[별지]

FADU SoC팀 실습은 아래 2가지 주제로 진행됨.

< 주제 1 : Out-Of-Band Management Protocol 구현 > 인턴희망 인원 2 명

개요: OOB(Out-of-Band) 관리는 기본 네트워크 연결과 물리적으로 분리된 보조 인터페이스를 통해 보안 프로토콜 연결을 이용하여 장치를 원격으로 제어하고 관리하는 방법입니다. OOB 관리는 OS 상태 및 장치의 전원 상태와 관계없이 관리자가 장치를 모니터링하고 제어할 수 있도록 특별히 설계한 하드웨어와 펌웨어가 필요하며 데이터 센터나 서버 군에서는 MCTP (Management Component Transport Protocol)가 널리 사용되어지고 있습니다. 해당 프로토콜은 다양한 피지컬 계층 상에서 동작 가능하도록 설계되어 있으며 해당 프로토콜을 사용하여 탑재된 디바이스들의 상태 확인이나 상태 복구를 위해 많이 사용되고 있습니다.

자격 요건

- **C 언어**: 포인터 사용 및 데이터 구조를 활용할 수 있는 중급 이상의 능력 필요 + TCP/IP 소켓 프로그래밍이 가능한 분
- **Embedded 시스템 이해**: Embedded 시스템의 구조와 원리에 대한 기본적인 이해 우대
- **Linux Application 개발 경험**: 파일 시스템, 네트워크 기능을 포함한 Linux 기반 응용 프로그램 개발 경험 우대

실습 상세

- MCTP 계층 구현 - 리눅스 상 소켓 프로그래밍 기반 서버 클라이언트 모델로 작성
- MCTP 기반 상위 프로토콜 계층 구현
- PLDM (Platform Level Data Model), NVMe-MI (Management Interface), SPDM (Security Protocols and Data Models) 등
- 다양한 커널 버전 지원을 위한 리눅스 패키지 및 python 라이브러리 작성
- 다양한 운영체제 지원을 위한 Docker 기반 테스트 환경 구축

< 주제 2 : 보안 부팅을 위한 cryptography 라이브러리 기반 응용프로그램 및 펌웨어 구현 > 인턴희망 인원 1 명

개요: Security 는 클라우드 뿐만아니라 edge device 에서도 매우 중요한 요소로 장치가 하드웨어 해킹 등으로부터 안전하게 장치가 정상적으로 부팅이 되었는지 보장하는 보안 부팅에 대한 관심이 높아져가고 있다. 이에 따라 전통적인 AES, RSA, ECDH, ECDSA 와 같은 전통적인 알고리즘 뿐만아니라 PQC(Post-Quantum Cryptography)와 같이 기존 알고리즘들의 한계를 개선하고자 하는 다양한 알고리즘들 연구/개발되고 있다. 본 주제는 이미지 암호화/복호화, 그리고 데이터 무결성을 위한 디지털 서명 등을 이용한 보안 부팅을 위한 라이브러리와 검증을 위한 테스트 케이스를 작성하는데 그 의의가 있다.

자격 요건

- **C 언어**: 포인터 사용 및 데이터 구조를 활용할 수 있는 중급 이상의 능력 필요
- **Embedded 시스템 이해**: Embedded 시스템의 구조와 원리에 대한 기본적인 이해 우대
- **Linux Application 개발 경험**: 파일 시스템, 네트워크 기능을 포함한 Linux 기반 응용 프로그램 개발 경험 우대

실습 상세

- 공개 소프트웨어 기반 보안 라이브러리(OpenSSL, WolfSSL)를 이용한 다양한 응용프로그램 작성
- 예시: 미국 국립표준기술연구소에서 배포한 검증 프로그램 인증을 위한 테스트 케이스를 이용한 동작 정확성 검증
- 공개 소프트웨어 기반 라이브러리를 이용한 ARM 또는 RISCV 기반 머신으로 이식
- 예시:미국 국립표준기술연구소에서 배포한 검증 프로그램 인증을 위한 테스트 케이스를 이용한 동작 정확성 검증