기밀연산 인공위성 시스템 적용

종합설계 2회차

11조 - 조민성, 신희성, 김주호
지도교수 - 장진수 교수님

Table of contents

01. 기밀연산이란?

기밀연산

의미

데이터를 보호하고 암호화하여 전송 및 저장 중에도 보안을 유지하는 기술

예시

신뢰 실행 환경(TEE, Trusted Execution Environment)
종단 간 암호화(End-to-End Encryption, E2EE)
보안 다중 연산(Secure Multi-Party Computation, SMPC)
양자암호통신(Quantum Cryptography)

기밀연산의 필요성

필요성

클라우드 및 원격 서버에서의 보안 강화

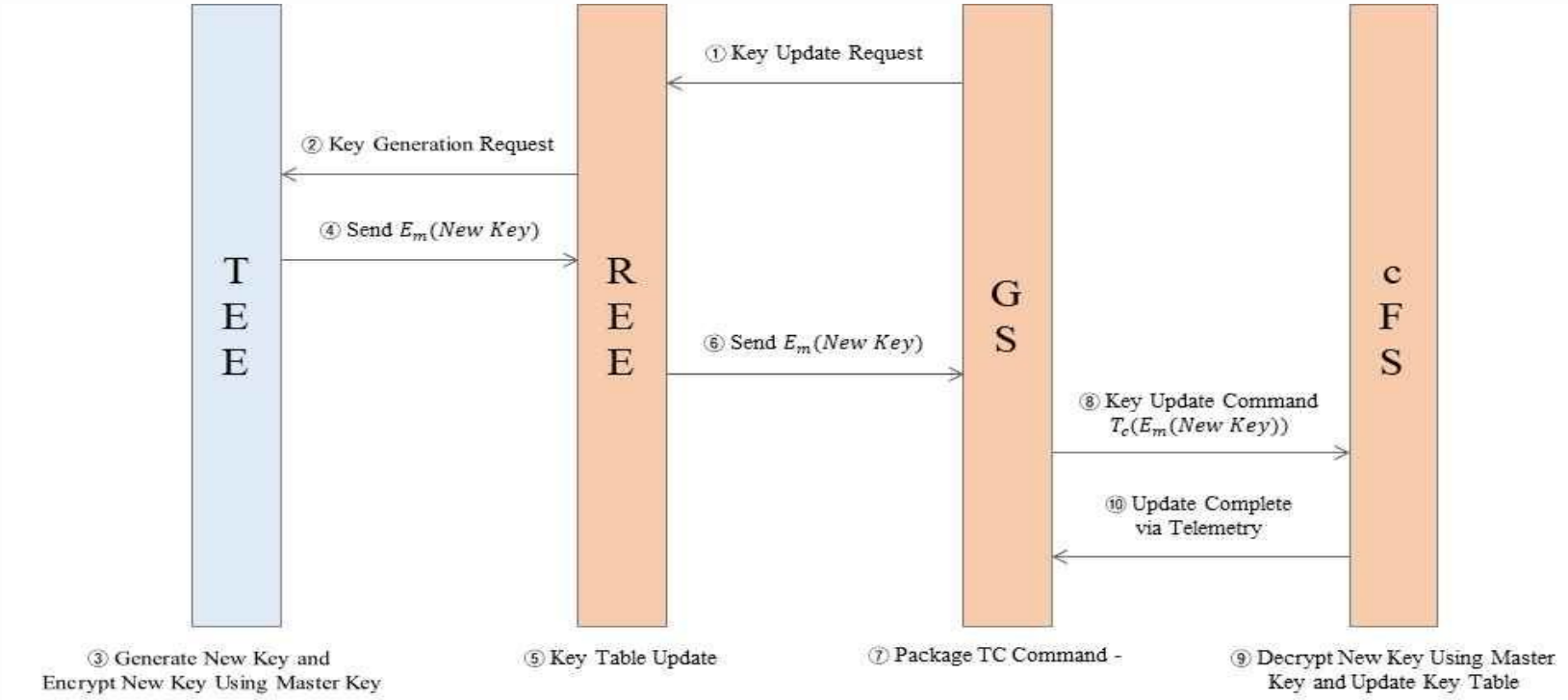
위협 예시

기업과 개인이 클라우드에 데이터를 저장하는 경우가 증가
클라우드를 제공하는 업체는 해당 데이터에 대한 높은 권한 보유
기업의 기밀 또는 개인 정보가 클라우드 제공 업체에 유출될 가능성 존재
클라우드 제공 업체가 볼 수 없는 하드웨어 기반의 보안 기술이 필요

03. 인공위성의 구조

[그림 1]

인공위성에서의 대칭키 교환 방법



[그림 2]

현재 대칭키 교환 방식의 상황

1. 위성-지상국 간 데이터 전송이 기본적으로 암호화되어 있지만, 일부 시스템은 강력한 암호화 기법 미적용

2. 위성 시스템은 소프트웨어 및 펌웨어 업데이트가 어려움으로 지연 가능성 증가

3. 군사 및 민간 위성 통신이 외부 전파 간섭(재밍)과 신호 변조(스푸핑)의 위협에 노출될 가능성 존재

4. 보안 사고 대응은 주로 지상 통제 센터에서 이루어지며, 자동화된 위협 탐지 및 대응 시스템이 제한적

현재 대칭키 교환 방식의 문제점

1. 암호화 취약점 : 일부 위성 통신이 강력한 암호화 없이 운영되어 감청 및 데이터 조작 위험이 존재

2. 사이버 공격 대응 부족 : 해킹, 재밍(Jamming), 스푸핑(Spoofing), 신호방해 등 위협이 증가하는데 방어 체계가 미흡

3. 보안 업데이트 어려움 : 위성이 우주에 있기 때문에 보안 패치를 적용하는 것이 제한적이고 지연될 가능성이 높음

4. 전자적 감시 위험 : 적국이 위성 신호를 감청하거나 위치를 추적할 가능성이 있어 군사 작전에 보안 위협이 존재

5. 레거시 시스템 : 많은 위성이 오래된 기술로 설계되어 현대의 사이버 위협에 대응하기 어려움

6. 복잡한 인프라 : 위성 시스템의 복잡성과 소프트웨어 의존도가 높아 보안 취약점이 발생 가능성 존재

실제 사례

2.4 Smart Grid 보안 피해사례

Smart Grid에 대한 연구와 보급화가 진행되고 있지만, 아직까지 보안위협에 대한 대비는 초기단계에 있다.

웜 바이러스에 의해 발전소가 가동이 중지된 사고를 예로 들었다. 2003년 1월, 원자력발전소의 사설 컴퓨터 네트워크에 슬래머 웜이 침투해 안전감시시스템이 5시간 동안 정지됐다.

Hacking과 같은 외부 요인 뿐 아니라 내부적으로 불안정한 시스템 운영으로 인한 사고도 있다. 2008년 3월, 미국 조지아주 해치(Hatch) 원자력발전소에서 운영 중인 시스템에 소프트웨어 업데이트 후 48시간 동안 가동이 중지됐다.

전력량을 측정하는 스마트 미터의 보안 취약성이 보도되기도 했다. 2009년 3월, CNN 등 외신은 스마트 미터를 통한 전력망 사이버침해 유발 가능성을 보도했다. Smart Grid의 소비자 측 설치기기인 스마트 미터를 통해 전력망에 침투할 수 있다는 가능성이 제기된 것이다.

전력망에서 악성코드가 발견돼 위험을 경고 했다. 2009년 4월, 미국전력 핵심 기반시설에 중국과 러시아 해커가 침입해 악성코드 설치된 것을 보도했다. 유사시에 미국 전력망을 마비시키는 것이 목적으로 추정됐다. 톰 도나휴(전 CIA 수석분석가)는 2008년 1월, 'Process Control Security Summit'에서 인터넷을 통한 침입으로 여러 국가에서 정전 사태가 발생했다고 발표 됐다. 부시대통령 재임 시 대통령 직속 국가정보국장인 마이크 맥코넬은 브라질에서 2005년 3개 도시, 2007년 수십 개의 도시에서 Hacking으로 인한 정전이 발생해 2007년 정전에서는 7개의 철광석 공장이 멈춰 700만 달러 이상의 피해가 발생 했다.

05. 기밀연산 적용시 기대

기밀연산 적용시 기대 결과

위성 및 지상국 간 인증**(Authentication)** 강화

- OP-TEE를 사용하면 공격자가 위성을 가장하여 가짜 키 교환을 수행하는 위협(스푸핑 공격)을 방지 가능
- 예를 들어, 디지털 서명(Digital Signature) 및 HMAC 기반 인증을 OP-TEE 내부에서 실행하면 보다 신뢰성 높은 키 교환을 수행 가능

키 교환 과정의 기밀성**(Confidentiality)** 강화

- 대칭키를 교환하는 과정에서 OP-TEE를 이용하면, 키가 메모리나 시스템 외부로 노출될 가능성이 감소
- TrustZone 내에서 키를 생성 및 저장하고, OS나 다른 애플리케이션이 직접 접근할 수 없도록 보호 가능
- MITM(Man-in-the-Middle) 공격이나 재전송 공격의 위험을 최소화 가능

기밀연산 적용시 기대 결과

키 저장소 보호**(Key Storage Protection)**

- 인공위성 내부 또는 지상국에서 OP-TEE를 사용하면, 대칭키를 안전한 스토리지에 저장 가능
- 일반 OS 영역(Non-secure world)에서 접근할 수 없기 때문에 키 유출 위험이 현저히 감소
- 하드웨어 기반 보안(HSM, TPM)과 유사한 효과를 제공하며, 물리적인 보안 위협에도 보안 강화

중간자 공격**(MITM)** 및 재전송 공격 방지

- OP-TEE를 활용하면 대칭키를 키 교환 프로토콜과 함께 보호 가능
- 예를 들어, Nonce(임의 난수) 및 타임스탬프 기반 인증을 OP-TEE 환경에서 처리하면 키 교환 시 재전송 공격을 차단 가능

출처

그림1, 2) 서홍석, 인공위성 시스템 암호 통신 향상을 위한 TEE 적용 방안, 충남대학교 대학원 논문, 2024.

참고 문헌) 박대우, 신진, "Smart Grid 기술에 대한 Hacking 공격과 보안방법", 한국컴퓨터정보학회하계학술대회 논문집, 2011.

Thanks!

CREDITS: This presentation template was created by **Slidesgo,** and includes icons, infographics & images by **Freepik**

https://github.com/isord/satellite_OPTEE/tree/week1