정 보 보 호 학 회 지
제 32 권 제5호, 2022. 10

FOSSLight를 활용한 공급망 보안 관리

김 경 애*

요 약

소프트웨어 개발이 고도화되고 개발 주기가 점점 짧아짐에 따라 단독으로 소프트웨어를 개발하는 것은 어려워졌다. 소프트웨어 개발의 복잡도가 높아짐에 따라 기업에서 함께 협업하는 여러 공급망 소프트웨어의 결합이 강화되고 이에 따라 소프트웨어 공급망 보안 강화가 함께 이루어져야 한다. 본고에서는 오픈소스 및 관리를 효율적으로 할 수 있도록 오픈소스로 공개된 FOSSLight 도구를 활용한 공급망 보안 관리 방안을 제안한다.

Ⅰ. 서 론

2021년 5월, 바이든 행정부는 국가 사이버보안 강화를 위한 행정명령(Improving the Nation's Cybersecurity, EXECUTIVE ORDER 14028)을 통해 연방정부와 사업 계약을 맺은 기업의 SBOM 제출을 의무화하였다. SBOM(Software Bill of Materials, 소프트웨어 자재명세서)은 소프트웨어의 구성 요소를 정리한 목록으로 미국 행정명령 문서에서는 이를 소프트웨어 구축에 사용되는 다양한 구성 요소의 세부 사항 및 공급망 관계를 정해진 형식에 따라 공식 기록하는 것이라고 표현하고 있다. SBOM을 통하여 소프트웨어의 생산자, 소비자 및 운영자는 이를 통해 공급망에 대한 이해를 높이고, 소프트웨어의 취약점과 위험을 쉽게 추적할 수 있게 된다는 의도이다.

이와 같이 바이든 행정부의 사이버보안 강화를 위한 행정명령이 아니더라도 최근 업계에서는 공급망 보안 이슈가 점점 중요해지고 있는데, 이는 2021년 12월 log4j 오픈소스 보안 취약점 사태를 겪으면서, 소프트웨어 사용 현황 및 이를 바탕으로 한 공급망 보안 관리의 필요성을 몸소 느끼게 되었기 때문이다.

최근 소프트웨어 개발이 고도화되고 개발 주기는 점점 짧아짐에 따라 소프트웨어를 단독으로 개발하는 회사는 거의 없다. 우리가 잘 알고 있는 안드로이드 플랫폼만 해도 구글이 직접 모든 것을 개발한 것이 아니라 리눅스 커널 및 여러 오픈소스를 많이 포함하고 있다. 비단 오픈소스뿐만이 아니라 여러 업체와의 협업을 통해서 소프트웨어 개발이 이루어지기 때문에, 기업은 자체적으로 개발하는 소프트웨어 외에 외부로부터 들여오는 모든 소프트웨어에 대한 책임을 함께 지게 된다. 이 범위에는 소프트웨어 품질뿐만 아니라 오픈소스 의무사항 준수 그리고 보안 취약점 관리가 포함된다. 소프트웨어 공급망 관리가 중요해지는 이유이기도 하다.

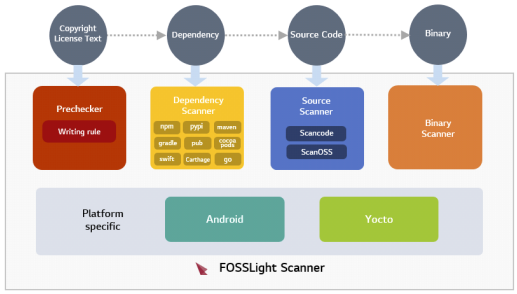
본고에서는 공급망 관리의 여러 요소 중 특히 공급망 보안에 초점을 맞추고, 이를 LG전자에서 개발하여 오픈소스 프로젝트로 공개한 FOSSLight를 활용하여 관리하는 방법을 제안하고자 한다.

Ⅱ. FOSSLight 프로젝트

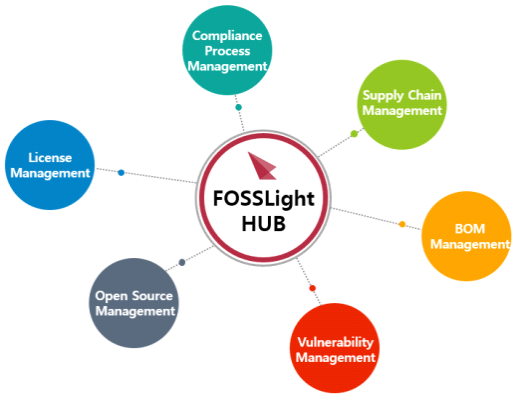
FOSSLight 프로젝트[1]는 오픈소스 분석을 수행하는 FOSSLight Scanner와 오픈소스를 통합적으로 관리할 수 있는 시스템인 FOSSLight Hub의 두 축으로 크게 나눌 수 있다. 22년 9월 기준 FOSSLight Scanner는 Prechecker, Dependency Scanner, Source Scanner, Binary Scanner 4가지의 스캐너로 구성되어 있으며, 이를 통합적으로 수행할 수 있는 All Scanner가 공개되어 있다. 또한 플랫폼 기반으로 오픈소스 분석을 쉽게 해주는 Android Scanner와 Yocto Scanner가 곧 공개될 예정이다. FOSSLight Scanner의 주요 기능은 소프트웨어를 분석하고, 소프트웨어에서 사용하는 오픈소스와 라이선스 정보를 추출한다.

FOSSLight Hub는 오픈소스와 라이선스를 관리하

* LG전자 SW센터 SW공학연구소 (Open Source Task Leader, kyoungae.kim@lge.com)



〔그림 1〕FOSSLight Scanner



〔그림 2〕FOSSLight Hub

고, 오픈소스 컴플라이언스 프로세스를 순차적으로 처리할 수 있는 통합 시스템이자 보안 취약점, 소프트웨어 공급망 관리 및 SBOM 관리 등 오픈소스와 관련된 모든 것을 관리할 수 있는 올인원 시스템으로 기획된 시스템이다. 하지만 FOSSLight Hub는 오픈소스에만 국한되지 않고 전체 소프트웨어를 관리할 수 있도록 확장 용이하기 때문에, SBOM 관리가 가능하다. FOSSLight Hub를 좀 더 자세히 살펴 보자.

2.1. 라이선스 관리

FOSSLight Hub는 라이선스 정보를 관리할 수 있다. FOSSLight Hub는 원래 오픈소스 라이선스를 관리하기 위해 기획된 시스템으로 오픈소스 라이선스에 특화되어 있기는 하지만, 상용 라이선스도 등록하여 관리할 수 있다. 라이선스는 Permissive, Copyleft, Proprietary 등으로 분류하여 관리하며, 특히 ISO/IEC 5962 표준인 SPDX[2] 준수를 위하여 SPDX 라이선스 식별자로 관리하고 있다.

또한 라이선스 준수를 위해 제일 중요한 라이선스 고지, 저작권 고지 및 소스 공개 등의 의무 사항을 관리할 수 있으며, 상용 사용 금지, 특정 플랫폼에서만 사용 가능, 재배포 금지, 수정 금지 등 라이선스마다 다른 여러 제약 사항들을 커스터마이징하여 관리할 수 있다.

2.2. 오픈소스 관리

FOSSLight Hub는 오픈소스 메뉴에서 오픈소스 정보를 저장할 수 있다. 각각의 오픈소스는 저작권 정보, 라이선스 정보, 오픈소스를 다운로드받을 수 있는 링크 및 홈페이지 정보를 저장한다. 라이선스를 선택하면 해당 라이선스에 따라 의무 사항이 자동으로 표시되고, 또 매일 업데이트되는 NVD(NATIONAL VULNERABILITY DATABASE)[3]정보에 따라 보안 취약점 정보도 자동으로 표시된다.

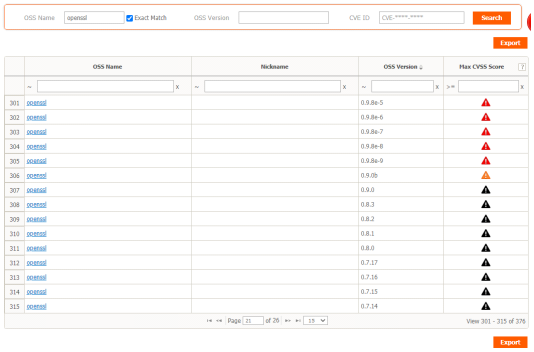
하지만 FOSSLight Hub는 오픈소스만 관리할 수 있는 게 아니라 상용 소프트웨어를 포함한 모든 소프트웨어를 등록하여 관리할 수 있다. 예를 들어 자체 개발한 모듈도 모듈 이름으로 등록하여 관리할 수 있고, 외부 공급망으로부터 입수한 소프트웨어도 직접 등록하여 관리할 수 있다.

2.3. 보안취약점 관리

FOSSLight Hub는 NIST (미국 국립표준기술연구소)에서 운영하는 NVD에서 제공하는 CVE (Common Vulnerabilities and Exposure) 정보를 취합하여 보안 취약점 정보를 제공한다. 매일 자동으로 NVD 정보를 업데이트하고 있으며, 소프트웨어와 그 버전에 따른 보안 취약점 조회도 가능하고, 해당 보안취약점의 CVSS 점수 (소프트웨어 취약성의 특성과 심각도를 전달하기 위한 개방형 프레임워크를 활용하여 제공하는 점수)를 버전 3 기준으로 제공한다.

소프트웨어 이름과 버전에 따라 검색하면 해당 보안 취약점 정보 중 가장 높은 CVSS 점수를 색깔별로 구분하여 보여주고 해당 정보를 클릭하면 다음 그림처럼 좀 더 자세한 정보를 보여준다.

CVSS 점수를 구분하여 보여주는 기준은 NVD에서 정한 심각도에 따른 점수 범위 그대로 보여주고 있다.



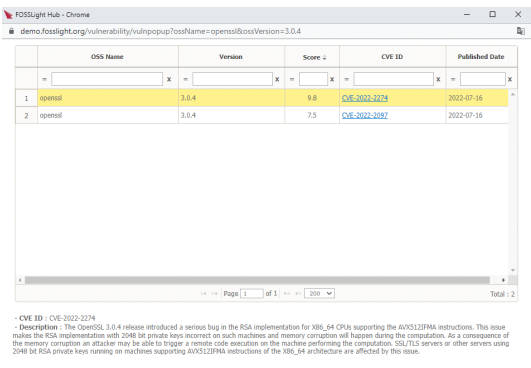
〔그림 3〕 보안취약점 조회

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

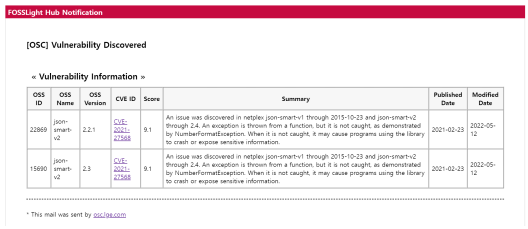
〔그림 4〕 보안 심각도에 따른 구분

CVE-2022-2274 보안 취약점을 예로 들자면, 보안 취약점 정보 링크와 하단 Description에서 요약 정보를 제공함으로써, 직접 보안 취약점 내용을 확인하고 조치를 할 수 있도록 도와준다.

보안 취약점은 새로 발견되고 또 제거되기도 하고 보안 취약점 점수가 낮아지는 등 수시로 업데이트되기도 한다. 이를 대비하여 이미 완료된 프로젝트에서 보안 취약점 정보가 업데이트된 경우를 위해서 FOSSLight Hub에는 해당 프로젝트 생성자와 관련자들에게 보안 취약점 업데이트에 대하여 메일로 알려주는 기능이 있다.



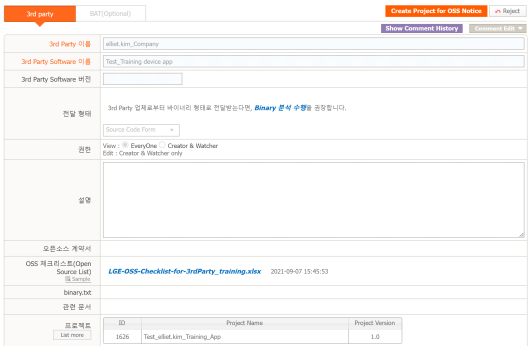
〔그림 5〕 보안 취약점 조회 상세 화면



〔그림 6〕 보안 취약점 알림 메일

2.4. 공급망 관리

FOSSLight Hub를 활용하여 외부에서 유입된 소프트웨어에 대한 관리가 가능하다. 외부로부터 전달받은 소프트웨어 안에 포함된 소프트웨어 정보와 해당 소프트웨어와 관련된 부가 정보 혹은 계약서와 같은 관련 문서 등을 저장할 수 있다. 저장할 수 있는 정보에는 소프트웨어 이름과 버전, 라이선스 정보, 해당 소프트웨어를 다운로드받을 수 있는 링크 및 홈페이지, 저작권 정보 등이 있다. 이를 기반으로 FOSSLight Hub는 오픈소스에 따른 의무 사항과 보안 취약점 정보를 자동으로 알려주고, 이를 개발 프로젝트에서 자동으로 불러올 수 있게 함으로써 오픈소스 컴플라이언스 관리 외에도 SBOM 관리를 효율적으로 가능하게 한다.



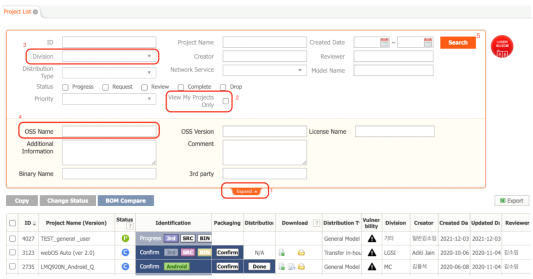
〔그림 7〕 공급망 소프트웨어 등록 화면

2.5. 프로젝트 관리

FOSSLight Hub는 오픈소스 컴플라이언스 프로세스 준수를 위한 프로젝트 관리를 하기 위해 개발된 시스템으로 본 기능이 매우 고도화되어 있다. 프로젝트를 생성하여 오픈소스 정보를 입력하고, 해당 오픈소

스 정보에 따른 의무 사항을 확인할 수 있다. 이를 식별 (Identification) 단계라고 부르며, 식별 단계 이후에는 소스 공개 의무 사항이 있는 오픈소스의 코드를 취합하여 확인하고, 고지 의무가 있는 오픈소스를 확인하여 오픈소스 고지문을 자동으로 생성하는 패키징 단계를 거친다.

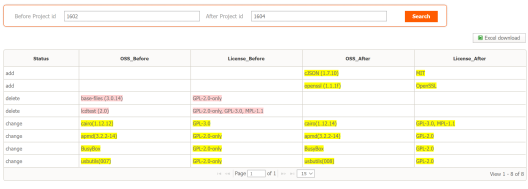
프로젝트 관리 메뉴에서 프로젝트와 관련된 여러 정보로 검색이 가능하고, 추적 또한 가능하다. 예를 들어 AGPL-3.0 라이선스를 사용하는 프로젝트 조회, log4j 오픈소스를 사용하는 프로젝트 조회 등이 가능하다. 이 기능을 활용하여 SBOM 관리 또한 쉽게 할 수 있다.



〔그림 8〕 프로젝트 조회 화면

2.6. SBOM 관리

FOSSLight Hub는 SBOM 관리가 가능하다. 프로젝트별, 공급업체가 제공하는 소프트웨어별 목록 관리가 가능하고, 각각의 단위로 SBOM 관리 또한 가능하다. 또한 프로젝트별로 소프트웨어 목록을 비교하는 기능이 있어, 프로젝트마다 혹은 프로젝트 버전이 변경될 때마다 변경되는 소프트웨어 확인도 가능하다.



〔그림 9〕 SBOM 비교 화면

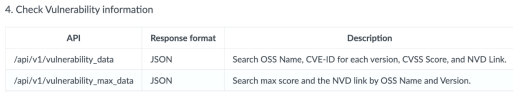
2.7. 스캐너 연동 기능

FOSSLight Hub의 주요 기능은 오픈소스 관리를 위한 시스템이지만, 오픈소스 분석을 손쉽게 제공하기 위하여 오픈소스 스캐너 연동 기능을 지원하고 있다. 현재 FOSSLight Hub의 Self-Check 리스트의 URL 분석 메뉴를 통해 스캐너 연동이 가능하며, FOSSLight 데모 사이트[4]에는 FOSSLight Scanner가 연동되어 있다. 즉 소프트웨어를 분석하고 싶은 소스 저장소 링크를 입력하면, FOSSLight All Scanner가 실행되어 그 결과를 FOSSLight Hub에서 직접 확인할 수 있다.

이 기능을 이용하여 기업에서 사용하고 있는 보안취약점 스캐너가 있다면 해당 스캐너를 FOSSLight Hub와 연동할 수 있다. FOSSLight Hub는 오픈소스 프로젝트로 공개되어 있기 때문에 기업에서 원하는대로 커스터마이징하여 개발할 수 있다는 점이 최대 장점이다.

2.8. API 제공

FOSSLight Hub를 통하여 자동화를 가능하게 하는 것은 FOSSLight Hub에서 Rest API를 제공하기 때문이다. 소프트웨어나 라이선스 검색, 보안 취약점 조회 등의 다양한 기능을 Rest API로 제공하여 이를 다양한 시나리오로 적용할 수 있다. 예를 들면 FOSSLight Hub의 보안취약점 관련 API 리스트는 다음과 같고, 이를 활용하여 보안취약점 알림 기능을 개발할 수 있다.



4. Check Vulnerability information

API	Response format	Description
/api/v1/vulnerability_data	JSON	Search OSS Name, CVE-ID for each version, CVSS Score, and NVD Link.
/api/v1/vulnerability_max_data	JSON	Search max score and the NVD link by OSS Name and Version.

〔그림 10〕 보안 취약점 조회 API

현재 FOSSLight Hub에서 제공되는 API를 통하여 상용 스캐너 도구인 FOSSID[5]나 Blackduck[6]에서 FOSSLight Hub 프로젝트 생성을 위한 연동 도구를 오픈소스로 공개하고 있으며, 이와 마찬가지로 다른 여러 스캐너도 FOSSLight Hub 연동 기능을 추가할 수 있다.

지금까지 살펴본 FOSSLight Hub의 기능을 요약하면 다음과 같다.

〔그림 11〕 FOSSLight Hub 기능

Ⅲ. 공급망 보안 관리 방안

FOSSLight Hub를 통하여 공급망 보안 관리를 하는 방안으로 크게 세 가지를 고려할 수 있다. 공급망으로부터 소프트웨어를 전달받기 전에 공급망 업체에서 미리 점검하는 방법, 기업에서 공급망 보안 관리를 시스템화하는 방법, 그리고 개발 부서에서 직접 보안 취약점 조회 및 관리를 하는 방법으로 이를 모두 활용하면 공급망을 포함하여 기업에서 보안 관리를 체계적으로 할 수 있을 것이다.

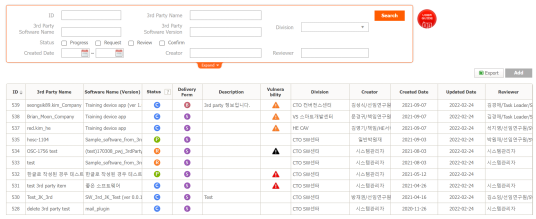
3.1. 공급망 업체 사전 점검

공급망에서 소프트웨어를 공급받을 때 SBOM 제출을 의무화함에 있어 공급망에서 사전 점검할 수 있도록 환경을 마련해주는 것은 중요하다. FOSSLight Hub를 공급망 업체가 사용할 수 있도록 서비스를 제공하여 FOSSLight Hub의 Self-Check 메뉴에서 사전에 보안취약점이 없는지 점검할 수 있는 환경을 제공할 수 있다.

또한 사전 점검 후에 FOSSLight Hub의 “Export” 기능을 이용하여 FOSSLight Report를 제출하게 하면 추후 공급망 소프트웨어 관리 시 FOSSLight Hub에 쉽게 등록할 수 있게 된다.

3.2. 공급망 관리

외부 공급망으로부터 소프트웨어를 전달받을 때마다 FOSSLight Hub의 3rd party 메뉴를 활용하여 등록하는 것을 규정화하면 좋다. 3rd party 메뉴에서 공급망과 관련된 모든 정보를 데이터베이스화해서 관리하게 되면, 여러 검색 기능을 통해서 원하는 정보를 쉽게 찾을 수 있을 뿐 아니라 공급망 소프트웨어의 SBOM 관리도 쉽게 가능하다. 예를 들어 log4j를 포함한 소프트웨어 공급망을 찾는다던가 소프트웨어 입수일, 사내에서 해당 공급망을 관리하는 담당자 등 여러 정보를 손쉽게 관리할 수 있다.



〔그림 12〕 FOSSLight Hub - 3rd party 메뉴

이처럼 공급망 소프트웨어를 등록하여 관리하면, FOSSLight Hub는 실제로 개발하는 프로젝트에서 공급망 소프트웨어를 자동으로 로드하는 기능을 제공한다. 이 방법을 이용하여 하나의 프로젝트에서 사용하는 여러 공급망 소프트웨어를 관리할 수 있다. 또는 하나의 공급망 소프트웨어를 그대로 하나의 프로젝트에 사용하는 경우라면 3rd party 메뉴에서 바로 프로젝트를 생성할 수 있는 단축 기능도 제공되니 쉽게 프로젝트를 생성할 수 있다.

이처럼 프로젝트 등록을 해두면, 해당 프로젝트의 소프트웨어에 보안취약점이 발견될 때마다 메일로 알림을 받을 수 있다. 현재는 CVSS 심각도 정도에 따라 9.0 이상인 경우 메일로 알려주도록 활성화되어 있는데, 이것 역시 설정값을 변경하여 조정할 수 있다.

3.3. 개발 부서의 보안 취약점 관리

개발 부서에서는 개발할 때 일정 주기에 따라 개발 레파지토리 소스 코드를 소프트웨어 스캐닝 도구로 분석하도록 환경 설정을 할 수 있다. 주기적으로 분석한 결과를 FOSSLight Hub의 API로 연동하여 해당 보안 취약점을 알림 받도록 하는 설정 또한 가능하다. 조치가 필요한 오픈소스 보안 취약점 기준 점수를 정해두면, 기준 점수보다 높은 보안 취약점이 발견되는 경우 해당 소스 코드를 추가한 개발자에게 알림이 되도록 자동화하는 것이다. 이와 같은 자동화를 통하여 소프트웨어 개발 시점부터 보안 취약점 관리를 함으로써,

선제적으로 보안취약점 대응을 할 수 있다는 장점이 있다.

물론 보안 취약점 알림 기능은 FOSSLight Hub에서도 자체적으로 제공하고 있지만, FOSSLight Hub에서 프로젝트 생성하기 전에도 보안 취약점 관리를 할 수 있다는 점에서 개발 레파지토리에서 보안 취약점 조회를 자동화하는 것이 더 유용하다. 또한 FOSSLight Hub는 프로젝트를 생성한 사용자나 Watcher로 추가된 사용자에게 알림이 가기 때문에 소스 코드를 직접 추가한 개발자가 놓칠 수도 있는 것을 막을 수 있다는 것도 큰 장점이 될 수 있겠다.

Ⅳ. 결 론

소프트웨어 공급망 관리의 중요성이 점점 높아짐에 따라 공급망 관리를 기존처럼 수작업으로 하게 되면 놓칠 수 있는 많은 약점이 존재한다. 공급망 관리를 시스템화하고, 보안 취약점 관리 또한 자동으로 이루어질 수 있는 환경이 되어야 한다. 지금까지 살펴본 것과 같이 FOSSLight 도구를 활용하여 공급망 관리 및 보안 취약점 관리가 가능하다. 또한 개발자들에게 자동 알림이 되도록 관리 방안이 구축된다면, 오픈소스 관리뿐만 아니라 보안취약점 관리가 개발과 별도의 작업이 아니라 개발과 동시에 자연스럽게 이루어질 수 있다. 이와 같은 활동은 오픈소스나 보안취약점에 대한 인지와 함께 긍정적인 선순환이 될 것이다.

참 고 문 헌

[1] https://fosslight.org/
[2] https://spdx.org/
[3] https://nvd.nist.gov/
[4] https://demo.fosslight.org/
[5] https://github.com/OSBC-Inc/fosslight_in tegration
[6] https://github.com/tech-kms/blackduck -fosslight-sync_CLI

〈저 자 소 개〉

김 경 애 (Kyoungae Kim)
2001년 3월 : 서울대학교 컴퓨터공학부 학사
2003년 8월 : 서울대학교 컴퓨터공학부 석사
현재 : LG전자 오픈소스 태스크 리더
<관심분야> 오픈소스, 정보보호, 거버넌스, SBOM