
Test Plan / Test Cases Design Document

Project Name	기밀연산 인공위성 시스템 적용
-----------------	------------------

11 조

202002558 조민성
201902711 신희성
201802076 김주호

지도교수: 장진수 교수님 (서명)

Table of Contents

1. INTRODUCTION	3
1.1. OBJECTIVE	3
2. TEST PLAN	4
3. TEST CASES	8
4. AI 도구 활용 정보	9

1. Introduction

1.1. Objective

본 문서는 “기밀연산 인공위성 시스템 적용” 프로젝트의 테스트 계획 및 테스트 케이스 명세를 포함하고 있다.

이 문서는 인공위성과 지상국 간의 PQC 기반 키 교환 시스템을 OP-TEE 환경에서 구현함에 있어 해당 기능이 의도한 대로 동작하는지 검증하기 위한 테스트 활동을 정의한다.

테스트 계획은 어떤 항목을 어떤 방법으로 테스트할지를 다루며, 테스트 케이스는 실제 시스템 기능에 대한 구체적인 검증 항목을 정의한다.

2. Test Plan

1. 배경과 목적
1.1 배경
우주라는 제한적인 환경에서 OP-TEE를 이용해 키를 안전하게 보관하고 양자컴퓨터 등장에도 PQC 알고리즘을 적용해 위성통신 간의 외부 공격을 차단하고 키 교환 시스템의 안정성과 기능성을 검증하기 위해 수행된다.
1.2 테스트 목적
본 프로젝트는 양자내성 암호(PQC) 기반의 키 교환 프로토콜을 OP-TEE 환경에서 구현하여 인공위성과 지상국 간의 안전한 통신 채널을 구축하는 것이 목적이다. 특히 REE에서만 키 교환이 이루어지고, TEE에 해당 키를 안전하게 저장하는 구조를 테스트한다.
2. 테스트 상세
2.1 테스트 항목
OP-TEE 내 TEE 어플리케이션의 정상 동작 REE ↔ TEE 간 키 전달 인터페이스 PQC 키 생성 및 교환 기능 인공위성 모사 환경에서의 통신 시뮬레이션 키 저장 후 접근 제어 기능
2.2 테스트될 요소(features)
- 요구사항 명세서에 나와 있는 시스템의 모든 기능이 테스트될 요소임 테스트 프로젝트는 다음의 요소를 테스트한다. <ul style="list-style-type: none"> • PQC 알고리즘을 통한 키 교환 기능 • 인공위성 시스템에서 OP-TEE를 이용한 키 저장 기능 • 시스템 구성 요소 간 연동 상태 점검 ...
2.3 테스트되지 않을 요소
- 해당 테스트를 실시하는데 포함되지 않을 요소를 명시함 <ul style="list-style-type: none"> • 실제 위성 통신 하드웨어 및 우주 환경에서의 성능 • 전체 시스템의 스트레스/부하 테스트 • 양자컴퓨터 공격을 직접 시뮬레이션하지 않음
2.4 접근 방법
단위 테스트: 각 기능별 PQC 구현, TEE 기능 시스템 테스트: 전체 흐름에 대한 테스트 테스트 기법: 블랙박스 테스트, 리그레션 테스트
2.5 테스트 항목의 pass/fail 기준
- 각 테스트 항목의 pass/fail 기준을 명시함 다음 각 항이 수행될 때까지 테스트는 완료된 것으로 간주하지 않는다.

<ul style="list-style-type: none"> • 단위 테스트 : PQC 알고리즘과 TEE 환경의 정상 작동을 확인해야 함. • 기능 커버리지 : 시스템 요구사항 명세서에 나와 있는 모든 기능은 수행된다는 것을 보여야 함. • 블랙 박스 테스트 : TEE가 아닌 REE 환경에서 키에 접근이 가능하면 실패로 간주한다. • 리그레션 테스트 : 시스템 오류 및 예외상황 발생이 일어나지 않아야 하고, 발생하더라도 대응이 가능해야 함.
2.6 테스트 산출물(deliverables)
<ul style="list-style-type: none"> • 테스트 계획서 • 테스트 케이스 명세서 • 테스트 수행 결과 보고서
3. 테스트 관리
3.1 작업
<p>- 테스트 프로젝트를 위해 수행할 작업을 기술함</p> <p>중요한 테스트 작업은 다음과 같다.</p> <ol style="list-style-type: none"> 1 테스트 계획을 개발한다. 2 테스트 팀을 구성한다. 3 시스템 요구 사항과 기능 명세를 검토한다. 4 테스트 케이스를 작성하고 테스트 절차를 개발한다. 5 테스트 계획, 테스트 케이스, 절차를 검토하고 승인한다. 6 상세한 테스트 계획에 따라 시스템 기능에 대하여 테스트를 수행한다. 7 발견된 결함을 보고한다. 8 결함을 수정한다. 9 수정된 내용에 대하여 재테스트 (또는 리그레션 테스트)를 수행한다. 10 테스트 결과를 문서화한다. 11 테스트 종료 조건을 기준으로 시스템을 릴리스 할 시점을 결정한다.
3.2 기술 자원
<p>- 테스트 프로젝트를 수행하는데 필요한 장비, 자동화 도구, 테스트 데이터베이스 등에 대하여 기술함</p> <p>테스트 프로젝트를 위하여 테스트 엔지니어는 OP-TEE를 구축할 수 있는 환경과 위성통신과 비슷한 환경의 가상통신망이 필요하다.</p> <ul style="list-style-type: none"> • OP-TEE가 구축된 OS 커널 • 가상의 키 • 위성통신을 대체할 수신 장비
3.3 책임과 권한 (인력 자원)
<p>- 테스트 프로젝트를 수행하는데 필요한 인력 자원과 그들의 책임과 권한을 기술함</p> <p>테스트 프로젝트를 위하여 필요한 인력은</p> <ul style="list-style-type: none"> • OS를 설치하고 테스트 키를 만들 수 있는 IT 인력 • 테스트 전문가 • 통신망을 구축하고 키 교환을 수행할 수 있는 인력
3.4 훈련
<p>- 테스트 프로젝트를 수행하는데 필요한 인력 자원의 훈련 계획을 명시함</p> <p>테스트 인력에게 시스템 테스트를 위해 간단한 테스트 교육을 실시함</p>
3.5 일정
<p>- 테스트 프로젝트를 수행하는데 필요한 기간 및 일정 계획을 명시함</p> <p>OP-TEE 환경 구축과 위성 통신 환경 구성에 2주 정도의 시간이 소요</p>
3.6 위험 요소와 비상 대처 상황
<p>- 테스트 프로젝트를 수행할 때 발생할 수 있는 위험 요소와 위험에 대한 비상 대처 상황을 명시함</p>

OP-TEE 환경과 가상통신망 구축에 시간이 걸릴 수 있으므로 해당 작업이 완료되면 테스트를 진행한다.

3. Test Cases

1. 서론																																		
1.1 테스트 범위																																		
<p>- 테스트 프로젝트의 적용 범위 및 테스트 대상에 대하여 명시함</p> <p>위성통신 환경에 OP-TEE를 적용하고 TEE 내부에 저장되어 있는 키를 PQC 알고리즘을 통해 지상국과 키 교환을 이룬다.</p> <ul style="list-style-type: none"> OP-TEE 기반 TEE 내의 PQC 키 저장 모듈 REE에서의 PQC 키 교환 요청 처리 지상국 ↔ 인공위성 간의 전체 시나리오 흐름 테스트 																																		
1.2 테스트 상황																																		
<p>- 테스트 프로젝트의 수행 상황에 대하여 명시함</p> <p>모든 팀원이 송수신 장비와 OP-TEE 환경을 가지고 테스트를 한다.</p>																																		
1.3 문서 표기법																																		
<p>- 테스트 케이스를 기술할 때 사용하는 표기법에 대하여 명시함</p> <p>특별한 표기법을 사용하지 않음</p>																																		
2. 테스트 케이스																																		
2.1 테스트 케이스 명세																																		
<p>- 요구사항 명세서에 나와 있는 시스템의 모든 기능을 테스트하여야 하며 각 기능을 테스트하기 위해 각 기능별로 테스트 케이스를 명세해야 함</p> <table border="1"> <thead> <tr> <th>Id</th><th>테스트 대상</th><th>테스트 조건</th><th>테스트 데이터</th><th>예상 결과</th></tr> </thead> <tbody> <tr> <td>TC-1</td><td>PQC 키 생성</td><td>지상국에서 키 요청</td><td>N/A</td><td>PQC 공개키/개인키 쌍 생성 성공</td></tr> <tr> <td>TC-2</td><td>키 교환 요청</td><td>REE -> TEE 전송</td><td>공개키 데이터</td><td>공개키 수신, TEE 내 저장 성공</td></tr> <tr> <td>TC-3</td><td>키 저장</td><td>TEE 내부 저장 동작</td><td>PQC 키 데이터</td><td>TEE 내 Secure Storage에 기록 확인</td></tr> <tr> <td>TC-4</td><td>접근 제어</td><td>REE에서 TEE 키 접근 시도</td><td>비인가 접근</td><td>접근 거부, 로그 기록 됨</td></tr> <tr> <td>TC-5</td><td>통신 시나리오</td><td>지상국 <-> 위성 간 시나리오</td><td>전체 키 교환 흐름</td><td>성공적인 키 교환 후 저장</td></tr> </tbody> </table>					Id	테스트 대상	테스트 조건	테스트 데이터	예상 결과	TC-1	PQC 키 생성	지상국에서 키 요청	N/A	PQC 공개키/개인키 쌍 생성 성공	TC-2	키 교환 요청	REE -> TEE 전송	공개키 데이터	공개키 수신, TEE 내 저장 성공	TC-3	키 저장	TEE 내부 저장 동작	PQC 키 데이터	TEE 내 Secure Storage에 기록 확인	TC-4	접근 제어	REE에서 TEE 키 접근 시도	비인가 접근	접근 거부, 로그 기록 됨	TC-5	통신 시나리오	지상국 <-> 위성 간 시나리오	전체 키 교환 흐름	성공적인 키 교환 후 저장
Id	테스트 대상	테스트 조건	테스트 데이터	예상 결과																														
TC-1	PQC 키 생성	지상국에서 키 요청	N/A	PQC 공개키/개인키 쌍 생성 성공																														
TC-2	키 교환 요청	REE -> TEE 전송	공개키 데이터	공개키 수신, TEE 내 저장 성공																														
TC-3	키 저장	TEE 내부 저장 동작	PQC 키 데이터	TEE 내 Secure Storage에 기록 확인																														
TC-4	접근 제어	REE에서 TEE 키 접근 시도	비인가 접근	접근 거부, 로그 기록 됨																														
TC-5	통신 시나리오	지상국 <-> 위성 간 시나리오	전체 키 교환 흐름	성공적인 키 교환 후 저장																														
2.2 테스트 환경																																		
<p>- 테스트 프로젝트를 준비, 실행하기 위해, 또는 결과를 기록하기 위해 필요한 테스트 환경을 기술함</p> <p>테스트 장비는 아래 나열한 것이 필요함.</p> <ul style="list-style-type: none"> QEMU 기반 OP-TEE 시뮬레이션 Ubuntu 22.04 LTS 개발 환경 클라이언트 ↔ 서버 간 시리얼 통신 시뮬레이션 도구 내부 테스트용 PQC 라이브러리 (예: CRYSTALS-KYBER) 																																		
2.3 테스트 절차 요구사항																																		
<p>- 테스트 케이스를 실행하기 위해 테스트 절차에 대한 제약 사항을 기술함. (예를 들어, 선행 조건, 후행 조건 또는 처리 등을 기술함)</p>																																		

OP-TEE 빌드 및 환경 구성 완료
Secure Storage 기능이 정상 작동할 것
지상국/위성 간 시뮬레이션 테스트 코드 준비

4.AI 도구 활용 정보

사용 도구	GPT-4o, Claude
사용 목적	테스트케이스 표 초안 작성
프롬프트	● PQC와 OP-TEE를 이용한 테스트케이스 표 작성해줘
반영 위치	1. 테스트케이스 표 생성 (p.7)
수작업 수정	있음(논리 보강 및 팀 목표에 맞게 수정 등)