제128회 정보관리기술사 해설집

2022.07.02

국가기술자격 기술사 시험문제

기술사 제 128 회 제 4 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 10 점)

1. 최근 NFT(Non-Fungible Token) 시장의 활성화 및 생태계 형성의 견인차인 NFT 마켓 플레이스가 해커들의 주요 타겟이 되고 있다. 대형 거래소인 OpenSea 의 보안 침해사례를 기반으로 NFT 특성과 NFT 마켓 플레이스에서의 보안 취약점을 설명하시오.

2. 웹서버의 안전한 운영을 위해 다양한 방안을 고려할 수 있다. 다음을 설명하시오.

가. 리버스 프록시(Reverse Proxy)의 개념, 동작원리, 설정방법

나. DDoS 사이버대피소

3. 6G 이동통신을 위한 위성-상공-지상 통합형 무선 네트워크(Satelite-Aerial-Terrestrial Integrated Network, SATIN)에 대하여 다음을 설명하시오.

4. 최근 정보통신의 발전으로 인해 도감청이 불가능한 양자암호통신에 대한 관심이 높아지고 있다. 양자암호통신에 대하여 다음을 설명하시오.

가. 양자암호통신의 암호키 분배방식

나. 양자암호통신의 주요 기술

다. 양자암호통신의 취약점

5. 데이터베이스의 병행제어(Concurrency Control)에 대하여 다음을 설명하시오.

가. 병행제어의 정의

나. 병행제어의 기법의 종류

다. 병행제어의 문제점

6. 식별(Identification)과 인증(Authentication)에 대하여 다음을 설명하시오.

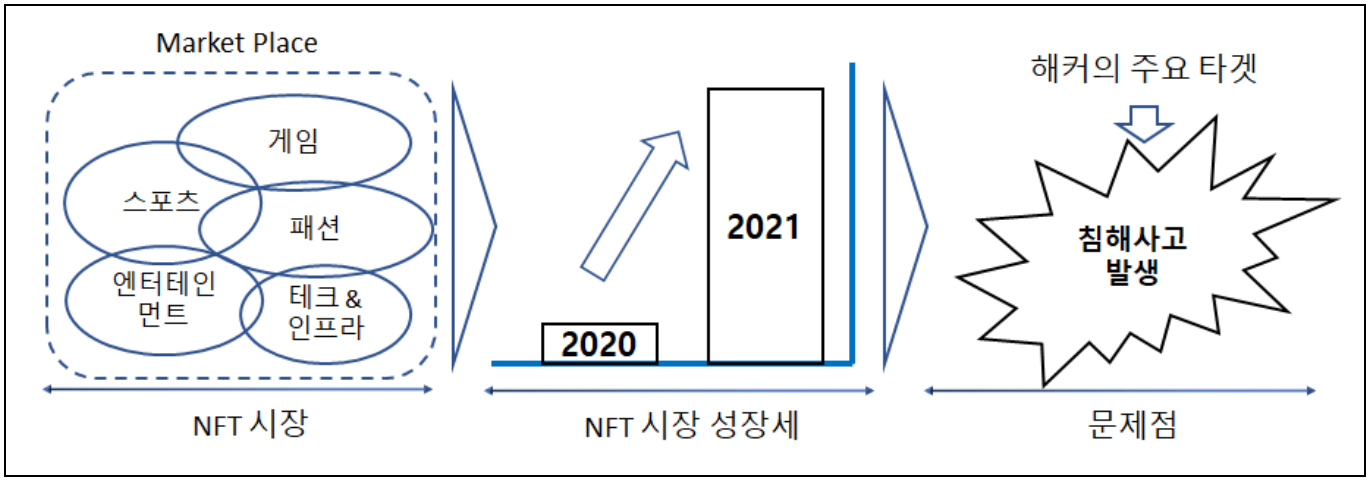
가. 개인 식별과 사용자 인증의 정의 및 차이점

나. 사용자 인증 시 보안 요구사항

다. 인증 방식에 따른 4 가지 유형 및 유형별 특징

01	NFT(Non-Fungible Token) 보안 취약점		
문제	최근 NFT(Non-Fungible Token) 시장의 활성화 및 생태계 형성의 견인차인 NFT 마켓 플레이스가 해커들의 주요 타겟이 되고 있다. 대형 거래소인 OpenSea의 보안 침해사례를 기반으로 NFT 특성과 NFT 마켓 플레이스에서의 보안 취약점을 설명하시오.		
도메인	보안	난이도	상 (상/중/하)
키워드	피싱, 프론트엔드 취약점, 데이터 유출		
참고문헌	http://www.thescoop.co.kr/news/articleView.html?idxno=53720 https://newdaycrypto.com/ko/opensea-nft-marketplace-switches-to-seaport-protocol/ 국내 NFT 거래의 보안 위협요소에 관한 연구 (2022.04.28)		
풀이기술사	NS반 백기현 기술사(제 122회 정보관리기술사 / onlyride@naver.com)		

I. NFT 시장 활성화와 생태계 형성의 견인차 NFT 마켓 플레이스의 보안의 필요성



- 지는 2월 세계 최대 NFT 거래소 OpenSea에서 피싱 공격을 당해 총 254개의 NFT가 도난당하는 침해사고가 발생이 되었고, 데이터 유출 등 해커들의 주요 타겟이 되고 있어 보안성 확립 중요성이 대두되고 있음

II. NFT 마켓플레이스 보안 침해사례로 보는 NFT의 특성

가. 마켓 플레이스 구성 측면의 NFT의 특성

구분	특성	설명
트랜잭션	- 보안성	- 블록체인 기반으로 위변조가 불가능하고 신뢰성 있는 트랜잭션 증명이 가능
	- 투명성	- 거래관계를 투명하게 공개하고, 소유권 증명에 용이
거래측면	- 분산원장	- 거래기록 및 데이터가 네트워크 참여자에게 모두 공유
	- 스마트 컨트랙트	- ERC721 또는 ERC1155 등 표준을 따름으로써 대체 불가능한 토큰을 구현하고 컨트랜트 간의 상호운용성을 확보하여 쉽게 거래
고유성	- 가치 산정된 토큰	- 가상자산과 콘텐츠 성격을 모두 가지는 가치가 산정되는 토큰
	- 데이터 인코딩	- 데이터를 16진수 값으로 숫자화하여 NFT의 고유성을 입증

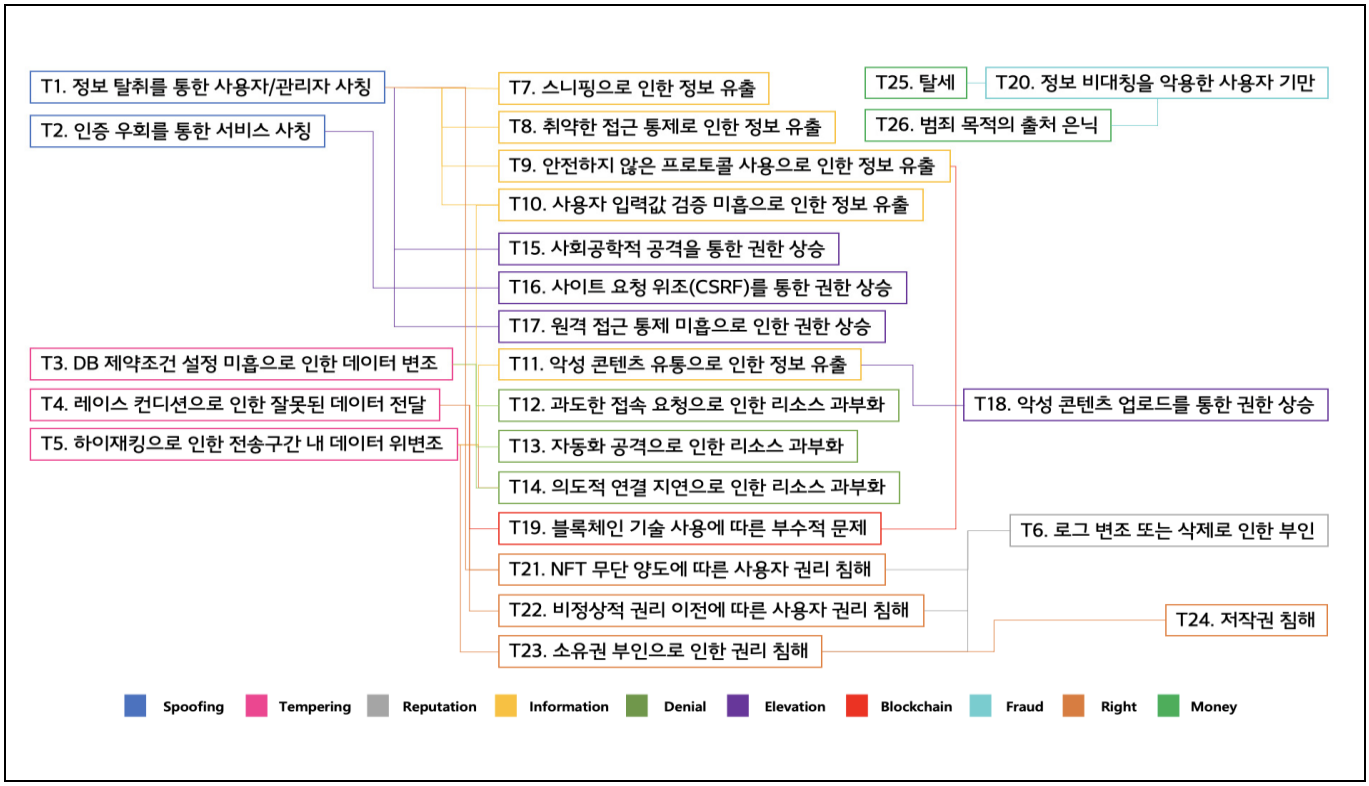
나. 마켓 플레이스 유형 측면의 NFT의 특성

구분	특성	설명
로그인 방식	- 암호화폐 지갑연동	- 메타마스크와 같은 지갑 어플리케이션 로그인을 통해 사용자 증
	- ID, PW 사용	- 일반적인 웹사이트처럼 회원가입 후 ID, PW으로 사용자 인증
중앙화 방식	- 중앙화	- 사용자들의 콘텐츠를 중앙화된 플랫폼에서 보관하고 콘텐츠 거래 및 생성 감독/심사 등 관리 기능을 지원
	- 탈중앙화	- 콘텐츠를 사용자 개인 스토리지 또는 클라우드, IPFS에서 보관하고, 거래내역 기록 등 중개 역할에 집중
NFT 민팅자격 방식	- 크리에이터 자격	- 유명인, 아티스트 등 특정한 크리에이터 자격을 갖춘 사람만 NFT 생성 가능
	- 자격없음	- 사용자 누구나 콘텐츠를 창작/등록 및 NFT 생성 가능

- NFT가 가치를 가지는 토큰의 특징을 가지고 있어 마켓 플레이스가 해커의 주요 타겟으로 부각이 되고있음

III. NFT 마켓 플레이스에서의 보안 취약점

가. 마켓 플레이스에서 NFT 거래 보안 취약점



- NFT 보안 취약점 관계에 대한 도식화로 연계성 확인이 가능

나. 마켓 플레이스에서 보안 취약점 유형 상세 설명

구분	보안취약점	설명
사용자	Spoofing Identity (신원 도용)	- 타인의 계정을 이용하여 시스템 권한 획득
	Fishing (피싱)	- 사용자의 정보를 가로채 거래를 탈취
	Sniffing (스니핑)	- 인증 우회를 통한 서비스 사칭
플랫폼 서비스	Tempering with data (데이터 변조)	- 데이터 또는 코드 변조
	Repudiation (부인)	- 작업 수행에 대한 부인
	Information Disclosure (정보 유출)	- 권한이 없는 사용자에게 정보 제공
	Denial of Service (서비스 거부)	- 서비스 거부 또는 정상적인 서비스 제공 방해
	Elevation of Privilege (권한 상승)	- 권한이 없는 자가 권한을 부여받아 서비스 수행
블록체인	Blockchain Dependency (블록체인 의존성)	- 블록체인 기술 사용으로 인한 부수적 위협
	Fraud (사기)	- 정보의 비대칭성을 이용한 사기 또는 기만 행위
	Right Infringement (권리 침해)	- 안전과 투명성이 보장되는 거래에 대한 권리침해
	Money Laundering (자금세탁)	- NFT 특징을 이용한 범죄 가능성
	Oracle Problem (오라클 문제)	- 비정상 거래 승인, 데이터 위·변조 등 신뢰성문제

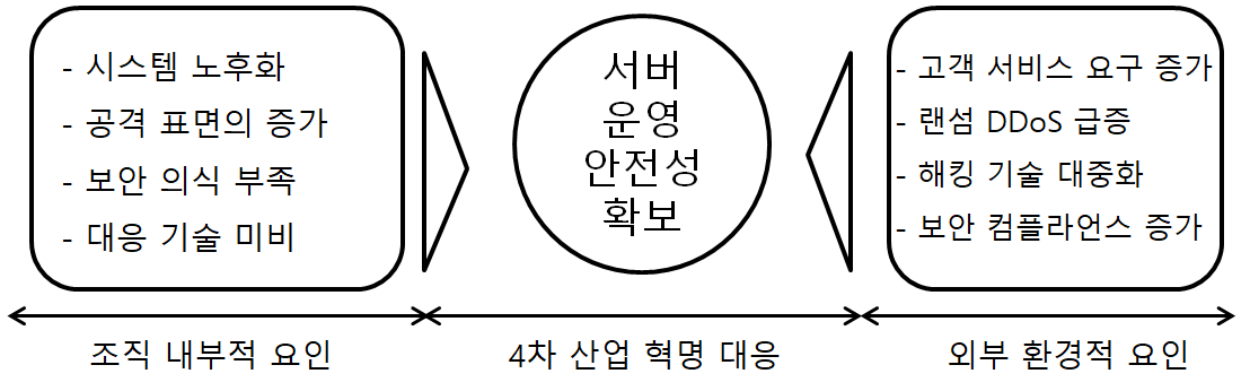
IV. 마켓 플레이스에서 보안 강화를 위한 방안

구분	방안	세부 방안	설명
사용자	2차 인증	- 휴대전화, 생체인식, OPT	- 개인정보를 이용한 2차인증 적용
	디바이스 보안강화	- OS 패치 - 취약점 점검	- 최신 OS 패치, 주기적인 업데이트 - 백신을 사용해 주기적인 취약점 점검
플랫폼 서비스	플랫폼 관리	- 거버넌스 구축	- 마켓 플레이스를 관리 및 통제를 위한 거버넌스 구축
	권한 관리	- 접근 제어	- 사용자 접근에 대한권한 관리
	취약점 점검	- 플랫폼 취약점 점검	- 모의해킹, 시큐어 코딩, 정적·동적 검사
	네트워크 보안	- 네트워크 보안	- IPS, IDS, Anti DDoS, WAF 관리
블록체인	Smart Contract 보안 강화	- Smart Contract 업그레이드	- Smart Contract 보안성 패치 - Smart Contract Audit을 통해 S/W 취약점 점검
	분산형 오라클	- 분산원장 오라클 서비스	- 분산원장 시스템 외부에 있는 데이터를 안전하게 분산원장 시스템 내부로 가져오는 서비스
기타	규제와 투자자보호정책	- 규제 - 투자자보호조치	- 시장의 성장을 규제가 못 따라가 투자자 보호가 되지 않고 있어 보호조치 및 규제가 병행이 필요

"끝"

02	리버스 프록시(Reverse Proxy), DDoS 사이버대피소		
문제	웹서버의 안전한 운영을 위해 다양한 방안을 고려할 수 있다. 다음을 설명하시오. 가. 리버스 프록시(Reverse Proxy)의 개념, 동작원리, 설정방법 나. DDoS 사이버대피소		
도메인	보안	난이도	중 (상/중/하)
키워드	트래픽, 라우팅, 보안 강화, 부하 분산, DDoS, KISA, 사이버 대피소, 중소기업 무료지원 서비스		
참고문헌	ITPE 기술사회 자료 참고 https://www.kisa.or.kr/1020202		
풀이기술사	NS반 차상인 기술사(제 125회 정보관리기술사 / itpe.ince@gmail.com)		

I. 4차 산업 혁명 대응 위한 웹서버 안전적 운영의 중요성 부각 배경

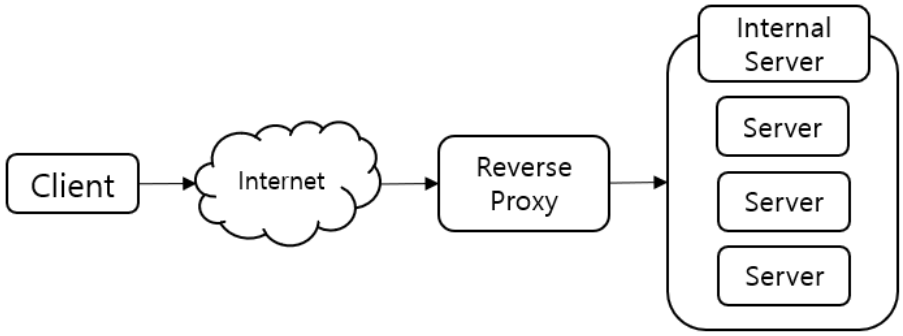


부각 배경	- 4차산업혁명과 함께 모든 사물과 인터넷이 연결되는 '초연결','클라우드' 기반 사회에서의 증가하는 사이버 범죄 피해 및 보안 컴플라이언스 대응을 위해 조직의 보안 혁신 필요

- 내부 자원 보호를 위한 간편 기술로 리버스 프록시 서버를 이용한 방법 존재

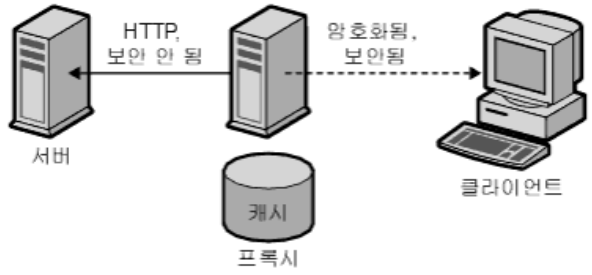
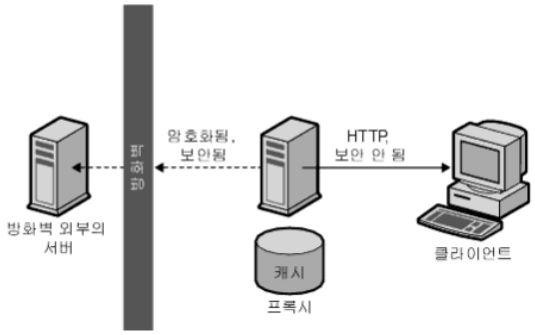
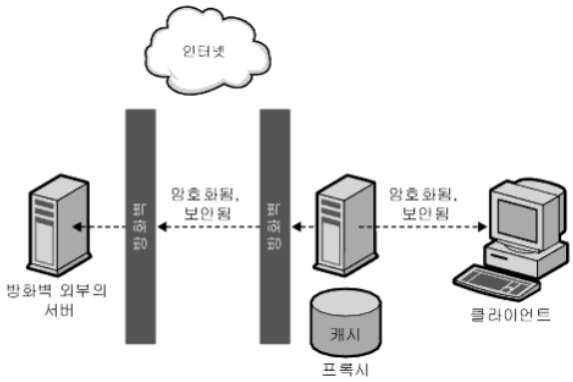
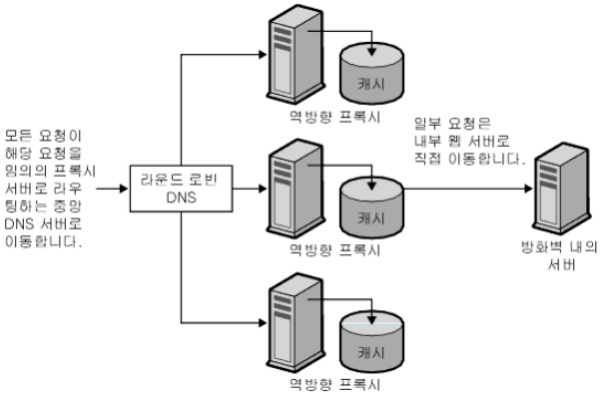
II. 내부 자원의 보안 강화 위한, 리버스 프록시

가. 리버스 프록시의 개념

구분	설명
개념	- 클라이언트가 특정 서버에 데이터 요청 시, 해당 서버에 대한 요청이 반드시 경유하도록 설치된 프록시 서버
개념도	

특징	보안 강화	- 서버에 대한 정보 은닉 및 접근 차단을 위한 방어 역할
	부하 분산	- 여러 서버로 부하를 분산하거나 데이터 버퍼링 역할
	성능 향상	- 캐싱 기능과 트래픽 분산 기능을 결합시켜 전반적인 서버 서능 향상

나. 리버스 프록스의 동작원리

구분	개념도	동작원리
보안 프록시		- 보안 클라이언트에서 프록시 연결
		- 보안 프록시에서 컨텐트 서버 연결
		- 보안 클라이언트에서 프록시 연결 및 보안 프록시에서 컨텐트 서버 연결
로드 밸런싱 프록시		- 한 조직 내에서 여러 프록시 서버를 사용하여 웹 서버 간의 네트워크 로드를 밸런싱

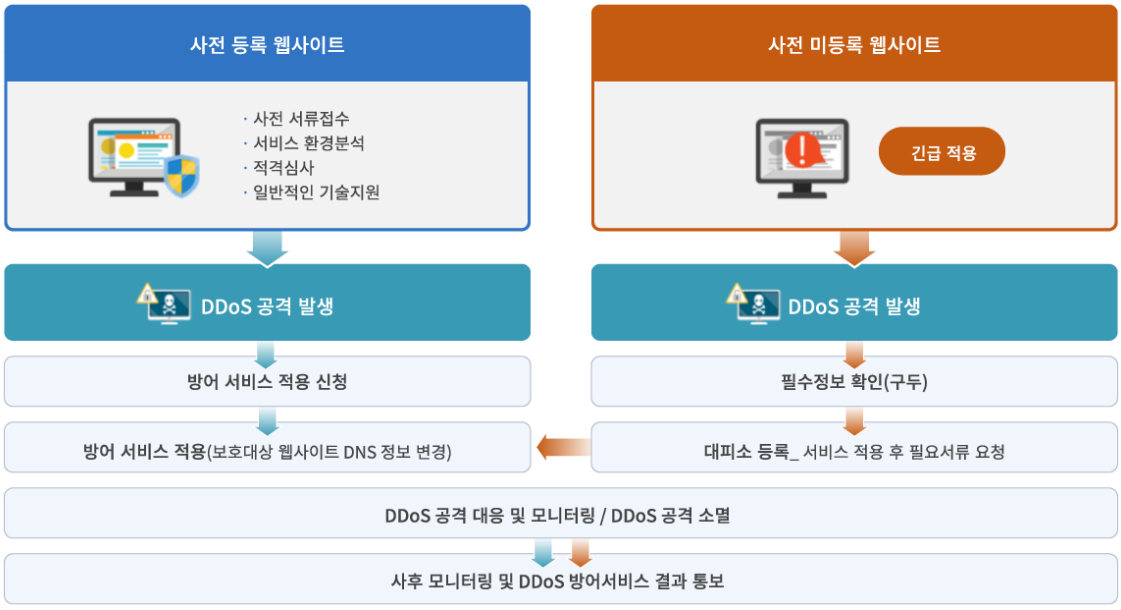
다. 리버스 프록시의 설정방법

구분	설정 방법	설명
매핑 방법	정상 매핑	- 클라이언트 요청을 타겟 서버로 재지정 - 프록시 서버는 정상매핑 이용 데이터 접근
	역방향 매핑	- 데이터 접근 재지정 위한 서버 트랩 생성 - 변경된 URL 정보를 프록시 서버 재지정
설정 정보 변경 방법 (Nginx기준)	proxy_pass	- 들어온 요청을 어디로 포워드 해줄지 설정 - URL 형태로 작성
	proxy_http_version	- 리버스 프록시를 위한 HTTP 프로토콜 버전을 정의 - 기본 값은 1.0
	proxy_redirect	- 백엔드 서버에 의해 촉발된 리다이렉션에 대해 로케이션 HTTP 헤더에 나타나는 URL을 재작성
	proxy_set_header	- 실제 서버에 전달해야할 헤더 값을 정의

- 리버스 프록시를 이용해 DDoS 트래픽을 DDoS 사이버 대피소로 라우팅해 보호가 가능

III. 중소기업 DDoS 방어 무료 지원서비스, DDoS 사이버 대피소

가. DDoS 사이버 대피소의 개념

구분	설명
개념	- 사이버대피소는 피해 웹사이트로 향하는 DDoS 트래픽을 대피소로 우회하여 분석, 차단함으로써 정상적으로 운영될 수 있도록 하는 중소기업 무료지원 서비스
서비스 이용 절차	
서비스대상	- "중소기업기본법 제2조" 및 "중소기업기본법 시행령 제3조"에 해당하는 중소기업
서비스 이용기간	- 방어 서비스 적용 후 1개월 - 재공격이 예상되는 경우 지속적으로 1개월 연장

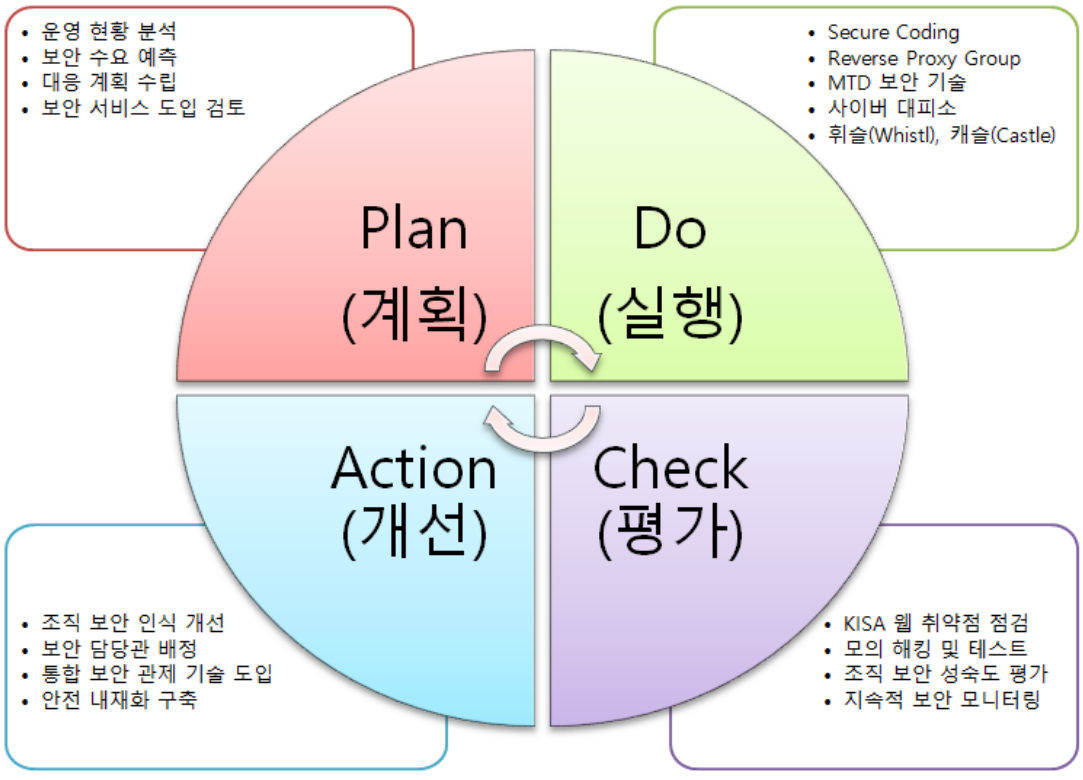
- 전체 500Gbps 규모의 연동망으로 대규모 공격 방어 가능, 24시간 365일 대응 통한 서비스 안전성 확보

나. DDoS 사이버 대피소 서비스의 DDoS 대응기법

구분	확인사항	설명
관리적 측면	HTTP 계열 방어정책	- X-Forwarded-For 설정으로 식별된 IP에 대해 60초 기준 1개 IP에서 같은 URL을 100회 요청시 60분간 차단되며, 임계치 임의 수정 가능
	WhiteList 관리	- 관리자 IP 혹은 지속적으로 요청이 많은 정상적인 URL 및 IP 기반의 예외 설정
	이상행위 IP 관리	- 웹서버 구간 내 이상행위 시도 좀비PC IP에 대한 사이버대피소 방어 서비스 인입 구간 차단 설정
기술적 측면	DNS 정보 변경	- DNS CNAME처리 또는 DNS A Record 변경 통해 해외에서 유입되는 트래픽의 차단
	CACHE 적용	- 정적 컨텐츠인 멀티미디어 파일 확장자의 경우 캐시 서비스 통해 속도 저하 문제 대응
	부하분산	- Least Connection 방식의 Load Balancing 기술 적용

- 국제적 협력 통한 대역폭 소진, 자원 소진, 웹/DB 부하 공격 별 대응 기법 및 노하우 공유

IV. 중소기업의 조직 웹서버 운영 안전성 확보를 위한 대응 방안



대응 방안	- 내부 자원의 보호 위한 기술적, 관리적, 물리적 보안 기술 도입 및 KISA 제공 각종 보안 강화 서비스를 적극적으로 이용하여 안정적 운영을 도모

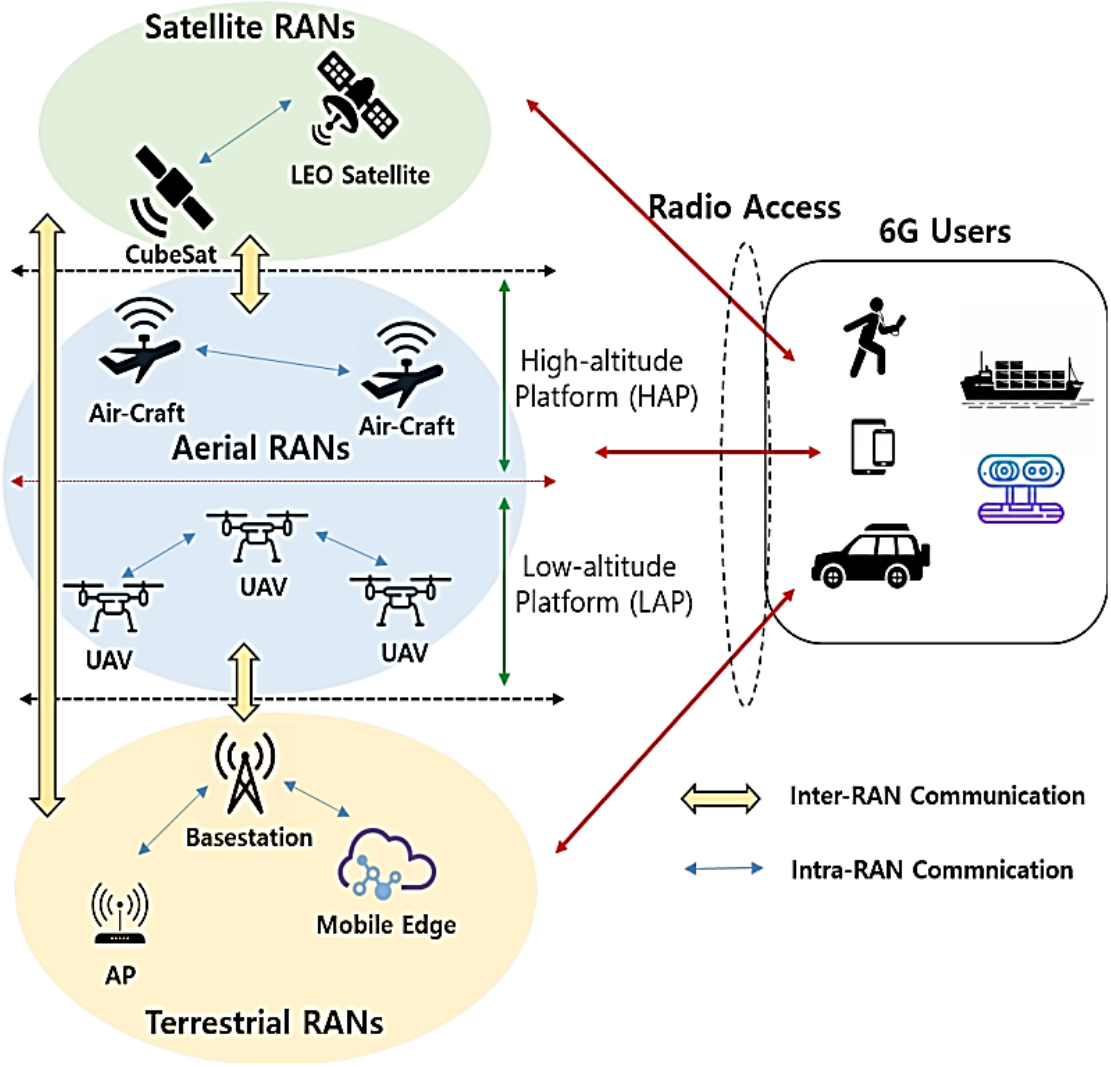
- KISA에서 제공하는 중소기업 침해사고 발생 시 원인분석 및 재발방지 위한 원인제거, 예방컨설팅, 보안교육 지원 등에 대한 적극적 참여 필요

"끝"

03	SATIN(Satellite-Aerial-Terrestrial Integrated Network)		
문제	6G 이동통신을 위한 위성-상공-지상 통합형 무선 네트워크(Satellite-Aerial-Terrestrial Integrated Network, SATIN)에 대하여 다음을 설명하시오. 가. SATIN의 개념 및 네트워크 특징 나. SATIN의 재난대비, UAV(Unmanned Aerial Vehicle) 활용, 낙후지역 네트워크 서비스에 활용방법		
도메인	네트워크	난이도	상 (상/중/하)
키워드	Satellite RANs, Aerial RANs, Terrestrial RANs, 스마트 농업		
참고문헌	6G 이동통신을 위한 위성-상공-지상 통합형 무선 접속 네트워크 연구(나웅수 공주대학교)		
출제자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / nikki6@hanmail.net)		

I. SATIN(Satellite-Aerial-Terrestrial Integrated Network) 의 개념 및 네트워크 특징

가. SATIN(Satellite-Aerial-Terrestrial Integrated Network) 의 개념



- 위성망의 역할을 상공망과 지상망이 협력하여 보완적인 커버리지를 제공해 효율적인 방송 및 멀티캐스팅 서비스를 가능케하는 프로젝트

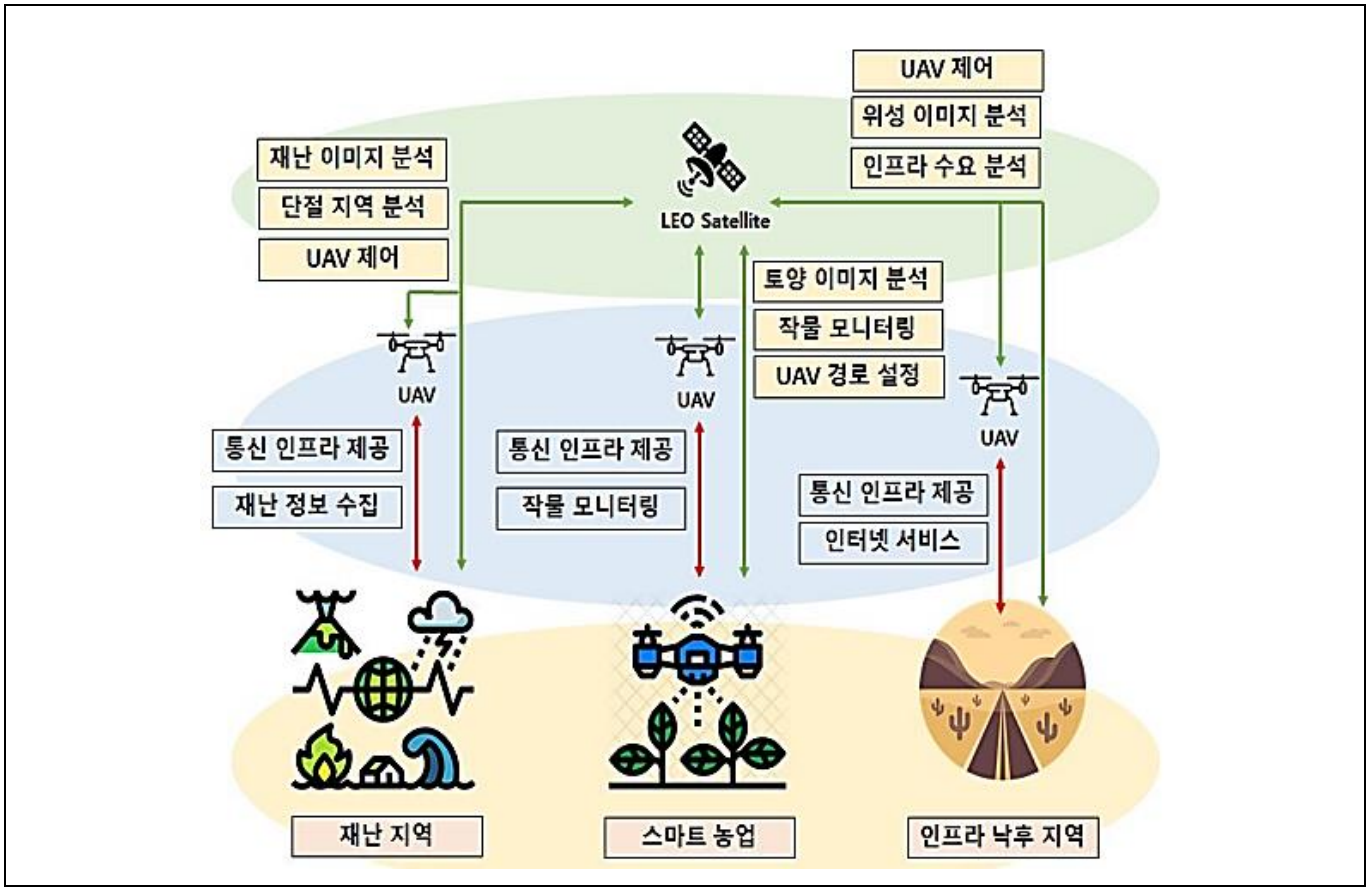
나. SATIN(Satellite-Aerial-Terrestrial Integrated Network) 의 특징

구분	주요 특징	세부 내용
Technical Factor	다중 접속 제어 (Multiple Access Control)	- SATIN 시스템에서는 네트워크 커버리지가 늘어나면서 동시에 망에 접속하는 유저의 수가 기하급수적으로 늘어남
	인지 스펙트럼 활용 (Cognitive Spectrum Utilization)	- 현재 저주파 대역의 스펙트럼 자원은 매우 제한적이고 6G의 요구사항을 만족하기에는 부족한 상황이기 때문에 고주파 대역의 주파수 자원을 활용하는 것은 앞으로 필수적
Administrative Factor	공동 간섭 및 자원 관리 (Joint Interference and Resource Management)	- 지상, 상공, 위성 RAN의 고유한 특성으로 인해 각 세그먼트의 특성을 고려한 SATIN 공동 자원 스케줄링은 단일 RAN보다 훨씬 정교하게 수행
	이동성 관리 (Mobility Management)	- SATIN 구조에서는 지상국에서 UAV로, 지상국에서 위성으로 등의 다양한 종류의 핸드오버가 많이 발생 - 원활한 사용자 QoS/QoE와 효율적인 리소스 활용을 보장하기 위해서는 더 정교하고 효율적인 핸드오버 기술이 반드시 필요

- 이러한 특징은 결과적으로 SATIN은 재난대비, UAV 활용 지원, 낙후지역 네트워크 등 광범위한 신규 어플리케이션 및 서비스를 지원할 수 있음

II. SATIN의 재난대비 활용방법

가. 재난대비, UAV 활용, 낙후지역 서비스 구성도



나. SATIN의 재난대비 활용방법 시나리오

구분	항목	세부 내용
기존 문제점	무선통신 인프라에 매우 의존적	- 한 지역에서 대규모의 재난이 발생하면 통신 인프라가 심각하게 손상되어 제 기능을 하지 못하는 문제가 빈번히 발생
	실시간 정보 획득 제한	- 재난 환 경에서 발생하는 수많은 네트워크 트래픽을 처리하기 위한 기술 들이 부족
SATIN 활용 시나리오	재난 UAV 배치	- 기지국 기능을 제공함과 동시에 상공 RAN의 자원을 활용하여 안정적인 통신 링크를 제공
	LEO 위성 시스템을 활용한 위성 이미지 분석	- 재난 감지 정확도를 향상시켜 재난에 신속하고 시기 적절하게 대응

- 이러한 통합형 SATIN 구조는 장애 감지, 장애 복구 등을 보장할 수 있는 구조로 큰 가능성을 지니고 있음

III. SATIN의 UAV 활용 및 낙후지역 네트워크 활용방법

가. SATIN의 UAV(Unmanned Aerial Vehicle) 활용 시나리오

구분	세부 내용	
주요 시나리오	- SATIN 구조에서는 상공 및 위성 영역에서의 이동 객체가 미리 정의된 경로를 따라 이동하며 사용자에게 주어진 기간 동안 네트워킹 서비스를 제공할 수 있는 시나리오가 가능	
주요 특징	최신 기술과의 융합	- 빅데이터, 머신러닝 및 UAV와 같은 최신 정보 통신 기술을 농업 운영에 통합
	잠재적 응용분야 활용	- 농부들은 농작물의 비료 살포 뿐만 아니라 농작물 모니터링 및 질병 감지를 포함한 많은 기능을 UAV를 활용하여 수행

나. SATIN의 낙후지역 네트워크 서비스 활용 시나리오

구분	세부 내용	
핵심 시나리오	- SATIN 구조는 낙후된 지역에 네트워크 서비스를 전달 할 수 있는 중요한 기술 중 하나 - UAV는 시스템 용량을 전반적으로 향상시킬 수 있을 뿐만 아니라 일시적 배치로 인해 상공 RAN을 형성하여 릴레이 역할을 수행	
주요 특징	속도 개선	- UAV는 매크로 셀과 스몰 셀의 사용자를 연결하기 위한 중간 링크의 역할을 수행 - 최근 연구결과에 따르면 UAV 지원이 없는 시스템과 비교 했을 때 최대 38%의 네트워크 효율성을 개선하였고 지연을 최대 37.5% 감소
	넓은 대역폭	- 지상 기지국 및 LEO 위성 통신과 협력하여 인구 밀도가 낮은 지역(숲, 사막, 바다 등)에 인터넷 서비스를 제공하기 위한 넓은 범위를 커버

- 현재 여러 표준화 단체에서 SATIN의 유즈케이스, 요구사항, 기술적 이슈 등의 관점에서 활발하게 논의를 하고 있음

IV. SATIN 표준화 및 산업동향

표준화 단체	세부 내용
3GPP	- 유즈케이스 및 요구사항에 대한 연구를 시작 - 지상, 상공, 위성 RAN의 통합을 위한 잠재적 솔루션을 조사 및 R16의 일부로 상공 RAN을 5G망에 통합하려는 연구가 진행중
ETSI (European Telecommunications Standards Institute)	- 2018년 말까지 위성과 고궤도 플랫폼 (HAP) 스테이션을 5G로 통합하기 위한 잠재적 아키텍처를 완성 - 위성 멀티캐스트를 통해 5G용 에지 콘텐츠 전송 작업을 하고 있으며, 향후 위성 통신 시스템에 NFV 프레임워크를 도입할 계획
재난 UAV 배치	- 기지국 기능을 제공함과 동시에 상공 RAN의 자원을 활용하여 안정적인 통신 링크를 제공

- ITU(International Telecommunication Union)는 위성 기술을 차세대 액세스 시스템 통합 진행 예정이며, IMT-2020 네트워크에서 NTN 통합에 대한 권장 사항을 작업 중

"끝"

04	양자암호통신		
문제	최근 정보통신의 발전으로 인해 도감청이 불가능한 양자암호통신에 대한 관심이 높아지고 있다. 양자암호통신에 대하여 다음을 설명하시오. 가. 양자암호통신의 암호키 분배방식 나. 양자암호통신의 주요 기술 다. 양자암호통신의 취약점		
도메인	보안	난이도	중 (상/중/하)
키워드	양자중첩, 얽힘, 불확정성, 양자키, QKD, QKE, 양자채널, 공공채널, 기저, 편광필터, 중간자 공격		
참고문헌	양자암호통신 기술(노태곤외 5, 전자통신동향분석 제20권 제5호, 05.10) ITPE 제2회 실전 명품모의고사 해설집		
풀이기술사	안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 양자의 중첩, 얽힘 특성을 이용한 양자암호통신의 개요

가. 양자암호통신의 개념

구분	설명	
개념	- 양자의 특성인 양자 중첩, 얽힘, 불확정성 등 양자역학원리를 이용하여, 암호화키를 송/수신부에 분배하고, 이를 통해 암호화 통신을 진행하는 암호통신기술	
특징	1) 양자특성이용	- 양자의 중첩, 얽힘, 불확정성 등의 양자역학원리 이용
	2) 양자키 분배	- 양자채널 및 공개채널을 이용하여 비밀키 분배 생성

나. 양자의 특성

항목	설명
양자 중첩	- 여러 상태가 확률적으로 하나의 양자에 동시에 존재하고 측정하기 전까지 정확한 양자 상태를 알 수 없는 특성
양자 얽힘	- 둘 이상의 양자가 가지는 비고전적 상관관계로 두양자가 멀리 떨어져 있어도 존재하는 특성
불확정성	서로 다른 물리량을 동시에 정확하게 측정이 불가한 것으로, 양자 암호 통신에서 복제가 불가능하다는 것을 증명해 주는 특성

- 양자암호통신은 양자의 중첩, 얽힘, 불확정성을 이용하여 구현함.

II. 양자암호통신의 암호키 분배방식

가. 양자암호통신의 암호키 분배방식 BB84프로토콜 개념

개념	- 0비트의 상태를 나타내는 편광 2가지와 1비트의 상태를 나타내는 편광 2가지를 정의한 다음 십자필터와 대각필터를 통해 측정함으로써, 안전하게 키를 교환하는 방법
특징	1) 기저와 편광필터 통해 양자키 교환 2) 도청에 시도에 대한 감지 폐기

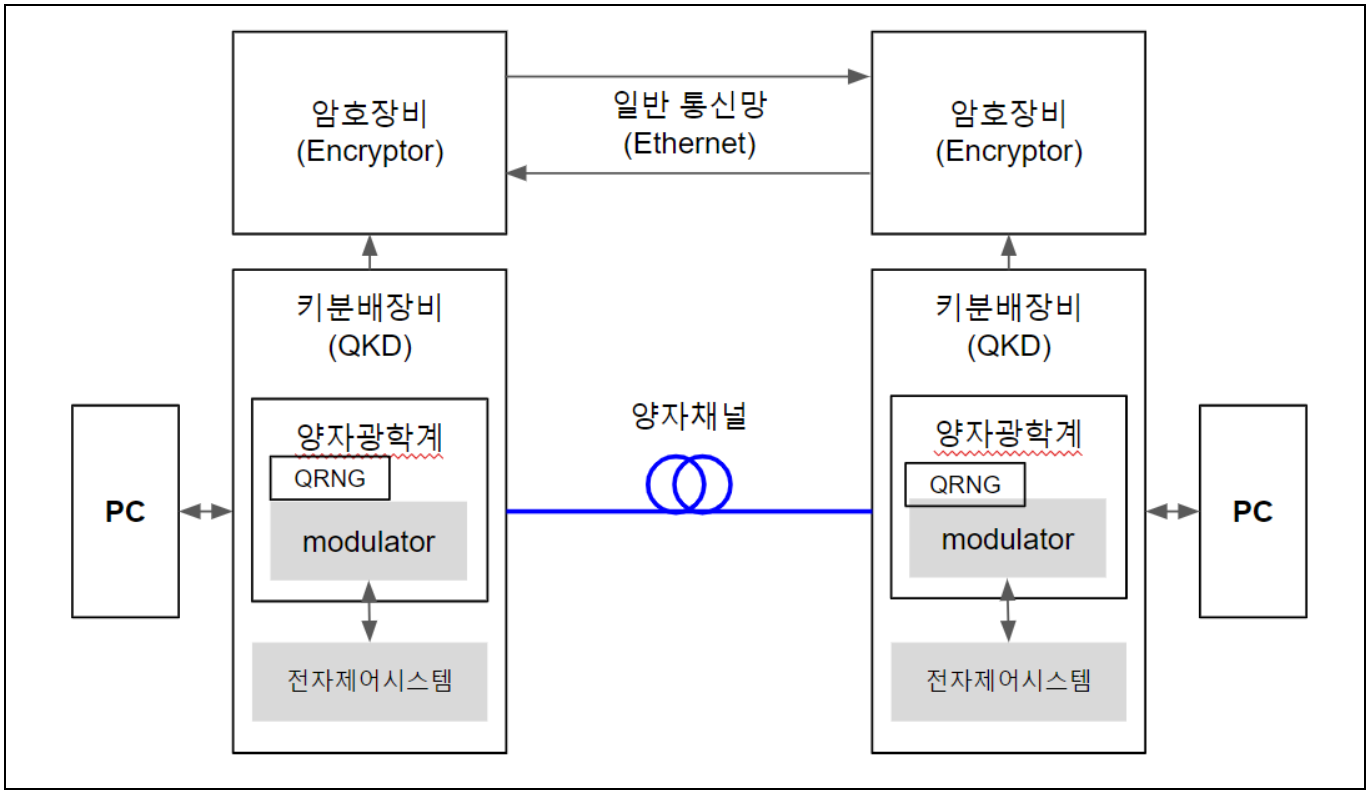
- BB84프로토콜은 안전하게 양자 채널을 통해 안전하게 키를 교환하기 위한 프로토콜
- 이외 양자 암호 프로토콜로는 서로 직교하지 않는 2개의 양자상태로 구현하는 B92방식 등이 있음

나. BB84프로토콜 양자키 분배 절차 예시

항목	설명	
필터(Basis)		
작동방식 예시	① 엘리스가 임의의 비트를 생성	0 1 1 0 1 0 0 1
	② 비트를 전송할 편광신호로 변환하기 위해 필터를 하나 선택	+ + X + X X X +
	③ 필터에 대응되는 편광신호를 생성하고 양자채널로 송신	↑ → ↘ ↑ ↗ ↗ ↘ →
	④ 밥은 측정하기 위한 편광필터를 임의로 선택	+ X X X + X + +
	⑤ 선택한 편광필터로 값을 측정하여 보관	↑ ↗ ↘ ↗ → ↗ → →
	⑥ 엘리스와 밥은 퍼블릭 채널을 통해 같은 필터를 사용했는지 여부를 검증	퍼블릭 채널을 통한 데이터 교환 (도청가능)
	⑦ 같은 필터를 사용한 비트에 대해서만 보관하고 서로 다른 필터를 사용한 비트는 제거	0 1 0 1 최종키 = 0101

III. 양자암호통신의 주요 기술

가. 양자암호통신의 주요 기술 구성도



나. 양자암호통신의 주요 기술

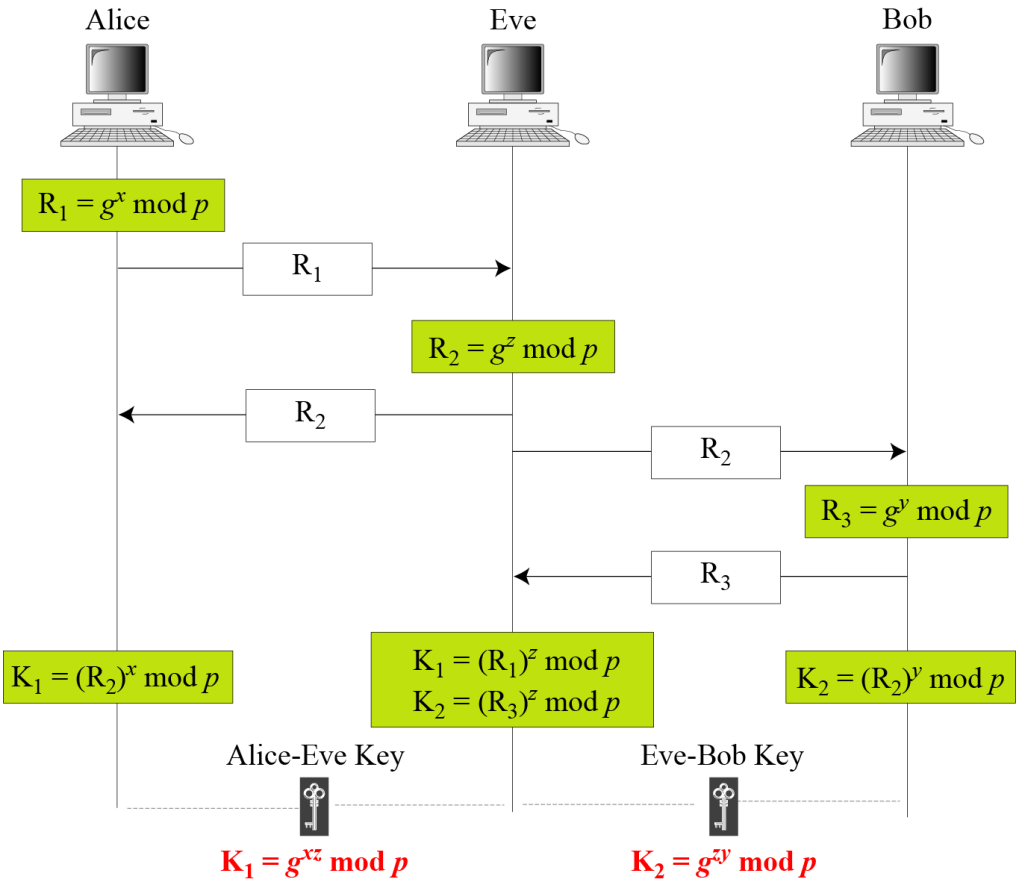
구현기술	주요역할	설명
양자광원	보안성 확보	- 광자를 훔치는 도청공격으로부터 보안성을 지키기 위해 단일광자광원이 사용 - 단일광자광원이란 사용자가 원하는 시간에 광자 하나만을 방사하는 광원
단일광자 검출기	광자 검출	- 광학적 특성과 전기적 특성을 이용하여 단일광자를 검출하는 핵심기술 - 광자검출기의 양자효율과 잡음(dark noise) 수준은 양자암호통신의 에러율과 직접적으로 관련됨 - 높은 양자효율과 낮은 잡음수준을 갖는 광자검출기는 양자암호통신 시스템의 성능을 좌우하는 핵심적인 사항
난수 발생기	도청방지	- 도청자도 예측할 수 없는 무작위수(난수)를 생성하는 기술
양자 암호 프로토콜	양자키 분배 및 전송	- 양자암호키 분배 및 전송을 위한 프로토콜 - BB84, Decoy based QKD, Plug & Play, Phase Differential Shift QKD
양자암호통신 채널	양자키 전송	- 양자암호 혹은 양자 키 분배 기술은 멀리 떨어진 두 사용자(Alice와 Bob) 사이에 양자역학적으로 완벽한 보안성이 보장되는 비밀 키를 분배하는 기술 - 양자암호통신에서는 양자상태를 전송하는 양자채널(비밀채널)과 도청자를 포함한 외부에 완전히 공개된 고전채널(공개채널)의 두 가지 통신채널을 사용

- 양자암호통신 구현기술 중 양자암호프로토콜은 안전한 암호키 분배를 위한 핵심요소
- 통신구간이 길어지면 광자 민감성으로 에러발생이율이 증가하는 한계점 존재
- QKD에서 별도의 인증기능 미제공으로 인해 중간자 공격 등에 취약

IV. 양자암호통신의 취약점

가. 양자암호통신의 취약점 1. 중간자 공격 (Man-in-the-Middle Attack)

정의	- 중간 공격자가 송신자 와 수신자사이에 들어가서, 송신자에 대해서는 수신자처럼, 수신자에 대해서 는 송신자처럼 행세하는 공격 기법



단계	설명
1	- 앨리스가 x를 선택한 후 R1=gx를 계산하여 R1을 밥에게 전송
2	- 제 3자(Eve) 가 R1을 가로챈 후, z를 선택한 다음 R2=Gz mod p 를 계산하여 R2를 앨리스와 밥에게 전송
3	- 밥이 y를 선택한 다음 R3=gy mod N을 계산해서 R3을 앨리스에게 전송, R3을 제 3자 (Eve)가 가로챔
4	- 앨리스와 제3자(Eve)가 공유한 키 K1=gxz mod p를 계산
5	- 제3자((Eve)와 밥은 공유한 키 K2=gzy mod p를 계산

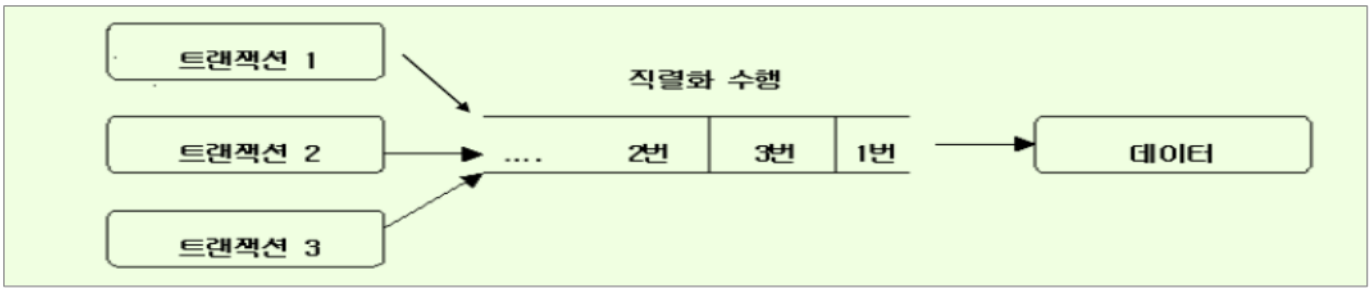
나. 양자암호통신의 취약점 2

취약점	설명
복제 공격법(cloning at-tack, symmetric individual attack)	- 전달되고 있는 큐빗에 양자 복제(quantum cloning)를 행하는 방법 - 양자 역학적으로 완전한 복제는 불가능하지만 암호 키에 대해 일부 정보를 얻는 형태의 공격
양자 비파괴 공격법(quantum non-demoli-tion attack)	- 광원이 완벽한 단일광자 상태를 만들어내지 못하고 일정 확률로 다중광자 상태를 내보내는 경우 이 다중광자 상태를 이용 - 전달되는 큐빗의 상태에 영향을 주지 않으면서 그 펄스에 포함된 광자의 개수는 측정이 가능
트로이의 목마 공격(Trojan horse attack)	- Alice가 Bob으로부터 받은 큐빗에 원하는 연산을 수행한 후 되돌려 보내는 방식인 plug and play 양자 암호 시스템에서 Eve가 스파이 펄스를 Alice에게 보냄으로써 Alice쪽 실험 장치의 상태를 알아내는 방법

"끝"

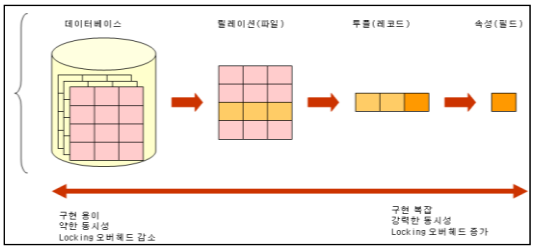
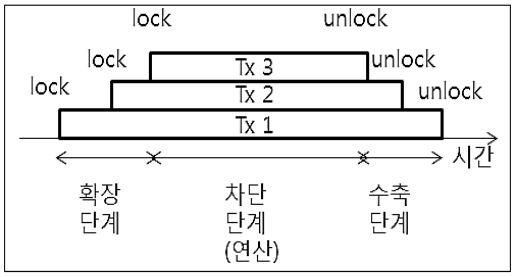
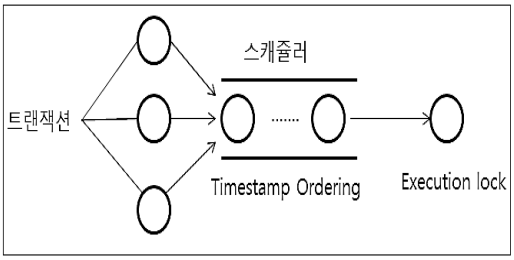
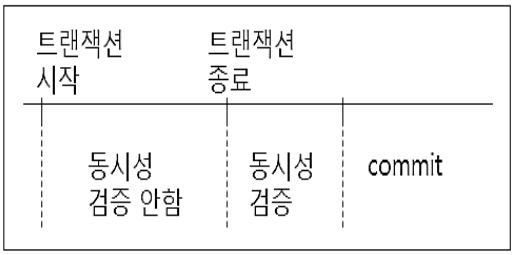
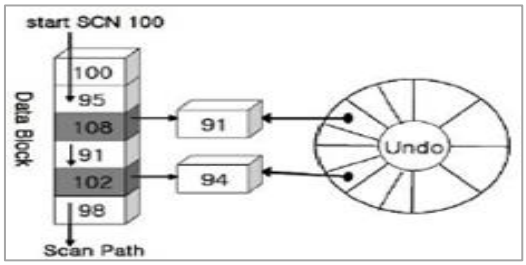
05	병행제어(Concurrency Control)		
문제	데이터베이스의 병행제어(Concurrency Control)에 대하여 다음을 설명하시오. 가. 병행제어의 정의 나. 병행제어의 기법의 종류 다. 병행제어의 문제점		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	다중사용자환경, 트랜잭션 직렬화, 갱신손실, 현황파악오류, 모순성, 연쇄복귀, Locking, 2PL Timestamp, 낙관적 검증, MVCC		
참고문헌	ITPE서브노트		
풀이기술사	유술사PE (제 113회 컴퓨터시스템응용기술사 / itpe_you@naver.com)		

I. 데이터베이스 무결성 확보를 위한 병행제어의 정의

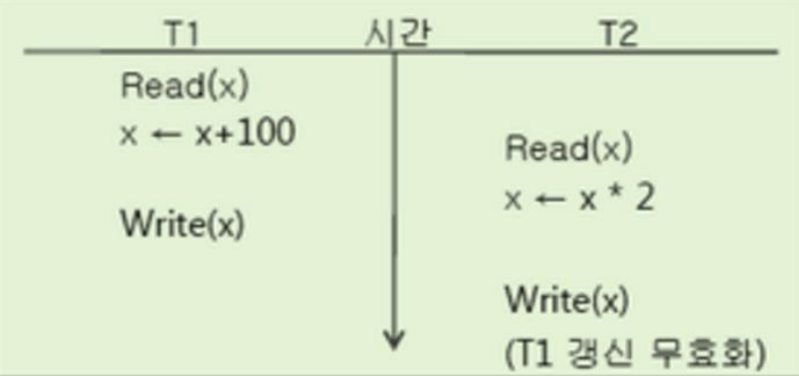
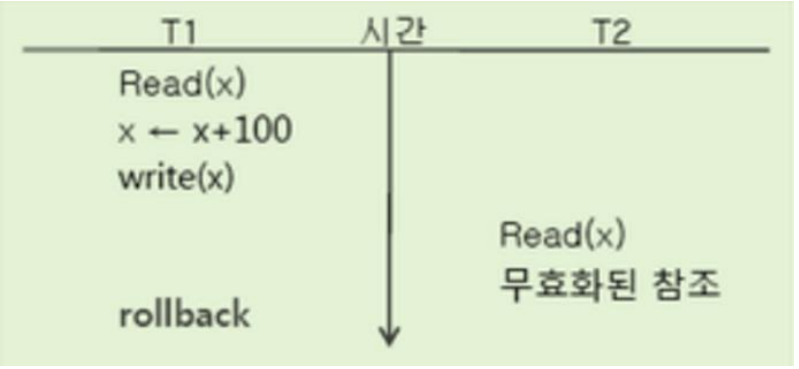
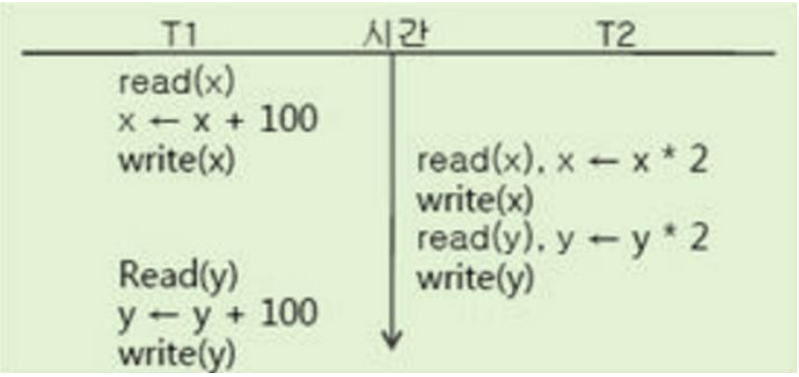
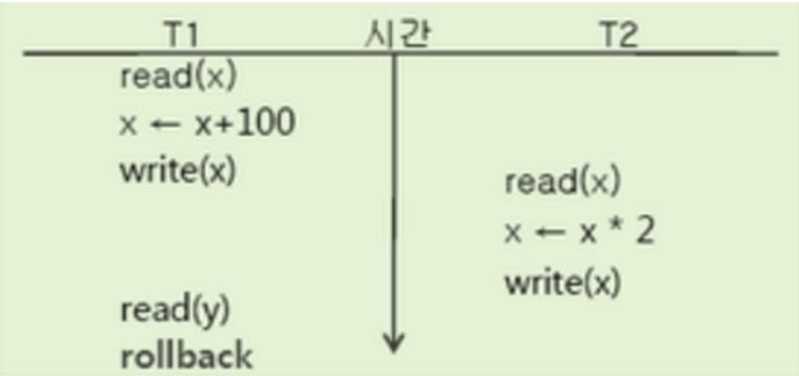


- 다중사용자환경을 지원하는 데이터베이스 시스템에서 여러 트랜잭션들이 '직렬성을 보장하고', 성공적으로 동시에 실행될 수 있도록 지원하는 기능
- 다중사용자환경을 지원하는 DB system의경우 필수적으로 지원해야하는 기능으로 병행제어라고도 함

II. 병행제어의 기법의 종류

기법	개념도	설명
Locking		- 트랜잭션이 사용하는 자원에 대하여 상호 배제(Mutual Exclusive) 기능을 제공하는 기법 - 상호배제는 특정 트랜잭션이 데이터 항목에 대하여 잠금(Lock)을 설정한 트랜잭션이 해제(unlock) 할 때까지 데이터를 독점적으로 사용할 수 있는 것
2PL (Phase Lock)		- 모든 트랜잭션들이 Lock과 Unlock 연산을 확장 단계와 수축 단계로 구분하여 수행 - 확장단계 : 트랜잭션은 lock만 수행할 수 있고, unlock은 수행할 수 없는 단계 - 수축단계 : 트랜잭션은 unlock만 수행할 수 있고, lock은 수행할 수 없는 단계
Timestamp		- 시스템에서 생성하는 고유 번호인 시간 스탬프를 트랜잭션에 부여하는 것으로 트랜잭션 간의 순서를 미리 선택하는 것 (시스템 시계, 논리적 계수기 등 활용)
낙관적 검증 (Validation)		- 트랜잭션이 어떠한 검증도 수행하지 않고, 일단 트랜잭션을 수행하고, 트랜잭션 종료 시 검증을 수행하여 데이터베이스에 반영
다중버전 병행 제어 (MVCC)		- 하나의 데이터 아이템에 대해 여러 버전의 값 유지 - 트랜잭션의 타임스탬프와 접근하려는 데이터 아이템의 여러 버전의 타임스탬프를 비교하여, 현재 실행하고 있는 스케줄의 직렬 가능성이 보장되는 적절한

III. 병행제어의 문제점

문제점	개념도	설명
갱신손실 (Lost Update)		- 동일데이터 동시갱신 - 이전 트랜잭션이 데이터를 갱신한 후 트랜잭션을 종료하기 전에 나중 트랜잭션이 갱신 값을 덮어쓰는 경우 발생
현황파악오류 (Dirty Read)		- 트랜잭션의 중간수행 결과를 다른 트랜잭션이 참조함으로써 발생하는 오류 - 수행전에 값을 읽어서 의도치 않은 결과가 발생
모순성 (Inconsistency)		- 두 트랜잭션이 동시에 실행할 때 DB가 일관성이 없는 상태로 남는 문제 - 각 트랜잭션의 결과가 다른 트랜잭션의 중첩으로 갱신 모순
연쇄복귀 (Cascading Rollback)		- 복수의 트랜잭션이 데이터공유시 특정 트랜잭션이 처리를 취소할 경우 다른 트랜잭션이 처리한 부분에 대해 취소불가능

"끝"

06	식별(Identification)과 인증(Authentication)		
문제	식별(Identification)과 인증(Authentication)에 대하여 다음을 설명하시오. 가. 개인 식별과 사용자 인증의 정의 및 차이점 나. 사용자 인증 시 보안 요구사항 다. 인증 방식에 따른 4가지 유형 및 유형별 특징		
도메인	보안	난이도	중 (상/중/하)
키워드	고유 식별자, 지식, 소유, 존재, 행위, MFA, 인가, 책임추적성		
참고문헌	https://m.blog.naver.com/wnrjsxo/221727680845		
풀이기술사	김민PE (제 120회 정보관리기술사 / itpe.min@gmail.com)		

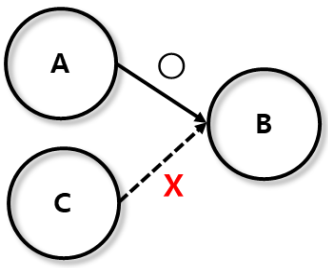
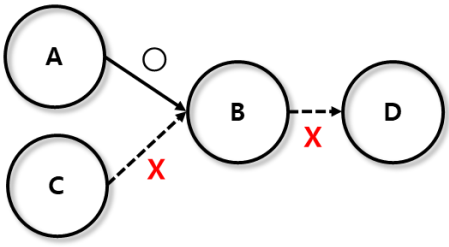
I. 개인 식별과 사용자 인증의 정의 및 차이점

가. 개인 식별과 사용자 인증의 정의

개인 식별	- 인증 서비스에 개인 스스로를 확인시키기 위하여 ID 등 고유 식별자를 이용하는 정보 주체의 활동
사용자 인증	- 식별된 주체의 신원을 검증하기 위해 지식, 소유, 존재, 행위 인증 방식 이용하는 정당한 사용자 증명 활동

- 식별, 인증, 인가 통해 책임 추적성 확보로 보안 사고시에 책임 소재의 명확성 제공

나. 개인 식별과 사용자 인증의 차이점

차이점	개인 식별	사용자 인증
개념도		
개념도 설명	- 사용자 A가 사용자 B와 협조하여 자신이 A임을 증명할 수 있으나 제3자 C는 자신이 사용자 A처럼 가장할 수 없는 것	- 사용자 A가 사용자 B와 협조하여 자신이 A임을 증명할 수 있으나 C는 자신이 A인것처럼 가장 불가하고 B는 제3자 D에게 A인것처럼 가장할 수 없는 것
증명	- 고유식별자(주민등록번호, ID)	- Password, 생체, 토큰, 움직임

II. 사용자 인증 시 보안 요구사항

가. 보안 속성 측면 사용자 인증 시 보안 요구사항

구분	보안 요구사항	기법
기밀성	- 사용자 인증 정보 암호화 적용 - 사용자 인증 정보 송수신 경로 암호화 적용 - 스누핑, 트래픽 분석 공격 차단 적용	- 대칭 암호(스트림, 블록) - 비대칭 암호(RSA, ElGamal)
무결성	- 사용자 인증 정보 변경 적법한 절차 적용 - 사용자 인증 정보 변경 인가된 주체 허용 적용 - 변경, 삽입, 삭제 재연 공격 차단 적용	- OTP - 디지털 서명
가용성	- 사용자 인증 적법한 사용자 언제든지 사용 가능 - 사용자 인증 정보 이중화 적용 - DDoS 공격 차단 적용	- HA(High Availability) - Anti-DDoS

나. 구현 측면 사용자 인증 시 보안 요구사항

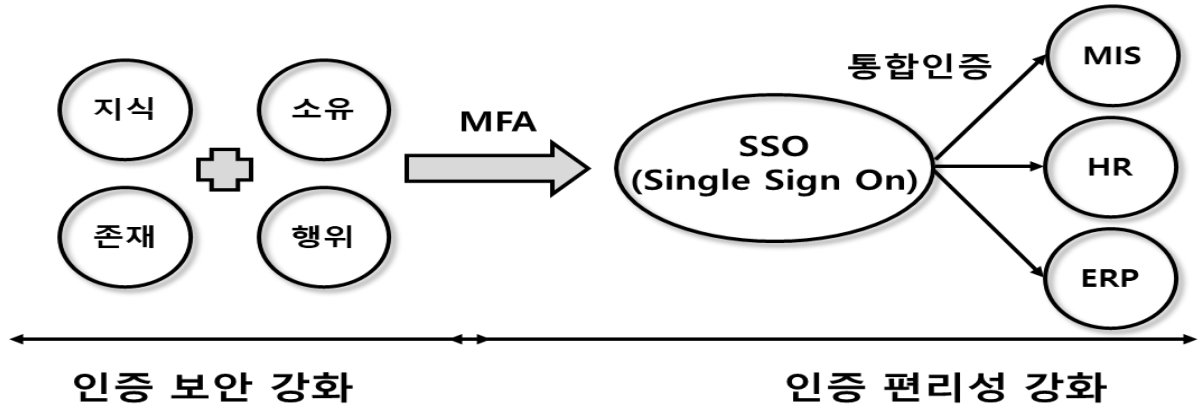
구분	보안 요구사항	기법
사용자 인증 방식 선택	- 취약한 암호 방식 미사용 준수 (SHA-0, SHA-1 등 사용 금지) - Brute Force 공격 불가 수준 인증 방식 적용	- 지식, 소유 - 존재, 행위
사용자 인증 정보 저장	- 역방향 분석으로 암호 해독 불가 적용 - 외부 침입 차단된 안전한 저장소에 분산 저장 적용	- Hash - 다분할 분산 저장
사용자 인증 유지 관리	- 적정한 접근 통제 수준 적용 - 인증 실패 허용 최대치 및 추가 인증 적용 - 일정 주기 인증 정보 재인증 적용	- RBAC, MAC, DAC - Lock / Unlock

III. 인증 방식에 따른 4가지 유형 및 유형별 특징

유형	특징	기법
지식	- 주체가 알고 있는 것(Something you know) - 비밀번호 크기와 랜덤성에 의해 보안성의 안전도 결정 - 지식이 노출될 경우 비인가자 인증 가능 취약점 존재	- Password - I-PIN
소유	- 주체가 가지고 있는 것(Something you have) - 고정된 정보의 위험성으로 동기/비동기 방식 OTP 사용 - 분실의 위험성 존재하여 비인가자 인증 가능 취약점 존재	- 신분증 - OTP - 토큰
존재	- 주체를 나타낼 수 있는 것(Something you are) - 생체 정보를 서버에 저장후 인증시 사용 - 인증 속도 및 정확도(1차, 2차 오류) 고려 필요	- 홍채 인식 - 지문 인식 - 얼굴 인식
행위	- 주체가 수행하고 있는 것(Something you do) - 주체 고유의 미세하게 다른 습관 기준 인증 - 무자각 인증으로 주체의 별도 인증 행위 불필요	- 서명, 걸음걸이 - 말하는 속도 - 음성 패턴

- 단일 인증 방식의 취약점 해결 위해 MFA 및 다중 인증 불편함 해소 위한 통합 인증 체계 사용

IV. MFA(Multi-Factor Authentication)과 통합 인증 체계 설명



MFA	- 단일 인증 방식의 취약점을 극복하기 위해 다른 종류의 인증 방식을 복합적으로 수행하여 인증 보안성 강화
통합 인증 체계	- 강화된 인증 보안성의 중복 수행의 불편함을 최소화하기 위해 통합 인증 방식 적용으로 사용자 편리성 강화

- 통합 인증 체계 적용으로 해킹 시 영향도 증대되어 MFA 보안성 강화에 각별한 유의가 필요함

"끝"

ITPE 기술사회
제128회 정보관리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2022년 07월 02일
집 필 강정배PE, 안경환PE, 전일PE, 유술사PE, 김민PE, 백기현PE, 차상인PE
출 판 **ITPE(Information Technology Professional Engineer)**
주 소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층
ITPE 선릉점 서울시 강남구 선릉로 86길 15, 3층 IT교육센터 아이티피이
ITPE 강남점 서울시 강남구 테헤란로 52길 21 파라다이스벤처타워 3층 303호
ITPE 영등포점 서울시 영등포구 당산동2가 하나비즈타워 7층 ITPE
연락처 070-4077-1267 / itpe@itpe.co.kr