ETRI Insight

ICT정책 이슈&트렌드 2023-03

사이버보안 강화를 위한 공급망 정책 현황과 전략

안춘모

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

본 보고서는 ETRI 기술정책연구본부 기본사업인 “국가 지능화 기술정책 및 표준화 연구”를 통해 작성된 결과물입니다.

Executive summary

공급망 위협 및 공격 현황

- 공급망에 대한 위협과 공격은 제품의 생산/유지에 사용되는 SW 내용 및 HW 부품 회로의 구성을 악의적으로 변경하는 범죄 행위임
- 2020년 SolarWinds 해킹, 2021년 Kaseya 랜섬웨어 유포, Apache Log4j 취약점 공격, 콜로니얼 파이프 라인 랜섬웨어 감염 등 최근 심각한 공급망 공격 급증
- 공급망 공격의 심각성은 단순 금품을 노린 개인의 행위에서 벗어나, 최근에는 국가가 주도하거나 지원하는 전문적인 해킹 그룹이 금전적인 위협뿐 아니라, 국가의 핵심 인프라, 나아가 국가 안보에도 영향을 미치고 있다는 점
- 공급망 공격은 HW, SW, 사용자를 대상으로 하며, 공격 표면은 다양해짐

구분		공격 유형
HW 측면	HW 구성요소 (IC칩, PCB, 펌웨어)	하드웨어 트로이 공격 (HT)
		부채널 공격 (SCA)
		FPGA 공격
SW 측면	업데이트 서버	위·변조 패치파일 배포
	인프라 구성요소 (CI/CD)	CI/CD 구성 도구 취약점 공격
	접근제어 우회 (인증/인가)	인증서 탈취
		관리자 페이지 노출
		원격접속 프로토콜 접근 계정 탈취
인적 측면	사회공학 (Social Engineering)	스피어 피싱 (Spear Phishing)
		워터링 홀 (Watering Hole)

주요국의 공급망 보안 정책 추진 현황

(미국) 행정명령 EO-14028을 중심으로 적극적인 정책 추진 중

- 행정명령 4절에서는 NIST가 기존 표준, 절차 및 기준을 참조하여 SW 공급망 보안을 강화하기 위한 관행을 식별하는 다양한 지침을 게시할 것을 요구
- 그동안 발표된 보고서 가운데 EO-critical SW의 정의, NISTIR 8397(벤더나 개발자의 개발 소스코드 테스트에 대한 지침), SP 800-218 (SSDF ver 1.1), SP 800-161 (C-SCRM 지침) 등이 공급망 보안을 위해 자주 언급되는 문서임

발표 날짜	보고서 명 등	보고서 목적
2021.6.26.	[정의] Publish definition of EO-critical software	• EO-Critical SW는 연방 정부에서 사용하는 주요 SW 제품에 대한 보안 기준을 개발하기 위해 행정명령에서 도입한 개념
2021.7.11.	[안전한 SW 개발 - 가이드라인] (NISTIR 8397) Publish guidance Recommending Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028 (4r)	• 행정명령에서 공급업체의 소스코드 테스트에 대한 지침 게시를 지시하고 있으며, NIST는 SW 공급업체 또는 개발자 검증을 위한 최소 표준을 권장하는 문서를 개발 • 본 가이드라인에는 벤더나 개발자에 의한 SW 검증 시에 추천되는 11개의 최저 기준 제시
2021.9.30. (초안) 2022.2.4. (최종)	[안전한 SW 개발 프레임워크] (SP 800-218) Secure Software Development Framework (SSDF) Version 1.1 : Recommendations for Mitigating the Risk of Software Vulnerabilities	• 초기 SSDF(Secure Software Development Framework)에는 보안 SW 개발 실무 문서를 기반으로 하는 기본적이고 건전하며 안전한 SW 개발 실무 세트
2022.5.5.	[공급망 보안 - 가이드 라인] NIST SP 800-161 Rev. 1, Cyber Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations	• 본 문서의 목적은 공급망 전반에 걸쳐 사이버보안 위험을 관리하는 데 도움이 되도록 기업 전반에 걸쳐 위험 관리 프로세스를 식별, 평가, 선택 및 구현하고 통제를 완화하는 방법에 대한 지침을 기업에 제공하는 것

◉ EU는 사이버보안 정책의 효과적 실행을 위한 지속적인 입법 추진

- NIS 2 지침, CER 지침 (주요 조직 복원력 지침), Cyber Resilience Act (사이버 복원력 법안), 사이버보안법 개정안 등을 추진 중
  - 사이버 복원력 법안은 EU 내 디지털 제품의 사이버보안을 강화하고 현재의 사이버보안 규제 격차에 대응하기 위함

공급망 보안 기술 현황

◉ HW 공급망 보안 기술 중 파괴적 기술로는 역공학, 비파괴적 기술로는 채널 분석, 테스팅, 이미징 등이 있음

◉ SW 공급망 보안 기술로는 정적 코드 분석과 동적 코드 분석이 중심 방법

- 정적 분석과 동적 분석은 일견 상반된 속성을 가지고 있으나, 보완적 활용 필요

정적 분석 도구	동적 분석 도구
화이트 박스 보안 테스팅	블랙 박스 보안 테스팅
소스 코드 필요	실행하는 애플리케이션 필요
SDLC 초기에 취약점 탐색	SDLC 종료로 향할 때 취약점 탐색
취약점 수정에 비싸지 않음	취약점 수정에 좀 더 비쌈
런타임 및 환경 관련 이슈 발견 불가	런타임 및 환경 관련 이슈 발견 가능
일반적으로 모든 종류 SW 지원	일반적으로 웹 애플리케이션과 웹 서비스 같은 앱만을 스캔

공급망 보안 강화를 위한 미래 전략(안) 제안

(제도 동조화) 미국, EU의 공급망 보안 시책과의 동조화 필수

- (전략 방향) 미국과 EU가 도입·추진하는 정책에 대한 동조화를 통해 국내 디지털 기기의 글로벌 경쟁력 확충

(SoC 보안 강화) 주요 기반시설 보호 체계화

- (전략 방향) 국내 주요 기반시설 인프라 보호를 위한 선진국 수준의 법률적 지원과 함께 인프라 위협 공동 대응 강화
  - 중요 인프라 보안 강화를 위한 기본법 제정 (중요 인프라 범위 설정, 거버넌스 포함)

(HW 공급망) HW 공급망 강화를 위한 종합적 시책 정립

- (전략 방향) 국내 HW 공급망 보안을 위한 정부 지원 체계 개선(조직, 제도 등) 및 domain 중심의 HW 공급망 연구개발 확대
  - HW 취약점 탐지 자동화 기술 개발 (바이너리 코드 분석, 역공학 등 포함)
  - 의료 분야에 대한 ICT 공급망 보안 R&D 추진 (ZT 제도 도입, HW 공격 감지 등)

(Domain별 전주기 관리구축) 국민 생활과 연계성이 높은 부문(의료, 자동차, 모바일 등)에 대해 Domain 특화형 전주기 관리 정책 구축

- (전략 방향) 국민 생활 안전을 지향하며 기기들에 대한 사전·사후 관리까지 포괄하는 공급망 보안 시책 구축
  - 의료 분야에 대한 ICT 공급망 보안 R&D 추진 (ZT 제도 도입, HW 공격 감지 등)
  - 스마트 자동차, 전기자동차 등에 대한 한국형 공급망 보안 가이드라인 구축

목 차 C O N T E N T S

참고문헌

국내자료

국가보안기술연구소 정은구 (2022), 하드웨어 공급망을 위한 하드웨어 역공학 기술, 2022 공급망보안 워크숍

김권일·김지원 (2020. 8.), 4차 산업혁명 기술 도입에 따른 하드웨어 공급망 위협과 대응 방안

김대원 등 (2020. 8. 1.), 공급망 보안기술 동향, Vol. 35 No. 4, 전자통신동향분석

KISA Insight (2023. 8.), EU의 디지털 미래 구축을 위한 사이버보안 방향과 시사점

국외자료

미하원 (2003), Consolidated Appropriations Act, 2023 : SUMMARY OF APPROPRIATIONS PROVISIONS BY SUBCOMMITTEE

백악관 (2022. 9. 14.), M-22-18 : MEMORANDUM FOR THE HEADS OF EXECUTIVE DEP ARTMENTS AND AGENCIES

백악관 (2021. 5.), 행정명령 EO-14028 - Executive Order on Improving the Nation's Cybersecurit

CISA (2023. 4. 27.), Secure Software Self-Attestation Common Form

Cynerio (2022), State of Healthcare IoT Device Security

ENISA (2021. 7.), ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

EU (2022. 12.), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Dire ctive (EU) 2016/1148 (NIS 2 Directive)

Microsoft (2020. 2. 3.), Guarding against supply chain attacks—Part 2: Hardware risks

METI (2022. 8. 23.), OSS Security Initiatives

NIST (2022. 5.), "Cybersecurity Supply Chain Risk Management Practices for Systems and Orga nizations", NIST SP 800-161r1, pp. 1-3

NIST (2021. 10. 13.), Definition of Critical Software Under Executive Order (EO) 14028

NIST (2022. 2.), NIST SP 800-218 : Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

NIST (2018. 12.), SP 800-37 Rev. 2, Risk Management Framework for Information Systems an

d Organizations: A System Life Cycle Approach for Security and Privacy

NIST (2020. 9. 23.), SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations

NIST (2011. 3.), SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View

NIST (2022. 5.), SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

NIST (2022. 2.), SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

NIST (2022.2.4.), Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e

NIST (2021. 7. 8.), Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0

NIST (2021. 7. 8.), Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-under

NIST (2021. 7. 7.), Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or

NIST (2021. 11. 8.), Executive Order 14028: Guidelines for Enhancing Software Supply Chain Security, https://www.nist.gov/news-events/events/2021/11/executive-order-14028-guidelines-%03enhancing-software-supply-chain

NIST (2022. 2. 4.), NIST Issues Guidance on Software, IoT Security and Labeling, https://www.nist.gov/news-events/news/2022/02/nist-issues-guidance-software-iot-security-and-labeling

NTIA (2021. 11. 1.), SBOM Myths vs. Facts

NTIA (2019), Roles and Benefits for SBOM Across the Supply Chain

NTIA (2021. 7. 12.), The Minimum Elements For a Software Bill of Materials (SBOM)

OMB (2022. 9.), "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices - MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPART

MENTS AND AGENCIES“, M-22-18, US Office of Management and Budget

The White House (2022. 9.), Enhancing the Security of the Software Supply Chain to Deliver a Secure Gover nment Experience from https://www.whitehouse. gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/

Sonatype (2022. 10. 18.), 8th Annual State of the Software Supply Chain

Synopsys (2016. 3. 5.), SAST vs. DAST: What's the best method for application security testing?, https://www.synopsys.com/blogs/software-security/sast-vs-dast-difference.html

웹사이트

백악관 홈페이지, https://www.whitehouse.gov.

이글루시큐리티, https://www.igloo.co.kr/

Appsealing, 빌드 보호를 위해 반드시 알아야 할 CI/CD 보안, https://www.appsealing.com/kr/ci-cd-보안/

Cynerio, “State of Healthcare IoT Device Security 2022”), https://www.cynerio.com/landing-pages/the-state-of-healthcare-iot-device-security-2022

LG전자 뉴스룸, [모빌리티 인사이드] #33 미래 차의 필수! 차량 사이버보안이란?, https://live.lge.co.kr/2304-mobility33-security/

신문기사

ITWorld (2020. 12. 17.), 공급망 공격을 탐지하기 어려운 이유, 솔라윈즈 공격 사건이 보여준다 (https://www.itworld.co.kr/news/176394)

데일리시큐 (2021. 1. 25.), [솔라윈즈 SUNBURST 보안위협 총정리] “한국 병원·대학·기관 등에서도 공격 스캔 발견”, (https://www.dailysecu.com/news/articleView.html?idxno=119928)

DataNet (2022. 7. 21.), 쿤텍·ETRI, 펌웨어 분석 활용 BoM 기술로 HW 공급망 보호, (https://www.datanet.co.kr/news/articleView.html?idxno=174744)

병원신문 (2022. 5. 16.), [공동기획] 의료기기 보안 취약점과 대응방안, (https://www.khanews.com/news/articleView.html?idxno=220540)

아이뉴스 (2019. 2. 11.), AI 사이버보안, 국제표준 주도권 누구 손에?, (http://www.inews24.com/view/1156488)

저자 소개

안춘모 ETRI ICT전략연구소 기술정책연구본부 기술경제연구실 책임연구원
e-mail: cmahn@etri.re.kr Tel. 042-860-5790

사이버보안 강화를 위한 공급망 정책 현황과 전략

발행인 한 성 수
발행처 한국전자통신연구원 ICT전략연구소
발행일 2023년 12월 31일

www.etri.re.kr

ETRI Electronics and Telecommunications Research Institute

34129 대전광역시 유성구 가정로 218
TEL.(042) 860-6114 FAX.(042) 860-6504