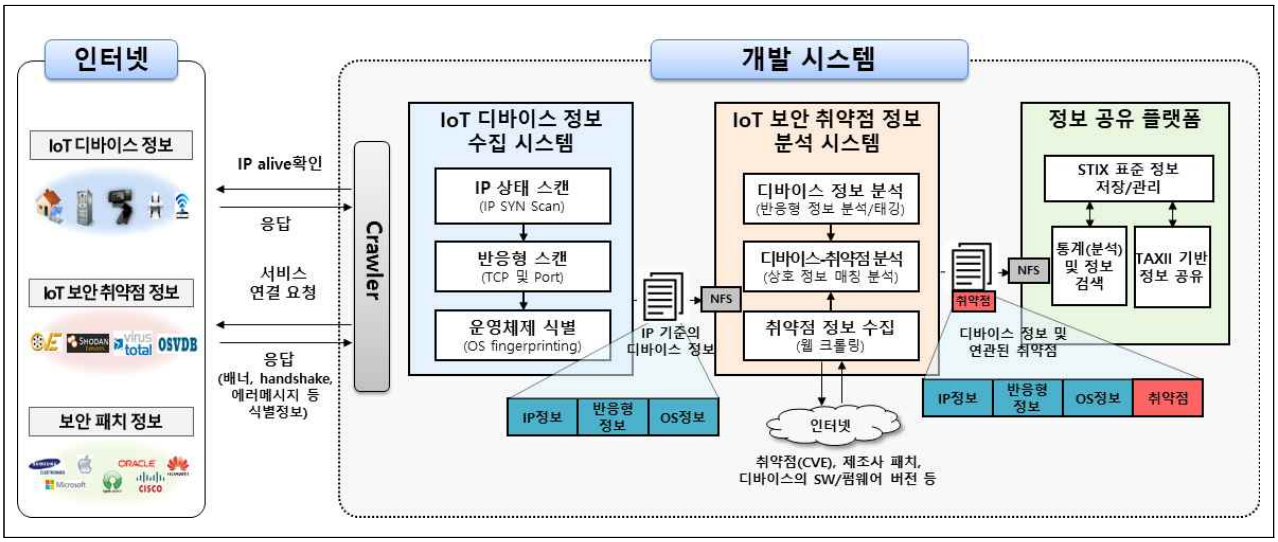
Ⅱ. 20년 기술이전 대상 목록

2 IoT 보안 취약점 검색·공유 및 시험 기술 ('16.4월 ~ '18.12월(3년))

□ 기술개요

o 네트워크 프로토콜, 오픈소스 SW 등의 보안이 취약한 디바이스를 DDoS 공격 등에 활용하는 보안 위협에 사전 대응하기 위한 기술 개발

< 기술 개념도 >



□ 기술의 특징 및 장점

o 인터넷에 연결된 디바이스의 정보(OS, SW 정보 등)를 수집하는 스캔
- IPv4/IPv6 기반의 공인IP 주소가 할당된 인터넷 연결 디바이스의 통신 패킷 및 오픈 포트 정보 수집

o 디바이스 정보와 공개된 취약점 정보의 연관성 분석을 통한 취약점 식별
- 디바이스 정보(CPE)와 취약점 정보(CVE)의 맵핑 분석을 통한 취약점 정보 식별

o 디바이스-취약점 정보의 공유를 위한 STIX·TAXII 표준 기반 정보 관리·연동

□ 활용 분야

o KISA 인터넷침해대응센터의 ‘취약점 탐지 및 분석 점검 시스템 개발‘ 사업에 개발 기술 적용

- 취약한 디바이스 현황 및 조치가 필요한 디바이스 정보 확보를 통한 사전 대응능력 강화를 위해 활용

□ 기술이전 내용 및 범위

구분	시스템	주요 내용
1	IoT 디바이스 정보 고속 수집 기술	o 인터넷에 연결된 호스트를 고속 스캔하고, 디바이스 정보를 수집하는 기술 o 세부 기술 구성 - 기술1 : 디바이스 스캔 및정보 수집 모듈 - 기술2 : 사용자 정의 프로토콜 기반 스캔(정보 수집) - 기술3 : OS 핑거프린트 기반 운영체제 식별 기술 - 기술4 : 디바이스 보안 취약점 점검 모듈
2	IoT 보안 취약점 정보 수집·분석 기술	o 공개된 취약점 정보를 기반으로 디바이스 취약점 정보를 식별하는 기술 o 세부 기술 구성 - 기술1 : 보안 취약점 정보·제조사 패치 정보 수집 - 기술2 : 디바이스 수집 정보 심층 분석 모듈 - 기술3 : 디바이스-취약점 정보 연관 분석 모듈

□ 기술이전 문의

기술이전 담당	김태은 책임연구원(061-820-1273, rndts@kisa.or.kr)