
F2 (소스 및 바이너리 파일 분석)	소프트웨어에 활용된 패키지 목록과 파일 개수를 나타내며 소스 코드, 라이브러리 등 구성요소를 명확히 가시화
F3 (수동입력 및 편집지원)	-
F4 (사람이 읽을 수 있는 형식)	타 상용 도구 대비 가시성 우수, 실제로 많은 도움이 되는 부분
F5 (SBOM간 차이점 파악)	Diff 기능은 확인하지 못하였음
F6 (시스템으로 불러오기)	JSON 파일을 쉽게 시스템으로 불러오기 및 등록이 가능
F7 (형식 변경)	형식변환이 용이하고 타 상용 도구 대비 우수한 기능으로 보여짐
F8 (SBOM간 결합)	명세서 결합 기능을 제공하여 결합 결과를 확인 가능
F9 (도구지원)	-

※ 현재 지원하지 않는 F1과 F9는 상용화 시 지원 예정이며, F3은 지원하지 않음

- SBOM 명세서에 대한 실증 주요 내용 및 결과

NTIA 최소구성요소	내용
공급자이름 (Supplier Name)	-
구성요소이름 (Component Name)	솔루션 내 컴포넌트 요소를 식별하여 표시
버전 (Version)	웹 UI 상에서 컴포넌트 이름 옆에서 버전을 확인 가능
기타 고유 식별자 (Unique Identifier)	구성요소, 이름 외 기타 고유 식별자를 표시
종속 관계 (Dependency Relationship)	Tree 형태로 가시화를 통해 솔루션, 컴포넌트간 종속관계를 표시
데이터 작성자 (Author of SBOM Data)	SBOM 명세서를 생성한 도구 표시
타임스탬프 (Timestamp)	SBOM 명세서를 생성한 시간 표시

Python언어로 된 솔루션에서 7개의 OSS 의존성을 발견하여 트리생성·가시화

※ 일부 SBOM 생성 실패 솔루션도 있었으나 .NET, C#등 현재 미지원 언어를 포함한 솔루션이거나 재사용이 많아 OSS 탐지가 어렵거나 솔루션 크기, 복잡도가 높아 타 상용 도구에서도 미검출 되는 상황임을 확인

- 취약점 분석 주요 내용 및 결과

취약점 분석결과 CVE 취약점 코드는 0개로 분석

- 결과분석 및 기대성과 달성 여부

솔루션의 컴포넌트, 컴포넌트의 버전, 종속관계 등을 가시화하여 확인할 수 있었으며 오픈소스 List 정리를 성공적으로 진행. 취약점탐지 개선은 필요한 것으로 사료

실증 시 애로사항 및 개선사항

- 도구의 제한적인 언어지원

현재 SBOM에 대해 실증을 해보고자 하는 제품은 주 언어가 C#, .NET으로 구성. 다른 솔루션들 또한 RUST, GO 등의 언어로 개발이 진행되어 있어 검증이 어려운 상황. 이에 대해 R&D 연구 개발 단계이고 차후 업데이트 계획이 있다는 개발측의 답변 회신. 산업계에서 주로 쓰이는 언어 업데이트를 통한 사용 수요 확대 필요

- 재사용된 소스코드에 대한 탐지 개선

소스코드에 수정이 가해져, 재사용된 OSS 구성요소가 없다고 판단될 경우 #files, dependencies 결과가 0으로 출력되는 경우가 발생. 실제 개발 과정에서 OSS 자체를 통째로 활용하여 수정 없이 사용되는 경우는 소수이므로 수정 및 활용에 대한 탐지 개선 필요

- 매뉴얼 및 활용 예제의 다양화

매뉴얼의 기능소개와 사용법에 대한 안내가 잘 이루어져있으나 특정 파일이 없거나 변환이 안되는 등의 오류 사항에 대해서는 사용자 자체 해결의 어려움 존재. 자주 발생할 수 있는 돌발상황에 대한 FAQ 및 다양한 활용 예제 추가 필요

실증결과를 통한 취약점 관리 방향

- 오픈소스 구성확인 및 업데이트

  오픈소스 컴포넌트 SBOM 생성 및 취약점 탐지 기능을 통해 솔루션에서 사용중인 오픈소스들을 list-up하여 정리. list를 가지고 알려진 취약점 목록과 비교, 대조하여 해당 사항이 있는 소스들을 대상으로 최신버전 업데이트를 진행

SBOM 관련 정책적/기술적 개선사항

- SBOM 담당 기관을 통한 신뢰성 확보

  SBOM을 통해 사용되는 솔루션이나 플랫폼에 대한 안전한 S/W 수요 증가. 이를 위한 SBOM 신뢰도 평가 기관은 현재 미비한 상태. SBOM 결과에 대한 신뢰도 평가 기관 지정 및 확인서 발급을 통한 대외적 신뢰성 제고 필요

- SBOM 전문성 강화를 위한 지원

  SBOM의 수요 증가와 해외 주요국의 Compliance 지정 흐름에 국내 SBOM 생성·관리도구의 속도는 따라오지 못하고 있는 상황. 중소·중견기업의 자체 SBOM 구축은 매우 어려운 문제로 도구의 발전 및 신뢰도는 중요한 문제. 내부 인력의 전문성 강화를 위한 별도 프로그램이나 지원 계획에 대한 구체적인 방안이 필요

4) 요약 및 시사점

구 분	A사	B사	C사
SBOM 도구 실증	- Analyze, Translate, Merge, Diff 등의 NTIA에서 명시하는 기능 유형의 대부분을 정상적으로 잘 수행하고 있으며 지원하지 않는 기능에 대해서도 차후 지원 예정임을 확인		
SBOM 명세서 실증	- 구성요소 이름, 버전, 종속성 등의 NTIA 명시 최소구성요소를 대부분 잘 나타내고 있음 - 솔루션에 대해 48개의 OSS를 확인하고 트리생성·가시화	- 서브모듈에서 각 2개, 6개, 1개의 OSS를 확인하고 트리생성·가시화	- 하나의 솔루션에서 7개의 OSS를 확인하고 트리생성·가시화
취약점 분석 실증	- 1개의 CVE 취약성 코드를 발견하였으나, 활용중인 패키지 버전은 이미 업데이트되어 해결된 버전임을 확인 - 취약점 분석 도구 외에도 추가적으로 개발자의 확인 필요	- C++ 서브모듈에서 2가지 유형, 5개의 CVE 취약성 코드 발견 - Python 서브모듈에서 3가지 유형, 6개의 CVE 취약성 코드 발견 - Python 서브모듈에서 0개의 CVE 취약성 코드 발견	- CVE 취약성 코드는 검출되지 않음
정책적 개선사항	- 체계적인 SBOM의 관리를 위한 SBOM 정의, 필요성, 우수사례 등에 대한 명확한 가이드라인 필요 - SBOM의 신뢰성을 위한 SBOM 자동생성 도구의 표준 준수 검증 및 명세서 인증체계 도입	- SW 품질 식별성을 향상시키는 본연의 목적을 잘 살리고 기업의 부담을 최소화할 수 있는 절차 수립 - SBOM 정책의 기술적인 완전성과 시행적인 효율성 측면에서 모두 만족할 수 있는 제도 마련	- SBOM 담당기관의 지정과 평가기관, 확인서 등을 통한 SBOM의 대외적 신뢰도 확보 - SBOM 컴플라이언스 확대로 필수가 될 가능성이 높아보이나 중소기업에겐 어려운 과제, 내부 인력 교육이나 지원 계획에 대한 방안이 필요
기술적 개선사항	- 웹 UI 명세서 조회 외 별도 명세서 파일 다운로드 기능 지원	- 지원 언어의 확대 필요 - 바이너리 및 동적링킹 소스에 대한 분석 기능 추가	- 지원 언어의 확대 필요 - 재사용 OSS에 대한 탐지기능 개선 - 기술적 오류, 문제에 대한 FAQ 및 사용 가이드 필요
도구 개선 및 보완	<실증 내용> - (Python 가상환경) Python 가상환경에서 사용되는 OSS 미탐지 - (재사용 OSS) 수정을 거친 OSS 미탐지 - (다른이름으로 저장) 새창에서 JSON 형태로 파일을 생성하여 별도 저장이 불편 - (Supplier Name) Supplier Name 누락 - (Build & Tool Support) 도구 기능 유형 중 Build, Tool Support는 부분 탑재 - (언어 확장 지원) 추가 언어지원 필요 - (생성기 명칭) SBOM 생성을 위한 해시생성기와 취약점 탐지를 위한 해시생성기의 이름이 동일하여 혼동	<조치 및 보완> - (Python 가상환경) 가상환경에서 사용되는 OSS들을 해시화하여 입력하도록 가이드 - (재사용 OSS) Threshold값 조정을 통한 탐지율 향상 - (다른이름으로 저장) 차기년도 검토 예정 - (Supplier Name) Required Field가 아니지만 차기년도 외부 의존성 추가 시 반영 검토 - (Build & Tool Support) 해당되는 API 구현 및 공개를 검토 - (언어 확장 지원) 차기년도 언어확장 예정 - (생성기 명칭) 명칭변경 또는 통합생성기 검토	

[표 8] **SBOM 실증 조사 결과 요약 및 보완 조치**

구 분	실증결과에 대한 평가
총평 및 시사점	- R&D 연구개발된 SBOM 생성도구를 통해 솔루션의 SBOM을 생성하여 그 **도구와 명세서가 NTIA 기준에 맞게 정상적으로 작동하고 대부분의 컴포넌트 및 취약점에 대한 성공적 검출을 확인** - 일부 미탐 라이브러리 및 컴포넌트, 취약점에 대해서는 **기능향상을 위한 기술적 지원 필요** - 공통적으로 **SBOM에 대한 가이드 및 지침 필요, 지원언어 확대** 등을 개선방안으로 제안 - SBOM의 신뢰성 향상을 위한 표준 준수, 담당기관 지정, 중소기업 교육 등 **SBOM 신뢰성 확보와 역량강화를 위한 정책 지원 필요**
Lesson Learned	- 미국, 유럽 등 SBOM 컴플라이언스 시행에 따른 국제 SW 무역규제 대비에 막연한 불안감이 있었으나 이번 실증사업 참가를 통해 자체 내부 검토 필요성을 인식하는 계기가 됨 - 기업에서 보유한 SW OSS 구성요소에 대해 투명하게 관리할 수 있는 관리체계(담당부서)의 필요성 인식 - SW공급망 공격에 대한 대비를 위해 사용중인 OSS라이브러리와 구성요소를 목록화하고 취약점을 체계적으로 관리해야하는 필요성을 인식 - 식별된 OSS의 보안 취약점을 사전에 탐지하여 예방할 수 있는 조치를 검토하게 된 계기가 됨 - 실증사업 참여를 통해 자체적으로 사용중인 OSS를 목록화하고 업데이트를 수행하는 계기가 됨 - SBOM 도구를 통한 OSS 확인과 취약점 개선을 통한 안정적 SW경쟁력 확보방안의 가능성을 확인

[표 9] 실증 결과에 대한 평가

5.
참 고

Chapter 5

참 고

참고 문헌

- SPRi 김향규 연구원(2022), "미국 SBOM(Software Bill of Materials) 정책 분석 및 시사점", SPRi 이슈 리포트 IS-144
- SPRi 김향규 연구원(2022), "주요국 SBOM(Software Bill of Materials) 정책 분석", SPRi 이슈 리포트 IS-150
- SPRi 김향규, 박태형 연구원(2023) "SW명세서(SBOM) 도입 및 활성화 방안 연구" SPRi 연구보고서 RE-137
- ETRI 류원옥, 박수명, 이승윤 연구원(2023) "SW공급망 관리 및 SBOM 동향"
- Scribe Security "SBOM 표준 형식"
- 과학기술정보통신부, 국가정보원, 디지털플랫폼정부위원회 (2024), "SW 공급망 보안 가이드라인 v1.0"

출 처

1) Gartner(2024.6.), "Leader's Guide to Software Supply Chain Security"
2) Snyk, Cybersecurity Ventures(2023), "2023 Software Supply Chain Attack Report"
3) Federal Reguster(2021), "Executive Order 14028, Improving the nation's Cybersecurity"
4) CISA(2024.3.), "Secure Software Development Attestation Form Instructions"
5) European Union(2022.12), "Directive (EU) 2022/2555 of the European Parliament and of the Council"
6) European Parliament(2022.9.), "Regulation of the European Parliament and of the council : on horizontal cybersecurity requirements for products with digital elements and amending Regulation(EU) 2019/1020"
7) Trublo.eu "https://www.trublo.eu/d-sbom/"
8) 총무성(総務省, 2022) "ICT サイバーセキュリティ総合対策 2022"
9) 경제산업성(経済産業省, 2023.7.), "ソフトウェア管理に向けた SBOM の導入に関する手引 Ver. 1.0"

10) NISC (サイバーセキュリティ戦略本部, 2024.7.), "サイバーセキュリティ 2024"

11) 과학기술정보통신부 보도자료(2024.08.) "과기정통부, 선도형 연구개발 체제 전환을 통한 미래도약 가속화"

12) 과학기술정보통신부 보도자료(2024.09.) "국가 소프트웨어 공급망 보안정책 마련을 위한 전담반 가동"

13) 지디넷코리아, "래브라도랩스, SW공급망 자동관리플랫폼 '래브라도SCM' 출시 " https://zdnet.co.kr/view/?no=20240819143642

14) IT Daily, "오픈소스 취약점 노린 SW공급망 보안 위협, 'SBOM'이 해결사 될까" http://www.itdaily.kr/news/articleView.html?idxno=212417

15) The Linux Foundation Projects "About SPDX"

16) OWASP "CycloneDX One Pager"

17) NTIA SBOM Formats & Tooling Working Group(2021.03.) "SBOM Tool Classification Taxonomy"

18) NTIA, Department of Commerce(2021.07.) "The Minimum Elements For a Software Bill of Materials"