정 보 보 호 학 회 지
제 32 권 제5호, 2022. 10

소프트웨어 공급망 보안 관리를 위한 기술 동향 조사와 향후 발전 방향 제언

강 우 성*, 방 혁 준**

요 약

디지털 트랜스포메이션(Digital Transformation)으로 인해 소프트웨어에 대한 의존성이 강화되면서 소프트웨어 공급망의 역할이 커지고 있다. 그러나 안전한 소프트웨어 개발 및 이용을 위한 소프트웨어 공급망 보안 관리는 사실상 어려운 실정이다. 공급망이 복잡해질수록 공급망 공격의 유형은 다각화되는 반면 공급망을 구성하는 공급업체 및 구성요소에 대한 식별 및 취약점 분석은 어려워지기 때문이다. 이에 저자는 국내외 소프트웨어 공급망 보안 관리를 위한 기술 동향에 대한 조사 분석을 수행하고 이를 기반으로 향후 적용할 수 있는 공급망 보안 관리 체계의 발전 방향에 대해 작성하였다.

Ⅰ. 서 론

다양한 산업분야의 융합으로 소프트웨어가 고도화되면서 복잡한 기술이 요구되는 제품은 더 이상 하나의 단일 업체의 기술력만으로 제품을 개발하고 출시할 수 없게 되었다. 이에 따라 다양한 공급업체로부터 각종 소프트웨어 및 구성요소를 공급받아 완성된 제품을 개발 및 출시하는 소프트웨어 공급망(Software Supply Chain)이 형성되고 있으며, 각종 산업 분야의 기술력이 발전하면서 소프트웨어 공급망 역시 거대해지고 있다. 특히 최근 각종 산업 분야가 맞고 있는 디지털 전환의 국면인 '디지털 트랜스포메이션(Digital Transformation)'으로 인해 더욱 확장되고 있는 추세이다.

이러한 소프트웨어 공급망은 공급망을 구성하는 공급업체의 수 자체가 많고, 각 공급업체가 복잡하게 연결되어 있기 때문에 사이버보안 상태를 점검하고 해결하는 것이 쉽지 않아 사이버 공격에 노출될 수 있는 보안 허점의 범위가 넓다. 이에 따라 상대적으로 공격자들이 공급망의 내부 시스템으로 침투하는 것이 용이하고, 특정 공급업체에 대한 공격으로 해당 공급업체와 공급망으로 연결되어 있는 다수의 업체에 연쇄적으로 피해를 입힐 수 있기 때문에 '공급망 공격(Supply Chain Attack)'이 증가하고 있는 추세이다.

대표적인 공급망 공격 사례로는 2020년12월 발생한 솔라윈즈(SolarWinds) 사태를 꼽을 수 있다. 솔라윈즈 사태는 최악의 해킹 사고로 평가되고 있으며, 이로인해 미국의 9개 연방 기관, 100여개의 민간 기업이 피해를 입은 것으로 파악되었으며 1만 8,000개 이상의 기업이 악성 프로그램을 다운로드 받은것으로 확인되어 추가적인 피해규모를 예측할 수 없는 상황이다.

이처럼 공급망 보안을 제대로 관리하지 못할 경우 기하급수적인 연쇄 피해가 발생할 수 있어 사전에 차단하는 것이 중요하지만 소프트웨어 공급망을 형성하는 각 공급업체들은 자사가 개발한 소프트웨어 또는 구성 요소를 외부의 업체에 제공할 때 소스코드를 공개하지 않기 때문에 보안 취약점 분석에 어려움이 있다. 또한 소프트웨어 공급망을 구성하는 공급업체들의 보안 상태를 일률적으로 점검하고 관리하는 것이 쉽지 않기 때문에 체계적인 보안 관리가 어려운 문제점이 있다.

이에 저자는 현재까지의 공급망 보안 관리 기술에 대한 국내외 동향을 조사하고 이를 토대로 추가적인 발전을 위해 필요한 체계적인 공급망 보안 관리 방안을 살펴보기로 한다.

* 쿤텍㈜ 임베디드보안개발팀 (수석연구원, wilson@coontec.com)
** 쿤텍㈜ (대표이사, joon@coontec.com)

Ⅱ. 공급망 보안 관리 현황

2.1. 공급망 공격 발생 동향

공급망 공격으로 인한 피해 사례는 지속적으로 보고되고 있다. 앞서 언급한 솔라윈즈 사건 외에도 대만의 컴퓨터 제조사인 에이수스(ASUS)에 대한 악성코드 유포로 인한 업데이트 서버 공격 사건, 코스트코(Costco), 월마트(Walmart), 테스코(Tesco) 등이 연쇄적으로 피해를 입은 PNI 디지털 미디어 사건 등이 대표적인 공급망 공격 사례 중 하나이다. PNI 디지털 미디어 사건은 사진 인화 서비스를 제공하는 플랫폼인 PNI 디지털 미디어가 악의적인 사이버 공격을 받게 되면서 해당 공급망을 형성하고 있던 업체들이 연쇄적으로 피해를 입게 된 사건이다.

공급망 공격은 기존의 사이버 공격과는 공격의 패턴이나 유형이 다른 것이 특징이다. 예를 들어 공급망 공격의 경우 소프트웨어 공급업체의 네트워크에 침투하여 악성코드를 삽입하거나 액세스를 제어할 수 있는 권한을 부여하는 방식, 부적절한 계정 접속 권한을 부여할 수 있는 코드 서명을 삽입하는 방식 등으로 공격을 수행하고 있으며, 최근 도입이 급증하고 있는 오픈소스 소프트웨어의 라이브러리에 악성코드를 삽입하는 방식의 공격 유형도 증가하고 있는 추세이다.

이처럼 소프트웨어 공급망을 형성하고 있는 특정 공급업체를 겨냥하는 방식의 공격 또는 불특정 다수가 사용하는 오픈소스 라이브러리에 악성코드를 삽입하는 방식의 공격 등은 비교적 적은 리소스를 사용해 대규모의 연쇄적인 피해를 유발할 수 있기 때문에 공격자 입장에서는 효율적인 공격이라고 할 수 있다.

2.2. 공급망 보안 관리 동향

이처럼 피해의 규모를 예측하는 것이 어려운 공급망 보안을 효율적으로 관리하기 위해서는 공급망을 형성하고 있는 공급업체와 구성 요소에 대한 식별 및 분석이 선행되어야 한다. 과거에는 공급망의 규모가 크지 않았고 공급망에 대한 조직의 의존도가 낮았기 때문에 공급망 보안 관리 자체에 대한 어려움이 없었지만, 공급망이 지속적으로 확대되고 각 조직의 공급망 의존도가 높아지고 있는 현재 시점에서는 기존의 방식이 아닌 새로운 방식으로 공급망 보안을 관리해야 한다.

이러한 추세에 따라 최근 자동화 기반의 공급망 관리 플랫폼이 시장에 출시되고 있으며, SBOM(Software Bill of Materials)을 기반으로 공급망의 구성요소를 관리할 수 있는 대응 방안 수립이 가속화되고 있다.

Ⅲ. 공급망 보안 관리의 어려움

공급망 공격은 소규모 공격으로 기하급수적이고 연쇄적인 피해를 유발할 수 있기 때문에 사전 보안 관리를 통해 공격을 차단하는 것이 중요하다. 그러나 기존의 전통적인 방식으로 공급망 보안을 관리하는 것에는 몇 가지 어려움이 있다.

3.1. 공급망 구성 요소 식별

공급망을 형성하고 있는 구성요소는 물리적인 수가 많고 각 구성요소 사이의 관계가 복잡하기 때문에 일회성에 그친 분석만으로는 식별 및 파악이 쉽지 않다. 특히 공급망에는 상용 소프트웨어 구성요소만 포함되어 있는 것이 아니고 바이너리, 지적재산권, 내장형 소프트웨어 및 오픈소스 소프트웨어 등 다양한 구성 요소들이 유기적으로 연결되어 있기 때문에 각 구성요소의 특성을 기반으로 가시성을 확보하는 것이 중요하다. 또한 각 구성요소가 포함되어 있는 소프트웨어 사이의 에코시스템도 공급망 구성요소 식별에 있어서 중요한 분석 요소 중 하나이지만 이러한 에코시스템의 경우 글로벌 에코시스템을 형성하고 있기 때문에 수동으로는 가시성을 확보하는 것이 불가능하다.

3.2. 취약점 관리

가시성 확보를 기반으로 공급망을 구성하는 구성요소에 대한 식별이 완료되었다고 하더라도 전문 플랫폼을 사용하지 않을 경우 각 구성요소에 내재되어 있는 취약점을 탐지하는 것이 쉽지 않다.

소프트웨어 공급망을 대상으로 수행되는 공급망 공격은 악성코드 배포를 통한 공격 외에도 업데이트 서버, CI/CD 도구 취약점 공격, 접근제어 우회 등 다양한 경로를 통해 수행될 수 있기 때문에 철저한 사전 보안 관리가 중요하다. 그러나 사실상 수동으로 모든 보안 취약점을 사전에 탐지하고 각 취약점에 대한 완화 방안을 마련하는 것은 불가능하기 때문에 신속한

취약점 탐지부터 우선순위에 근거한 취약점 완화방안 제시까지 하나의 사이클로 제공할 수 있는 전문 취약점 관리 플랫폼을 통해 지속적으로 취약점을 관리하는 것이 필요하다.

Ⅳ. 국내 공급망 보안 관리 연구 동향

최근 공급망 침투 방식은 소프트웨어의 내용 및 로직을 악의적으로 변경하거나 펌웨어를 변경하는 공격 유형으로 구분할 수 있다. 이에 대응하기 위하여 FW (Firm ware) 및 SW(Soft Ware) 위협 대응 연구가 활발히 이루어지고 있다.

4.1. FW 공급망 위협 대응 연구

하드웨어 공급망 공격은 시스템의 펌웨어를 대상으로 악성코드 등을 삽입하는 행위 위주로 이루어지고 있다. 이러한 공격에 대응하기 위하여 펌웨어에 숨겨진 의도적 보안 취약점을 분석/검증하는 기술이 개발되고 있다. 공급망 보안을 위해서, 5G 네트워크 장비 등의 펌웨어에 숨겨진 의도적 보안 취약점을 분석하고, 플랫폼 별로 펌웨어 언팩/리팩 및 동적 분석환경을 구축하여 펌웨어 수준의 보안 취약점을 자동 분석하고, 자동 분석된 결과를 이용하여 SBOM(Software Bill of Materials)을 생성하며, CVE 취약점을 분석 및 모니터링 할 수 있는 시스템을 개발하고 있다.

4.2. SW 공급망 보안을 위한 연구

Trustwave 2020에 따르면, 최근 소프트웨어 제조/유통 과정에서 Backdoor 및 Trojan 등을 삽입/변경하는 등의 보안 사고가 증가하고 있다. 이러한 사고를 방지하기 위하여 소스코드 기반의 SBOM을 자동 생성하고, 바이너리 기반의 소프트웨어 구성요소 및 오픈소스 자동식별 기술이 개발되고 있다. 자동 생성된 SBOM을 이용하여 SW 패키지의 유효성 검증 및 암호 기술 등 다양한 무결성 보장 기술로 SW 공급망의 신뢰성을 확보하고, CVE 등 SW 취약점에 대해서 DB와 연동하여 소스코드 및 바이너리 취약점 탐지 기술이 개발되고 있다. 향후 SBOM에 대한 무결성 검증 및 안전성 확보를 위하여 블록체인 형태로 SBOM을 공급한다면 보다 안전한 공급망을 확보할 수 있을 것으로 전망하고 있다.

Ⅴ. 글로벌 공급망 보안 관리 동향

공급망 공격으로 인한 피해 사례가 연이어 보고되면서 미국의 바이든 정부는 사이버보안 강화를 위한 행정명령을 발표하게 되었다. 또한 CISA는 공급망 보안 관리와 관련된 지침을 발표하며, NIST 사이버 공급망 위험 관리(C-SCRM)[1] 문서를 사용해 인프라에서 특정 소프트웨어 사용에 따르는 위험을 파악할 것을 권장하고 있다. NIST가 제시하는 방법은 다음과 같다.

1) C-SCRM을 조직 전반에 통합
2) 공식적인 C-SCRM 프로그램을 마련
3) 핵심 구성요소 및 공급업체를 파악해 관리
4) 취약점이 발견된 기업의 공급망 소프트웨어 파악
5) 주요 공급업체와 긴밀히 협력
6) 탄력성, 개선 활동에 주요 공급업체를 포함
7) 공급망 관계 전반에서 평가와 모니터링 실시
8) 전체 라이프사이클을 계획

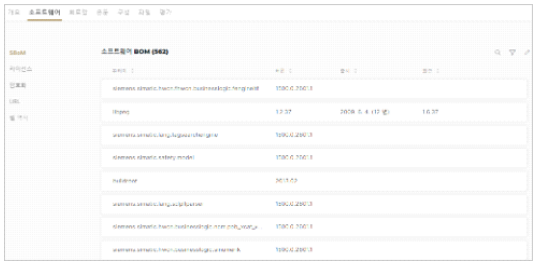
이러한 국제적인 요구 사항을 충족하고 공급망 보안 관리를 효과적으로 수행하기 위해서는 공급망 보안 위협의 유형을 정의하고 각 위협 유형에 체계적으로 적용할 수 있는 대응 방안을 확립해야 한다.

5.1. SW 바이너리 공급망 보안 관리

바이든 정부의 행정명령에는 사이버보안 사고에 대한 대응절차 표준화 지침 수립, 소프트웨어 공급망 보안 향상 및 소프트웨어 보안 강화를 위한 상세한 요구사항이 포함되어 있으며, 특히 SBOM에 대한 생성 및 관리 체계 구축이 필수적인 요소로 명시되었다.

소프트웨어 구성 요소에 대한 일종의 목록을 제공하는 SBOM은 소프트웨어를 개발, 구입, 운영하는 사람들이 공급망 관계를 추적하고 필요한 정보를 확인할 수 있도록 인벤토리를 제공하는 역할을 한다.

그러나 공급망 보안 관리에 있어서 타사가 개발 및 제공한 소프트웨어의 소스코드를 확보하는 것은 불가능하기 때문에 SBOM에 대한 생성 관리를 수행하기 위해서는 바이너리 기반 분석이 필수적으로 진행되어야 한다.



〔그림 1〕 Cybellum의 SBOM 분석 화면

상용 멀티플랫폼 바이너리 분석 도구인 사이벨리움(Cybellum)은 소스코드에 접근하기 어려운 환경에서도 바이너리 분석을 통해 SBOM을 신속하고 정확하게 생성할 수 있으며, 이를 기반으로 공급망을 구성하는 소프트웨어 구성 요소에 대한 완전한 가시성을 확보하고 나아가 자동화 플랫폼 기반의 취약점 관리 기능을 제공하여 보안 위협 상황에 빠르게 대응할 수 있도록 지원한다.

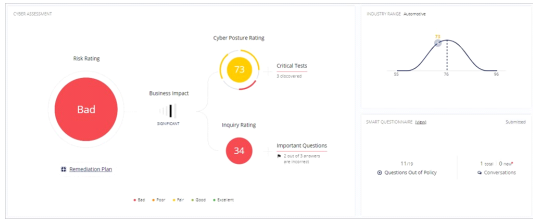
5.2. 오픈소스 공급망 보안 관리

최근 소프트웨어 개발에 있어서 오픈소스 소프트웨어가 차지하는 비중이 급진적으로 증가하고 있다. 오픈소스 소프트웨어를 사용할 경우 기존에 개발되어 있는 요소를 일부 차용할 수 있기 때문에 개발 비용 및 시간을 줄일 수 있으면서도 오픈소스 커뮤니티에서 검증된 오픈소스 컴포넌트를 활용할 수 있어 기능적인 측면에서도 품질을 보증할 수 있다. 그러나 오픈소스 소프트웨어의 경우 소스코드가 공개되어 있기 때문에 사이버보안 공격에 노출될 가능성이 상대적으로 크다는 문제점이 있다.

이러한 문제점을 보완하기 위해서는 오픈소스 라이브러리에 사용된 구성 요소를 빠르고 정확하게 식별하고, 각 구성 요소에 내재되어 있는 취약점을 탐지하여 적절한 완화 조치를 취하는 것이 중요하다.

5.3. 공급망 어택서피스(Attack Surface) 관리

공급망 보안 관리가 까다로운 이유 중 하나는 사이버보안 위협에 노출될 수 있는 공격표면인 '어택서피스(Attack Surface)'의 범위가 넓기 때문이다. 공급망을 형성하고 있는 공급업체와 각 공급업체가 제공하는 구성 요소는 빠르게 증가하고 있지만 기존의 수동 기반 보안 관리 방안으로는 공급망 확대의 속도를 따라잡을 수 없다.



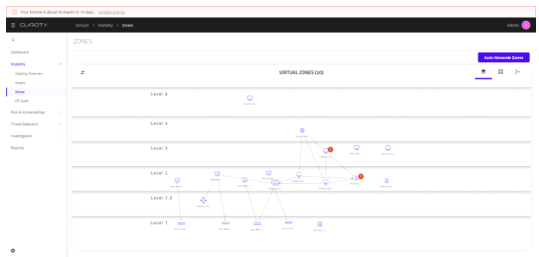
〔그림 2〕 Panorays를 통한 공급망 위험 등급 평가

공급망 어택서피스 관리를 위한 상용 플랫폼인 파노레이(Panorays)는 공급망을 구성하는 공급업체에 대한 보안 평가 및 관리 프로세스를 자동화하여 수동 관리 시 발생할 수 있는 오탐을 줄이고 신속한 보안 관리를 지원한다.

5.4. 공급망 네트워크 보안 관리

앞서 공급망 보안 관리와 관련하여 소프트웨어 공급망을 중점적으로 서술하였으나, 공급망은 소프트웨어만으로 구성되는 것이 아니며 하드웨어 요소도 포함되어 있다[1]. 이에 따라 소프트웨어와 관련된 보안 취약점 외에 하드웨어를 기반으로 공급망 공격이 이루어질 수도 있기 때문에 철저한 공급망 보안 관리를 위해서는 하드웨어 측면의 보안 관리도 수행해야 한다.

그러나 하드웨어 구성 요소 역시 소프트웨어와 마찬가지로 각 구성 요소에 대한 가시성을 확보하는 것에 한계가 있기 때문에 전문적인 스캔 기술을 토대로 하드웨어 구성 요소 사이의 가시성을 확보할 수 있는 상용 도구를 활용하는 것도 하나의 대응 방안이 될 수 있다.



〔그림 3〕 OT/ICS 보안 모니터링 도구, Claroty를 통한 하드웨어 자산의 가시성 분석

Ⅵ. 공급망 보안 관리 연구의 필요성

공급망 보안 관리 체계를 구축하기 위해서는 현재까지 발생한 공급망 공격 사례를 중심으로 추후 발생할 것으로 예상되는 공급망 공격 동향을 파악하는 것이 중요하다. 이와 더불어 앞서 언급한 각종 표준 및 규제의 요구사항에 대한 분석을 토대로 공급망 보안 관리의 핵심적인 역할을 수행할 수 있는 기술을 식별하고, 각 기술을 전문적으로 활용할 수 있는 플랫폼을 도입하여 보안 관리를 수행하는 것이 중요하다.

Ⅶ. 결 론

설시한 바와 같이 지속적으로 확대되고 있는 공급망 공격으로 인한 피해를 최소화하고 안전하게 소프트웨어 기반 제품을 사용하기 위해서는 공급망 보안을 체계적으로 관리하는 것이 무엇보다 중요하다. 공급망 보안의 체계적인 관리를 위해서는 공급망 공격의 유형을 세분화하여 분석하고 각 공격 유형에 대응할 수 있는 보안 관리 방안을 수립하는 것이 필수적이다.

이와 더불어 공급망을 구성하고 있는 구성 요소를 명확하게 식별하여 각 구성 요소 사이의 가시성을 파악하는 것이 전제되어야 할 것이다.

또한 사이버 공격의 타겟이 될 수 있는 보안 허점을 효과적으로 관리하기 위해서는 이러한 분석 데이터를 기반으로 SBOM과 DBOM을 생성하고 관리하여 공급망에 내재되어 있는 보안 취약점을 탐지하고 각 취약점을 완화할 수 있는 지속적인 모니터링 체계를 구축 및 운영해야 할 것이다.

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 1711126056)

참 고 문 헌

[1] 김대원 외 4, "*공급망 보안기술 동향*", 전자통신동향분석, 제35권 제4호, pp. 149-157, 2020년

〈저 자 소 개〉

강 우 성(WooSeong Kang)
2008년 8월 : 광운대학교 미디어콘텐츠 석사
2010년 6월 : 광운대학교 정보디스플레이학과 박사 중퇴
IT & 정보보안 경력 20년
현재 : 쿤텍㈜ 임베디드보안개발팀 수석연구원
<관심분야> 정보보호, 임베디드

방 혁 준 (Hyunkjun, Pang)
2004년 2월 : 강원대학교 경영학과 학사 졸업
2022년 3월 : 고려대학교 세종캠퍼스 융합과학대학원 석사 재학
2015년 12월 : ㈜MDS테크 보안 솔루션 사업부 팀장 근무
현재 : 쿤텍㈜ 대표이사
<관심분야> 정보보호, 임베디드