『IoT 보안테스트베드』 이용 및 교육 신청서

단체명		부서명		방문자 수	명
(유형)	□공공 □학계 □일반	직 위			
신청인 성명		신청인 연락처	내선번호 : 휴 대 폰 : 이 메 일 :		
주소					
이 용 희망일	**년 월 일 (오전 09:30~11:30 / 오후 14:00~17:00 중 택 1)** ※ 운영시간 : 월~금요일 09:30 ~ 17:00 (단, 토·일요일, 공휴일은 휴무)				

이용목적 (□에 체크표시)	□ 테스트 및 견학(붙임1)	□ IoT 보안 점검지원(붙임2)	□ 테스트베드 상시교육(붙임3)(4명 이상)
	□ IoT서비스 분야별 시연 환경 견학	□ 소스코드 취약점 점검 □ 오픈소스 및 SBOM 점검 □ 통신 프로토콜 취약점 점검 □ 펌웨어 취약점 도구	□Ⅰ. 시큐어 코딩 및 소스코드 점검 도구 가이드 □Ⅱ. 오픈소스 취약점 분석 도구 사용법 □Ⅲ. 디바이스 퍼징 테스트 □Ⅳ. 코딩 드론 ※ 기초교육은 별도 신청

점검분야			
□ 가전 □ 의료 □ 교통 □ 제조·생산 □ 금융 □ 주택 □ 도시 □ 통신 ※ IoT 보안 점검지원 신청 시 체크	점검대상 (제품 및 서비스)		
	이용 희망 도구	※ 붙임2 참조	
	점검 연계 제도	*예 : IoT 보안인증, 신속확인제도, 해당없음 등*	

< 개인정보 수집 · 이용 동의 안내 >

진흥원은 다음의 목적을 위해 개인정보를 수집·이용합니다. 수집된 개인정보는 정해진 목적 이외의 용도로는 이용되지 않으며, 수집 목적 등이 변경될 경우에는 사용 신청자에게 알리고 동의를 받을 예정입니다.

◈ **개인정보 수집·이용 내역**

개인정보 수집·이용 목적	개인정보 항목	보유·이용 기간
IoT 보안테스트베드 이용 및 교육 신청 (신청자 본인확인, IoT 보안테스트베드 이용 및 교육 신청, 설문조사 안내 등)	단체명, 부서명, 직위, 신청인 성명, 신청인 연락처(내선번호, 휴대폰번호, 이메일), 주소	**3년**

※ IoT 보안테스트베드 신청자는 개인정보 수집·이용에 동의하지 않을 권리가 있습니다. 단, 동의를 거부할 경우 IoT 보안테스트베드 시설 이용이나 교육 안내 등의 제한이 있을 수 있습니다.

▷ **개인정보 수집 · 이용 동의 여부** 동의 □ 미동의 □

< IoT 보안 점검지원 결과 활용 안내 >

진흥원은 IoT 보안 점검지원 시 점검도구를 통해 산출된 결과를 연구·통계 및 서비스 개선 목적으로 활용할 수 있으며, 이 과정에서 개인 또는 기업을 식별할 수 있는 정보는 익명 또는 가명 처리 후 활용 목적 내에서만 사용됩니다.

◈ **IoT 보안 점검지원 결과 활용**

결과 활용 목적	결과 활용 항목	보유·이용 기간
연구·통계·분석을 통한 IoT 보안 연구	보안 취약점 점검 결과 보고서	**5년**

※ IoT 보안테스트베드 신청자는 결과 활용에 동의하지 않을 권리가 있으며, 동의하지 않더라도 시설 이용에는 제한이 없습니다.

▷ **IoT 보안 점검지원 결과 활용 동의 여부 (선택)** 동의 □ 미동의 □

『IoT 보안테스트베드』 이용 신청서를 제출합니다.

년 월 일

신청인 (서명)

한국인터넷진흥원 귀하

※ 신청서 작성 후 iottestbed@kisa.or.kr로 송부 (붙임을 제외한 신청서만 송부)

붙임 1 IoT 서비스 분야별 시연 환경(안)

시연 환경	설명 및 활용방안	
홈	 	- 홈IoT 제품군 소개 ※ 스마트 TV, 냉장고, 스타일러, 에어컨, 청소기 등. ※ 무선 월패드, 스마트 도어락 , 움직임 감지, 스마트 버튼, 문열림감지기 등 - 홈IoT 제품(IP카메라, 공유기, 도어락) 해킹 시연 ※ IP 카메라 : 사생활 영상 탈취, 원격제어 및 사생활 침해 ※ 공유기 해킹 : 공유기 비밀번호 탈취, 피싱사이트 유도 ※ 도어락 : 도어락 태그 복제
건설		- 스마트 건설 보안취약성 해킹 시연 ※ 타워 크레인 해킹을 통한 무료주파수 조작 시연
의료		- 스마트 의료 보안취약성 해킹 시연 ※ 원격 투약환경 취약점을 이용한 인퓨전 펌프 오작동 시연
안전		- 스마트 안전재난 보안취약성 해킹 시연 ※ IoT전용망 해킹을 통한 안전재난 시스템 오작동 시연
드론	 	- 드론 보안 위협 해킹 시연 ※ 서비스 거부공격 시연 ※ MAC 주소 변조 시연 ※ GPS 조작 공격 시연 - 드론 시뮬레이터 ※ 가상환경 드론 운전 /autopilot 기능 - 드론체험관 ※ 해킹 시나리오 기반 드론 비행 체험 공간

※ 상기 테스트 및 시연 환경은 사정에 따라 변경될 수 있음

붙임2 IoT 보안 점검도구 현황

□ IoT 개발 단계에서의 보안테스트베드 도구 활용

설계·개발	테스트	운영
(소스코드 점검) Sparrow **(오픈소스 점검)** Cybellum, Insignary Clarity		
	(통신프로토콜 점검) Vanguard **(퍼징 테스트)** Defensics **(펌웨어 분석)** Trace32	

□ 세부 점검도구 리스트

소스코드 취약점 분석	**제품명**	Sparrow	**제조사**	스패로우	**수량**	2식
	**내용**	행안부 보안약점, CVE, OWASP, MISRA-C 등의 기준을 기반으로 소스코드의 보안 취약점을 빠르게 점검하는 정적 분석 테스트 도구				
오픈소스 취약점 분석	**제품명**	Cybellum	**제조사**	Cybellum	**수량**	1식
	**내용**	소프트웨어 실행파일 자체를 분석하는 '바이너리 파일 분석'을 통해 알려진 취약점 및 알려지지 않은 취약점 탐지, SBOM 제공				
오픈소스 취약점 분석	**제품명**	Insignary Clarity	**제조사**	Insignary	**수량**	1식

	**내용**	바이너리를 소스코드나 리버스 엔지니어링 없이 점검하여, 오픈소스 라이선스 및 보안 취약점 관리				
펌웨어분석	**제품명**	TRACE32	**제조사**	Lauterbach	**수량**	1식
	**내용**	프로세서 내부에 내장된 표준 디버그 인터페이스(JTAG)를 통해서 ARM/MIPS 아키텍처 타깃을 제어 및 모니터링				
펌웨어분석	**제품명**	JTAGulator	**제조사**	Grand IDEA Studio	**수량**	1식
	**내용**	IoT 디바이스, 보드 등에서 Serial 및 JTAG 인터페이스의 Pin 배치를 확인하는 도구				
프로토콜분석	**제품명**	Defensics	**제조사**	Synopsis	**수량**	2식
	**내용**	퍼징 기법을 통해 Bluetooth, Can-Bus를 사용하는 IoT 디바이스의 알려지지 않은 보안 취약점 점검(CWE, CVE 매칭 제공)				
프로토콜분석	**제품명**	Open Sniffer	**제조사**	Open Source	**수량**	1식
	**내용**	Zigbee 프로토콜을 사용하는 IoT 디바이스 대상 프로토콜 패킷 수집 및 분석				
프로토콜분석	**제품명**	AirPcap Nx	**제조사**	Riverbed	**수량**	1식
	**내용**	Wi-Fi 프로토콜을 사용하는 IoT 디바이스 대상 프로토콜 패킷 수집 및 분석				
프로토콜분석	**제품명**	HackRF One	**제조사**	Open Source	**수량**	1식

	**내용**	RF 1MHz ~ 6GHz의 무선 신호를 송수신 할 수 있는 SDR (소프트웨어 정의 무선 신호) 분석 장치				
프로토콜분석	**제품명**	Vanguard	**제조사**	Ellisys	**수량**	1식
	**내용**	2.4GHz ISM 대역 전체를 캡처하여 Bluetooth, BLE, WiFi, Zigbee, 6LoPAN 프로토콜 패킷을 실시간으로 캡처하고 분석				
프로토콜분석	**제품명**	멀티프로토콜 분석기	**제조사**	Truenetworks	**수량**	1식
	**내용**	Serial, Ethernet, Fieldbus 등 산업 네트워크에서의 데이터 및 메시지 전송 정보를 모니터링				

※ 상기 도구 구성은 변경 될 수 있음

붙임 3 IoT 보안테스트베드 교육 프로그램(안)

□ 추진 계획

o **(교육일정)** ’26. 5. 15 ~ 9. 18, 상시과정의 경우 연중

o **(교육장소)** 온라인 또는 오프라인

o **(교육대상)** IoT 관련 개발자, 대학(원)생, IoT 교육희망자 등

o **(교육과정)** 기초과정(4개), 상시과정(4개), 세미나(1개) 과정 운영

과정명		시간	일시	인원	비고
기초 과정	Ⅰ. 시큐어코딩 (sparrow)	3H	5.15, 8.21	00명	온라인/ 오프라인
	Ⅱ. IoT 디바이스 퍼징테스트 (defensics)	3H	5.22, 8.28	00명	
	Ⅲ. IoT 디바이스 펌웨어 분석 (trace32)	3H	6.5, 9.4	00명	
	Ⅳ. 오픈소스 취약점 분석 (Cybellum)	2H	6.12, 9.11	00명	
상시 과정	Ⅰ. 시큐어 코딩 분석 및 점검 도구 가이드	1일 3시간	상시	0명	오프라인
	Ⅱ. 오픈소스 취약점 분석 도구 사용법		상시	0명	
	Ⅲ. IoT 디바이스 퍼징 테스트		상시	0명	
	Ⅳ. 코딩 드론		상시	0명	
세미나	Ⅰ. 세미나 – IoT 보안인식 제고	1일 3시간	6.19, 9.18	00명	온라인

※ 제공사항 : 교육비 무료, 실습 기자재 제공(오프라인 시 주차는 1일 2시간 무료)

※ 교육방법 : 온라인을 기본으로 진행하며, 상황에 맞추어 오프라인으로 전환가능, 오프라인 장소 추후 안내

※ 교육신청 : 기초과정 및 세미나의 경우 교육일 2주 전부터 온오프믹스 (onoffmix.com), 상생누리 (winwinnuri.or.kr) 등을 통해 모집 을 통해 모집

※ 교육 세부 사용방법 및 절차 등 안내는 교육신청자 대상으로 별도 안내 예정

※ 상기 교육과정 등은 변경될 수 있으며, 변경 시 홈페이지 공지사항을 통해 안내 예정

□ IoT 보안테스트베드 교육과정(안)

o 기초과정

과정명	교육 내용	시간	방법
Ⅰ. 시큐어코딩 (Sparrow)	- SW 개발보안 정의 및 필요성 - SW 보안취약점 유형 - SW 보안취약점 점검도구 소개 - SW 보안취약점 점검도구 테스트 시연	2회 3시간	온라인/ 오프라인
Ⅱ. IoT 디바이스 퍼징테스트 (Defensics)	- 퍼징 기법 소개 - 보안 취약점 탐지 사례 - 퍼징 도구 소개 - 퍼징 도구 테스트 시연	2회 3시간	
Ⅲ. IoT 디바이스 펌웨어 분석 (Trace32)	- IoT 디바이스 디버깅 도구 소개 - IoT 디바이스 역분석 및 플래시 프로그래밍 - 소스 코드 디버깅 및 변수 확인	2회 3시간	
Ⅳ. 오픈소스 취약점 분석 (Cybellum)	- 오픈소스 개요 및 동향 - 오픈소스 라이선스 대응방안 - 오픈소스 취약점 점검 도구 소개 - 오픈소스 취약점 테스트 시연	2회 3시간	

o 상시과정 (4인 이상)

과정명	교육 내용	시간	방법
Ⅰ. 시큐어 코딩 및 소스코드 점검 도구 가이드	- 시큐어 코딩의 이해 - 점검도구 주요 기능 및 환경 설정 가이드 - 분석 수행 절차와 주요 기능 활용 - 점검 결과 해석 및 개선 방향 도출	3H	오프라인
Ⅱ. 오픈소스 취약점 분석 도구 사용법	- SBOM의 이해 - 주요 분석 기술과 작동 원리 및 주요 기능 - 오픈소스 라이브러리의 취약점 탐지와 분석 절차 - 분석 결과를 기반으로 SBOM 리포트 생성	3H	
Ⅲ. IoT 디바이스 퍼징 테스트	- IoT 디바이스 퍼징 테스트 이해 - 퍼징 사례 소개 및 도구 소개 - IoT 디바이스 퍼징 시연 - IoT 디바이스 퍼징 테스트 실습 (Bluetooth / CAN_Bus)	3H	
Ⅳ. 코딩 드론	- 드론코딩의 이해 - 드론 조정하기 - 카드코딩/모션코딩/엔트리 코딩하기 - 코딩 드론 실습	3H	

o 세미나

과정명	교육 내용	시간	방법
IoT 보안인식 제고	- 추후 안내	2회 3시간	온라인