[신기술 - 시스템 관리2]

* UCC (User Created Content, 사용자 제작 콘텐츠)
: 인터넷 사업자나 콘텐츠 공급자가 아닌 일반 사용자들이 직접 만들어 유통되는 콘텐츠. (ex. YouTube 동영상)

* UCC Guide line
: 정부가 제정한 건전한 사용자 제작 콘텐츠(UCC) 생산과 유통 및 이용에 관한 지침서.

* 관계기술 (Relation Technology)
: 상호관계를 이해하는 관계성을 기반으로 하는 새로운 기술 패러다임. 기술위주로 발전하는 정보기술(IT)에 나와너, 사람과 사람 등 문화, 인문학 등의 논리위주의 관계기술(RT)이 접목되어야 한다는 점을 강조하며 이어령 이화여대 명예교수가 만들어 낸 신조어다.

* tagging (태그달기)
: 콘텐츠의 내용을 대표할 수 있는 검색용 꼬리표인 키워드, 또는 태그(Tag)를 다는 것. 글을 올린 사람이나 사이트 관리자가 글이나 이미지를 관련된 주제나 카테고리의 형태로 분류될 수 있도록 키워드 처리를 해주는 것

* Quickdom (퀵돔)
: 영어의 'Quick'과 'Domain'이 결합된 합성어로, 2단계 영문 kr도메인의 브랜드명. 퀵돔은 gisafirst.kr과 같이 gisafirst.co.kr과 같은 3단계 형태의 도메인에 비하여 짧은 형태의 도메인으로 기억하기 쉽고 주소창에 입력하기도 간편하다.

* 사이버 정보전 (Cyber Information Warfare)
: 특정한 정치나 사회적 목적을 가진 개인,테러 집단 또는 적이 되는 나라가 해킹을 하거나 컴퓨터 바이러스를 유포하는 전자 공격으로 정보 통신 기반 시설을 파괴하거나 마비되게 함으로써 사회 혼란과 국가 안보를 위협하는 행위.

[신기술 - 시스템 관리2]

* HCE (Host Card Emulation)
: 스마트폰과 같은 모바일 기기에서 물리적 보안 요소(secure element)를 이용하지 않고 순수 소프트웨어 방식으로 모바일 결제 서비스를 제공하는 근거리 무선 통신(NFC: Near Field Communication) 기술.

* wearable technology (착용 기술)
: 정보통신(IT) 기기를 사용자 손목, 팔, 머리 등 몸에 지니고 다닐 수 있는 기기로 만드는 기술.(ex. 스마트워치)

* digital mesh
: 차량, 카메라, 가전제품, 스마트폰, 착용 컴퓨터(웨어러블 기기) 등 많은 다양한 기기들이 상호 연결되어 촘촘한 그물망 같은 형태를 가리키는 것.

* AllJoyn (올조인)
: 사물 인터넷(IoT: Internet of Thing) 연합 단체인 올신얼라이언스(AllSeen Alliance)에서 표준화한 오픈 소스 기반의 IoT 플랫폼.

* Wi-Fi HaLow (와이파이 헤일로)
: 와이파이 얼라이언스(Wi-Fi Alliance)에서 저전력 와이파이 표준(IEEE 802.11ah)을 탑재한 장치를 일컫는 명칭.

* 용도 자유 대역 (K-ICT Free Band)
: 기기 간 혼신 방지를 위한 최소한의 기술기준만 충족하면 허가·신고 없이 자유롭게 사용할 수 있는 주파수 대역. 전파의 창의적 이용을 확산시키고, 늘어나는 사물 인터넷(IoT) 서비스 수요나 새롭게 출현될 다양한 정보통신기술(ICT) 수요에 유연하게 대응하기 위하여 우리나라에서 지정한 대역이다.

[신기술 - 시스템 관리2]

* 집단 지성 (Collective Intelligence)
: 다수의 개체가 서로 협력하거나 경쟁하여 얻게 되는 지적 능력의 결과로 얻어진 집단적 능력. 자발적으로 참여하고 다양한 의견을 가진 개인의 지식이 모이면 개체적으로는 미미하게 보이나 집단적으로는 능력 범위를 넘어선 힘을 발휘해 특정 전문가나 기업의 전문 지식보다 더 우수하게 된다는 대중의 지혜를 나타내는 개념으로 웹 2.0의 주요 개념이다. (ex. 위키피디아, 지식iN 등)

* XML (Extensible Markup Language, 확장성 생성 언어)
: 하이퍼텍스트 생성 언어(HTML) 기능을 확장할 목적으로 월드 와이드 웹 컨소시엄(WWW Consorsium)에서 표준화한 페이지 기술 언어.

* Alt text (대체 텍스트)
: 시각장애인의 웹 접근성을 위한 대표적인 방법으로 웹 사이트에 게시된 이미지를 시각장애인이 이해할 수 있도록 설명해 주는 글이나 문구.

* MMS (Multimedia Messaging System)
: 3세대 이동 통신 서비스의 기본 요소로서 정지 영상, 음악, 음성 및 동영상 등의 다양한 형식의 데이터를 주고받을 수 있는 메시징 시스템. (SMS: 단문 메시지)

* 디지털 원주민 (Digital Native)
: 컴퓨터, 인터넷, 휴대 전화 등의 디지털 기술을 어려서부터 사용하면서 성장한 세대. 컴퓨터나 인터넷 등을 복잡하고 어려운 기술로 생각하지 않고 그냥 손에 익은 장치 정도로 여기면서 쉽게 활용한다.

[신기술 - 시스템 관리2]

* 망 중립성 (Network Neutrality)
: 모든 네트워크 사업자는 모든 콘텐츠를 동등하게 취급하고 어떠한 차별도 하지 않아야 한다는 원칙. 망운영의 근본적인 원칙으로 중립성을 보장하기 위해 비차별・상호접속・접근성 등 3가지 원칙이 모든 통신망에 동일하게 적용되야 한다는 것이다.

* 앱 중립성 (app neutrality)
: 앱이 모바일 운영 체제(OS)의 종류에 구애받지 않고 두루 동작할 수 있는 성질. 앱 융통성이라고도 할 수 있다.

* CSO (Chief Security Officer, 정보 보호 최고 책임자)
: 기업에서 내부 정보 보안을 위한 대책을 책임지고 기술적 대책과 법률적 대응까지 총괄 책임을 지는 최고 임원. 특히 특정 정보 보안을 책임진다는 의미에서 최고 정보 보안 책임자(CISO: Chief Information Security Officer)라고 하며, 기업에 따라서는 물리적 혹은 기능적 보안을 책임지는 경우와 문서 파일, 네트워크 및 기업내 각종 컴퓨터 보안을 책임지는 경우가 있다. CSO나 CISO 산하에 데이터 보안 책임자(DSO: Data Security Officer), 정보 시스템 보안 책임자(ISSO: Information Systems Security Officer), 보안 책임자(SECOFF: Security Officer), 시스템 보안 책임자(SSO: System Security Officer) 등이 있다.

* gap filler
: 고층 빌딩에 의해 전파가 차폐되는 지역에서 방송을 수신할 수 있도록 송신소로부터 발사된 전파를 수신하여 재송신하는 소출력 중계소.

* smart plug
: 와이파이(Wi-Fi)나 스마트폰 등의 스마트 기능을 추가한 플러그. 기존의 전기 플러그에 와이파이(Wi-Fi)나 스마트폰 등의 기능을 추가하여 원격에서 전기를 켜거나 끄는 것은 물론 전기 사용량을 감시할 수 있다.

[신기술 - 시스템 관리2]

* dark data
: 정보를 수집한 후, 저장만 하고 분석에 활용하고 있지 않는 다량의 데이터.
다크 데이터는 처리되지 않은 채 미래에 사용할 가능성이 있다는 이유로 삭제되지 않고 방치되어 있어, 저장 공간만 차지하고 보안 위험을 초래할 수 있다.

* dark web
: 일반 인터넷 검색 엔진에서 검색되지 않고, 특정 환경의 인터넷 브라우저에서만 접속되는 웹사이트.
다크 웹은 심층 웹(Deep Web: ex. 유료 데이터, 기업 비밀 자료) 보다 접근이 더 어렵다. 다크 웹에서는 비트코인 불법 거래, 랜섬웨어를 이용한 돈 요구 등 사이버 범죄가 발생되기도 한다.

* 표면 웹 (Surface Web)
: 일반 검색 엔진으로 검색이 가능한 콘텐츠의 인터넷 환경. 구글(Google), 네이버(Naver), 다음(Daum)과 같은 일반 검색 사이트에서 검색되지 않는 심층 웹과는 비교되는 용어이다.

* 평면 디자인 (flat design)
이차원 그래픽스 사용자 인터페이스(GUI). 삼차원(3D) 공간으로 표현하지 않고, 단순히 레이아웃, 대비 등 기본적인 요소로만 디자인(깔끔)한다. 대표적인 예로, 마이크로소프트(Microsoft)의 윈도우 8(Windows 8)과 애플(Apple)사의 iOS7를 들 수 있다.

[신기술 - 시스템 관리2]

* registry
: 윈도즈 운영 체계에서 환경 설정 및 각종 시스템에 관련된 정보를 저장해 둔 장소. 응용 프로그램을 설치 또는 삭제할 때마다 레지스트리 정보도 함께 수정되며 regedit.exe 파일을 이용해 임의로 레지스트리 내용을 열람 또는 수정, 삭제할 수 있다.

* 인터넷 연동 (IX; Internet eXchange)
: 서로 다른 인터넷 서비스 제공자(ISP: Internet Service Provider) 간에 트래픽을 원활하게 소통시키기 위한 인터넷 연동 서비스. 인터넷 연동(IX) 서비스를 통해 ISP 간의 상호 접속 이외에 대규모 트래픽이 발생하는 콘텐츠 전송망(CDN: Content Delivery Network) 서버와 네이버, 다음카카오 등과 같은 포털 서버의 회선에 직접 연결되어 트래픽 중계 비용 절감과 서비스 품질의 향상 효과를 얻을 수 있다.

* Mobile Computing
: 휴대형 기기로 이동하면서 자유로이 네트워크에 접속하여 업무를 처리할 수 있는 환경.

* App Store
: 애플사가 개발한 모바일용 온라인 소프트웨어 장터. (안드로이드: Play Store)

* Proteur (professional amateur)
: 전문가 같은 아마추어. 프로페셔널(professional)과 아마추어(amateur)의 합성어이다. 웹 2.0(데이터의 소유자나 독점자 없이 누구나 손쉽게 데이터를 생산하고 인터넷에서 공유할 수 있도록 한 사용자 참여 중심의 인터넷 환경. ex.Blog)이 일반화되면서 일반 네티즌이 정보의 수요자가 아닌 공급 주체로 떠오르면서 적극적으로 자신의 의견을 개진하고 전문가 못지않은 식견을 가진 사람을 말한다.

[신기술 - 시스템 관리2]

* W-CDMA (wideband code division multiple access, 광대역 부호 분할 다중 접속)
: 국제 전기 통신 연합(ITU)이 표준화를 추진하고 있는 국제 이동 통신 시스템(IMT-2000)을 위해 부호 분할 다중 접속(CDMA) 방식을 광대역화하는 기술. (대표적인 3세대(3G) 이동통신 접속 표준)

* 와이브로 (wibro)
: 핸드셋, 노트북, 개인 휴대 정보 단말기(PDA), 스마트 폰 등 다양한 휴대 인터넷 단말을 이용하여 정지 및 이동 중에서도 언제, 어디서나 고속으로 무선 인터넷 접속이 가능한 서비스

* 이동통신 방식의 발전 과정

	1G	2G	3G	pre-4G / 4G
접속방식	아날로그	GSM CDMA	WCDMA CDMA2000 와이브로	LTE / LTE-Advanced 와이브로- 에볼루션(와이맥스2)
전송속도	-	14.4 ~ 64kbps	144kbps ~ 2Mbps	100Mbps ~ 1Gbps
전송형태	음성	음성/문자	음성/문자/동영상 등	음성/문자/동영상 등
다운로드 속도 (800MB 동영상)	다운로드 불가	약 6시간	약 10분	약 85초~6초(이론적)

* WIPI (Wireless Internet Platform for Interoperability, 위피)
: 한국형 무선 인터넷 플랫폼 표준 규격. 이동통신 업체들이 같은 플랫폼을 사용하도록 함으로써 국가적 낭비를 줄이자는 취지 (3세대 휴대폰용 운영체제, 국제무선인터넷표준화기구가 국제표준 채택 거절 → 2009년부터 의무 탑재 폐지 → 실폐)

[신기술 - 시스템 관리2]

* 서비스형 백엔드 (Backend as a Service)
: 웹 및 모바일 애플리케이션(앱) 개발자를 위한 클라우드 서비스. → 개발 시간을 단축하고 코드의 복잡성을 줄일 수 있다.

* 와이파이 오프로딩 (Wi-Fi offloading)
: 이동 통신의 데이터가 폭증함에 따라 이동 통신 트래픽의 일부를 와이파이(Wi-Fi) 망으로 분산시키는 방법.

* 지오로케이션 (geolocation)
: 유무선망에 연결된 휴대 전화, 컴퓨터 등 기기의 지리적 위치 정보 → 이를 기반으로 사용자 위치 정보를 얻고, 이를 기반으로 사용자에게 길 안내 기능, 근처의 편의 시설, 맛집, 병원 등 유용한 정보를 서비스한다.

* PS-LTE (Public Safety-LTE)
: 전국 규모의 광대역 공공 안전 통신망을 구축하는 LTE(Long Term Evolution) 기술.
LTE기술은 전국망 구축이 용이한 광대역 이동통신 기술로 국제적으로 검증이 완료된 기술이다. PS-LTE 기술은 기존의 LTE 기술에 D2D(Device to device) 통신, 그룹 통신을 제공하는 GCSE(Group Communication System Enablers) 등 재난 안전에 필수적인 기능을 추가한 것이다.

* CTTH (Coax To The Home)
: 기존 케이블 방송망으로 초고속/대용량 서비스를 제공하는 새로운 전송 방식. 총 1Gbps 용량을 여러 가입자가 공유하는 구조로 일반 가정에 130Mbps의 빠른 인터넷 속도를 제공한다.

* AppBook
: 스마트폰, 태블릿 PC, 개인용 컴퓨터 등 단말 기기에서 별도의 애플리케이션으로 실행되는 전자책.

[신기술 - 시스템 관리2]

* VMC (Vehicle Multihop Communication, 차량 멀티홉 통신)
: 자동차에 정보 기술(IT)을 접목해 차량 충돌을 예방하는 기술. 자동차와 노면 간 라디오 주파수(RF) 통신을 주고받아 제한 속도를 넘으면 자동으로 차량 속도가 감속되는 것은 물론 차량 간 통신으로 충돌을 예방하는 기술이다.

* UWB (Ultra-wideband, 초광대역 무선)
기존 IEEE 802.11과 블루투스 등에 비해 빠른 속도(500Mpbs/1Gbps)와 저전력 특성이 있다. 평균 10~20m, 최대 100m의 단거리무선망(WPAN)에서 PC와 주변기기 및 가전 제품들을 초고속 무선 인터페이스로 연결하거나 벽 투시용 레이더, 고정밀도의 위치 측정, 차량 충돌 방지 장치, 신체 내부 물체 탐지 등 여러 분야에서 활용 가능하다.

* Piconet (피코넷)
: 여러 개의 독립된 통신장치가 블루투스 기술이나 UWB 통신기술을 사용하여 통신망을 형성하는 무선 네트워크 기술. 주로 수십 미터 이내의 좁은 공간에서 네트워크를 형성하는 점과 정지 또는 이동 중에 있는 장치를 모두 포함하는 특징을 가지고 있다. WLAN(무선랜)과 달리 전송을 위한 기반구조가 미리 설정되지 않고 상황에 따라 기기들 간에 조정 프로토콜에 의하여 네트워크를 형성한다.

* HSDPA (High Speed Downlink Packet Access, 고속 하향 패킷 접속)
: 비동기식 3세대 이동 통신의 하향 링크에서 10Mbps 수준의 고속 패킷 데이터 서비스를 제공하는 전송 규격. 인터넷 통신은 주로 내려받기가 많아 하향 링크의 고속화가 서비스의 필수 요소이며, 고속 데이터는 주로 정지 상태에서 사용되므로 이러한 조건을 최대한 수용하도록 하향 링크의 전송 규격을 개선한 것

[신기술 - 시스템 관리2]

* USN (Ubiquitous(시간과 장소에 구애받지 않고 언제나 네트워크에 접속할 수 있는 통신 환경) Sensor Network)
: 각종 센서에서 감지한 정보를 무선으로 수집할 수 있도록 구성한 네트워크. WPAN(wireless personal area network), ad-hoc network 등의 기술이 발전함에 따라 u센서 네트워크 기술이 매우 활성화되고 있다. 센서의 종류로는 온도, 가속도, 위치 정보, 압력, 지문, 가스 등 다양하게 존재한다.

* GIS (Geographical Information System, 지리 정보 시스템) → 지리 정보를 디지털화
: 지도에 관한 속성 정보를 컴퓨터를 이용해서 해석하는 시스템. 취급하는 정보는 인구 밀도나 토지 이용 등의 인위적 요소, 기상 조건이나 지질 등의 자연적 환경 요소 등 다양하다. 속성 정보를 가공하여 특정 목적을 위해 해석하고 계획 수립을 지원하는 것을 목적으로 하며, 시설 관리(FM) 시스템과는 구별하는 경우도 있다. 지리 정보 시스템은 도시 계획, 토지 관리, 기업의 판매 전략 계획 등 여러 가지 용도에 활용된다.

* IT 839 전략 → 정보통신부 2004년 수립
: IT 서비스 → 인프라 → 기기 → 소프트웨어 및 콘텐츠가 수직적으로 연결되어 있는 IT 산업의 가치사슬에 따라 8대 신규 정보통신 서비스를 도입, 활성화하여 유무선 통신, 방송, 인터넷 등 3대 인프라에 대한 투자를 유발하고, 이를 바탕으로 9개 첨단기기와 단말기, 소프트웨어, 콘텐츠 산업이 동반 성장하는 IT 산업의 발전전략. 참여정부 출범과 함께 국가 전략과제로 선정한 차세대 10대 신성장동력 중 정보통신부 관련 내용으로서 구체적으로는 8대 신규 서비스(WiBro, DMB, 홈 네트워크, 텔레매틱스, RFID 활용, W-CDMA, 지상파 DTV, 인터넷전화(VoIP)), 3대 첨단 인프라(광대역통합망(BcN), u-센서네트워크(USN), 차세대 인터넷 프로토콜(IPv6)), 9대 신성장동력 (차세대 이동통신 기기, 디지털TV/방송 기기, 홈네트워크 기기, IT SoC, 차세대 PC, 임베디드 S/W, 디지털 콘텐츠(DC) & S/W 솔루션, 텔레매틱스 기기, 지능형 서비스 로봇)의 분야별로 계획을 수립하여 추진한다.

* SBAS (Satellite-Based Augmentation System, 위성 기반 보정 시스템)
: GNSS(인공위성을 이용하여 위치를 파악하는 항법 시스템, ex) GPS 등 통칭)의 위치 오차를 보정한 정보를 위성을 통해 사용자에게 전달하는 광역(wide-area)의 위성 항법 보정 시스템

* GBAS (Ground-Based Augmentation System, 지상 기반 보정 시스템)
: 공항 인근과 같은 협역에서 세계 위성 항법 체계(GNSS)의 위치 오차를 보정한 정보를 지상국에서 직접 사용자에게 전송하는 위치 보정 시스템.

* Multicast
: 구내 정보 통신망(LAN)이나 인터넷에 접속되어 있는 일부 사용자 내에서 한 사람이 몇 사람에게 정보를 송신하고 그것을 수신한 몇 사람이 같은 내용을 버킷 릴레이(bucket relay)식으로 복수의 사람에게 송신함으로써 정보를 전파하는 특정 다수인에 대한 전송(지정된 그룹에게만 같은 정보 동시 발송). 인터넷에서 멀티캐스팅을 지원하는 컴퓨터간의 가상 네트워크를 엠본(MBONE)이라고 한다. 엠본은 한 개의 인터넷 주소로 특정 그룹에 참여하는 모든 사람에게 동일한 데이터를 전달한다. 그러므로 많은 사람들이 한꺼번에 특정 서버에 접속하여 대용량 멀티미디어 정보를 전송받을 때 겪게 되는 정보체증 현상을 크게 해소할 수 있다. 실시간 공동작업을 효율적으로 보장하는 전송기법이다. (ex. 회의 시스템 등)
- Unicast: 특정 1인에게 송신 (1:1)
- Broadcast: 불특정 다수인에게 정보를 송신
- Anycast: IPv6에서 Broadcast 가 없어지고, 생김. 수신자들을 묶어 하나의 그룹으로 나타낸 주소를 사용하여 그룹 내에서 가장 가까운 호스트에게만 전송하는 것

* IPv6 (Internet protocol version 6)
: IPv4의 주소공간을 4배 확장한 128 비트 인터넷 주소 체계.

[신기술 - 시스템 관리2]

* OPE (Order Preserving Encryption, 크기 보존 암호화)
: 데이터베이스에서 암호화된 데이터들이 원본 숫자 데이터의 크기와 동일한 순서로 정렬될 수 있도록 해 주는 암호화 기술. 검색 속도 저하를 극복하기 위한 암호화 방법

* 범용 통합 플랫폼 (universal integration platform)
: 기업에서 사용되는 다양한 애플리케이션 개발·운영을 위해 크로스 플랫폼(cross platform)과 범용 서버(universal server), 업무 설계용 그래픽 사용자 인터페이스(GUI) 도구, 프로그램 저작 엔진 등을 제공하는 통합 플랫폼.
- 크로스 플랫폼: 소프트웨어나 하드웨어 등이 다른 환경의 OS에서 공통으로 사용되는 것. (ex. JAVA)

* EPC Class (Electronic Product Code Class)
: EPC 글로벌(단체)에서 정의하는 전파 식별(RFID) 태그 종류. 클래스 1은 태그 제조업체에서 고유한 인식 번호가 제작 단계에서 부여되어 물체에 부착된 뒤에 리더로 읽기만을 제공하는 읽기 전용 수동형 태그이고, 클래스 2는 읽기/쓰기가 가능하고 암호화를 적용할 수 있는 보다 발전된 형태의 수동형 태그다. 클래스 3은 배터리를 내장하여 리더로부터 오는 전력을 태그 정보 전송에만 활용하도록 하여 인식 거리를 증가시킨 반 능동형 태그이다. 클래스 4는 태그끼리 통신이 가능하며, 애드혹 네트워크 구성이 진화된 형태의 태그이다.

* ICMP (Internet Control Message Protocol, 인터넷 제어 메시지 프로토콜)
: TCP/IP 기반의 인터넷 통신 서비스에서 인터넷 프로토콜(IP)과 조합하여 통신 중에 발생하는 오류의 처리와 전송 경로의 변경 등을 위한 제어 메시지를 취급하는 무연결 전송(connectionless transmission)용의 프로토콜. OSI 기본 참조 모델의 네트워크층에 해당한다.

[신기술 - 시스템 관리2]

* SAM (Secure Application Module, Secure Access Module, 보안 응용 모듈)
: 스마트 카드(IC 칩이 표면에 부착된 전자식 카드) 보안 응용 모듈. 카드 판독기 내부에 장착되어 카드와 단말기의 유효성을 인증하고 통신 데이터를 암호화하여 정보의 노출 방지 및 통신 메시지의 인증 및 검증을 하며, 또한 카드에서 이전된 전자적인 가치를 저장하기도 한다. SAM은 일반적으로 하드웨어의 형태로 존재하지만 소프트웨어적인 형태로도 존재하며, 인터넷 전자상거래 시, 또는 PC 사용 시 프로그램 안에 카드 인증용 SAM을 내장하기도 한다.

* ANT+ protocol (Advanced and adaptive Network Technology plus protocol, 앤트플러스 프로토콜)
: 상호 운용성(기종이 다른 컴퓨터나 단말기를 연결해서 상호 이용)을 보장하는 초저전력 무선 센서 네트워크 프로토콜.

* RadSec (래드섹 프로토콜)
: 네트워크 이용자의 인증을 위해 전송 제어 프로토콜(TCP: Transmission Control Protocol)과 전송 계층 보안(TLS: Transport Layer Security)을 통해 레이디어스(RADIUS: Remote Authentication Dial In User Service) 데이터를 전송하기 위한 프로토콜. 래드섹(RadSec)은 'RADIUS over TLS(Transport Layer Security)'의 준말이다. RADIUS는 원격지 이용자의 접속 요구 시 이용자 아이디(ID)나 패스워드, IP 주소 등의 정보를 인증 서버에 보내어 인증, 권한 부여, 과금 등을 수행한다. 그러나 RADIUS는 신뢰성이 담보되지 않은 사용자 데이터그램 프로토콜(UDP: User Datagram Protocol) 전송으로 보안에 취약하다. 이러한 RADIUS 문제점을 보완한 프로토콜이 래드섹(RadSec)이다. RadSec은 신뢰성이 보장된 TCP 전송, TLS 암호화 통신 사용, 그리고 통신 주체 간 인증서 교환을 통한 상호 인증을 제공한다.

[신기술 - 시스템 관리2]

* NB-IoT (NarrowBand-Internet of Things, 협대역 사물 인터넷)
: 이동통신망을 통해 저전력 광역(LPWA: Low Power Wide Area) 통신을 지원하는 협대역(좁은 대역폭) 사물 인터넷 표준. GSM(Global System for Mobile Communications) 또는 LTE(Long Term Evolution) 망에서 좁은 대역을 이용하여, 수백 kbps 이하의 데이터 전송 속도와 10 km 이상의 광역 서비스를 지원한다. 따라서 수도 검침, 위치 추적용 기기 등과 같이 원거리에 있고 전력 소비가 낮은 사물 간의 통신에 적합하다.

* ZigBee
: 저속, 저비용, 저전력의 무선 망을 위한 기술. 주로 양방향 무선 개인 영역 통신망(WPAN) 기반의 홈 네트워크 및 무선 센서망에서 사용되는 기술

* CTI (Cyber Threat Intelligence, 지능형 사이버 위협 대응)
: 조직의 정보(information) 자산에 위협이 될 수 있는 취약 요소, 과거 공격 등 관련 정보를 기반으로 사이버 보안 위협에 효과적으로 대응하는 방법. 지능형 사이버 위협 대응(CTI)은 과거 조직 내부뿐만 아니라 여러 외부 조직에서 겪었던 많은 위협 정보를 수집·분석·활용하여, 지능형 지속 위협(APT)과 같은 공격을 사전에 방어한다.

* QoE (Quality of Experience, 체감 품질)
: 서비스 이용자가 각자의 기대치(expectation)에 근거하여 주관적으로 인지하는 어플리케이션 혹은 서비스의 총체적인 허용도. 통신 서비스의 품질에 관한 척도로서는 NP(망성능)와 QoS(서비스품질), QoE 등이 있다. NP는 망 자체의 성능이 중심이 되고, QoS는 서비스 제공자 입장에서 제공할 수 있는 품질로서 이들은 서비스를 받는 개개의 사용자의 서비스 만족도와는 직접적인 관계에 있지는 않다. 따라서 사용자가 요금을 지불한 서비스에 대하여 기대하는 기대치를 근거로 규정하는 품질 척도가 QoE이다.

[신기술 - 시스템 관리2]

* IDS (Intrusion Detection System, 침입 탐지 시스템)
: 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템. 침입 차단 (시스템)만으로 내부 사용자의 불법적인 행동(기밀 유출 등)과 외부 해킹에 대처할 수는 없으므로 모든 내·외부 정보의 흐름을 실시간으로 차단하기 위해 해커 침입 패턴에 대한 추적과 유해 정보 감시가 필요하다.

* UTM (Unified Threat Management, 통합 위협 관리) → 하나의 장비에 여러가지 보안 기능을 탑재
: 침입 차단 시스템, 가상 사설망 등 다양한 보안 솔루션 기능을 하나로 통합한 보안 솔루션. 보안 솔루션은 그 목적에 따라 방화벽, 침입 탐지시스템(IDS: Intrusion Detection System), 침입 방지 시스템(IPS: Intrusion Prevention System), 가상 사설망(VPN: Virtual Private Network), 데이터베이스 보안, 웹 보안, 콘텐츠 보안 등 다양한 솔루션 형태로 분화, 발전되어 왔으나 그 결과 각각의 보안 솔루션 운용 방법을 익히기 위한 시간 비용, 그리고 운용을 위한 물리적 공간과 인력 확보가 요구되었다. 통합 위협 관리(UTM)는 다양한 보안 솔루션을 하나로 묶어 비용을 절감하고 관리의 복잡성을 최소화하며, 복합적인 위협 요소를 효율적으로 방어할 수 있다.

* ESM (enterprise security management 기업 보안 관리) → 이 기종 보안 시스템을 통합, 관리
: 방화벽, 침입 탐지 시스템, 가상 사설망 등의 보안 솔루션을 하나로 모은 통합 보안 관리 시스템. 최근 기업 보안 관리(ESM)는 통합 관리 수준에서 벗어나 시스템 자원 관리(SMS), 망 관리 시스템(NMS) 등 기업 자원 관리 시스템까지 확대, 개발되고 있다. ESM은 기업들이 서로 다른 기종의 보안 솔루션 설치에 따른 중복 투자, 자원 낭비를 줄일 수 있으며, 솔루션 간 상호 연동을 통해 전체 정보 통신 시스템에 대한 보안 정책을 수립할 수 있다는 장점이 있다.

* PII (Personally Identifiable Information, 개인 식별 정보)
: 생존하는 개인에 관한 정보로서 해당 정보에 따라 개인을 식별할 수 있는 정보. ex) 주민등록번호

[신기술 - 시스템 관리2]

* BlockChain
: 온라인 금융 거래 정보를 블록으로 연결하여 피투피(P2P) 네트워크 분산 환경에서 중앙 관리 서버가 아닌 참여자(피어, peer)들의 개인 디지털 장비에 분산·저장시켜 공동으로 관리하는 방식. 블록체인의 기본 구조는 블록(block)을 잇따라 연결한(chain) 모음의 형태이며 피투피(P2P) 방식을 기반으로 한다. 일정 시간 동안 반수 이상의 사용자가 거래 내역을 서로 교환해 확인하고 승인하는 과정을 거쳐, 디지털 서명으로 동의한 금융 거래 내역만 하나의 블록으로 만든다. 그리고 새로 만들어진 블록을 이전 블록체인에 연결하고, 그 사본을 만들어 각 사용자 컴퓨터에 분산시켜 저장한다. 따라서 기존 은행처럼 거래 장부용 데이터베이스로 관리할 필요가 없어 관리 비용이 절감되며, 분산 처리로 해킹이 어려워 금융 거래의 안전성도 향상된다. (ex. 가상 화폐인 비트코인(Bitcoin))

* 브레드크럼즈 (breadcrumbs)
: 프로그램, 문서, 웹사이트 등에서 사용자의 탐색 경로를 시각적으로 제공해 주는 그래픽 사용자 인터페이스(GUI: Graphical User Interface).
예로, 전자상거래 경우 로그인, 쇼핑, 주문, 배송 정보 입력, 결제 정보 입력, 결제 완료 과정에 유용하다. 브레드크럼즈(breadcrumbs)는 헨젤과 그레텔 동화에서 자취를 남기기 위해 떨어뜨린 빵부스러기에서 이름을 인용하였다.

* OCAP (OpenCable Application Platform, 오픈케이블 응용 플랫폼)
: 모든 종합 유선 방송(CATV)에서 운용될 수 있도록 대화형(interactive) 텔레비전 서비스나 응용 프로그램을 설계할 수 있는 자바(Java) 기반의 미들웨어 소프트웨어 계층을 포함하는 디지털 케이블 방송 미들웨어(매개,중간 계층 프로그램) 표준.

[신기술 - 시스템 관리2]

* PIMS (Personal Information Management System, 개인 정보 관리 시스템)
: 현대인의 사회 생활과 개인 생활에서 발생되는 각종 정보를 효율적으로 관리해 주는 종합 시스템.

* ISMS (Information Security Management System 정보 보호 관리 체계)
: 정보 통신 서비스 제공자가 정보 통신망의 안정성 및 신뢰성을 확보하여 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위한 관리적·기술적 수단과 절차 및 과정을 체계적으로 관리, 운용하는 체계. 2010년부터 행정 기관은 정보 보호 관리 시스템 인증(ISO/IEC 27001)을 의무적으로 받아야 한다.

* extranet (엑스트라넷)
: 월드 와이드 웹(WWW)과 같은 인터넷 기술을 사용하여 기업체 내의 각 부문 간에 정보를 공유하기 위해 구축된 시스템이 인트라넷(intranet)인데, 납품업체나 고객업체 등 자기 회사와 관련 있는 기업체들과의 원활한 통신을 위해 인트라넷의 이용 범위를 그들 관련 기업체 간으로 확대한 것. 엑스트라넷은 '외부'를 의미하는 extra와 통신망을 의미하는 net을 합성한 조어이다.

* SSO (Single Sign-On)
단 한번의 로그인만으로 기업의 각종 시스템이나 인터넷 서비스에 접속하게 해주는 보안 응용 솔루션.

* EAM (Extranet Access Management, 엑스트라넷 접근 관리)
: 인트라넷, 엑스트라넷 및 일반 클라이언트/서버 환경에서 자원의 접근 인증과 이를 기반으로 자원에 대한 접근 권한을 부여・관리하는 통합 인증 관리 솔루션. 하나의 ID와 암호 입력으로 다양한 시스템에 접근할 수 있고 각 ID에 따라 사용 권한을 차등 부여하는 통합 인증과 권한 관리 시스템이다.
EAM = SSO + 권한관리 + 자원관리기능 + 보안정책수립 기능

[신기술 - 시스템 관리2]

* e-discovery (electronic discovery, 전자 증거 수집)
: 법적 증거로 사용할 목적으로 전자 데이터를 수집•조사•확보하는 절차. 중요 증거를 획득하기 위해 법원 명령이나 정부의 합법적 해킹 방법을 사용하기도 하며, 특수한 컴퓨터나 네트워크를 이용하기도 한다. 전자 증거 수집 과정에서는 모든 데이터가 증거로 채택되며, 거기에는 문서, 영상, 일정 파일, 데이터베이스, 스프레드시트, 음성 파일, 에니메이션, 웹사이트 및 컴퓨터 프로그램 등이 포함된다. 또한 바이러스나 스파이웨어 등 멀웨어도 확보•조사한다. 특히 이메일 같은 데이터는 일반 인쇄물보다도 증거 수집에 매우 유용하게 사용된다. 컴퓨터 포렌식스 (범죄에 사용된 컴퓨터나 범죄 행위를 한 컴퓨터로부터 디지털 정보를 수집하고 범죄의 증거를 확보하는 기술) 도 하드드라이브의 데이터를 조사하는 일종의 전자 증거 수집 형태이다.

* 토큰화 (tokenization)
: 모바일 결제 시스템에서, 신용카드와 같은 개인 정보를 보호하기 위해 관련 정보를 토큰(부호, 표지, 표 등)으로 변환하여 사용하는 방식. 금융 보안 분야에서 개인 정보를 보호하기 위해 보호되어야 할 신용카드나 개인 정보를 토큰화 하여 결제 시 원본 데이터 대신 토큰 데이터를 사용한다.

* HSM (Hardware Security Module, 보안 토큰)
: 전자 서명 생성 키 등 비밀 정보를 안전하게 저장, 보관할 수 있고 기기 내부에 프로세스 및 암호 연산 장치가 있어 전자 서명 키 생성, 전자 서명 생성 및 검증 등이 가능한 하드웨어 장치. 기기 내부에 저장된 전자 서명 생성 키 등 비밀 정보는 장치 외부로 복사 또는 재생성되지 않는다.

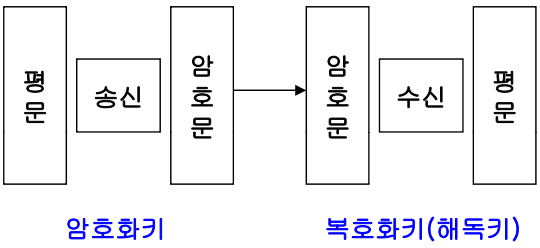
* Smart Token
: 보안 기능과 IC 카드 기능을 하나로 통합. 은행카드 기능을 내장한 IC칩, 보안모듈, CPU, 메모리, 공인인증서를 탑재해 기본적인 보안기능에 인터넷뱅킹, 전자통장, IC 카드 등의 기능을 제공한다.

[신기술 - 시스템 관리2]

* 암호화 기법

1) 개인키(Private) 암호화 알고리즘 : DES (암호화키 = 복호화키)
- 동일한 키를 이용하는 방식 → 보안 수준이 낮음
→ 알고리즘이 단순하고, 빠르다.

2) 공개키(Public) 암호화 알고리즘 : RSA
- 암호화키(Public Key) <> 복호화키(Private Key)
- 서로 다른 키를 사용하는 비대칭 암호화 방식
→ 보안 수준이 높음 → 속도가 느리고 알고리즘 복잡. 파일 크기도 크다.



* 인증 기관 (Certification Authority)

: 보안 적격 여부 및 메시지 암호화를 위한 공개 키의 발급과 관리를 담당하는 신뢰성이 보장된 온라인상의 기관.

* 공인 인증서 (Accredited Certificate)

: 전자서명법에 근거하여 공인인증기관이 발행한 인증서. 특정 홈페이지의 로그인 수단으로도 활용되고 있다.

* OTP (One-Time Password, 일회용 패스워드)

: 로그인 할 때마다 그 세션에서만 사용할 수 있는 일회성 패스워드를 생성하는 보안 시스템. 동일한 패스워드가 반복해서 재사용됨으로써 발생할 수 있는 패스워드 도난 문제를 예방하는 것이 목적이다. (ex. 은행 보안카드 대신)

[신기술 - 시스템 관리2]

* CRL (Certificate Revocation List, 인증서 폐기 목록)

: 더 이상 유효하지 않은 인증서 목록. 인증서 폐기 목록에는 취소된 인증서들의 일련번호가 들어 있으며 이를 받은 당사자는 목록을 참조하여 폐기된 인증서를 사용하지 않도록 해야 한다. 폐기된 인증서를 이용자들이 확인할 수 있도록 하기 위해 주로 인증 기관이 관리하며 메시지를 전달할 때 인증서와 함께 전달된다.

* Key Pair

: 공개키 암호 알고리즘에 사용되는 개인키(private key)와 공개키(public key)쌍.

* WPKI (Wireless Public Key Infrastructure, 무선 공개 키 기반 구조)

무선 인터넷상에서의 인터넷 뱅킹, 사이버 주식 거래시 외부 침입이나 정보 누출로부터 보호받을 수 있도록 하는 무선 인터넷 공개 키 기반 구조. PKI 기술의 핵심인 비밀성, 무결성 및 신원 확인과 부인 방지 같은 서비스를 무선 환경에서 구현함으로써 무선 보안을 가능케 한다.

* ActiveX

: 마이크로소프트 윈도우(Microsoft Windows) 환경에서 인터넷을 통해 다운 받은 내용을 쉽게 이용할 수 있도록 마이크로소프트사에서 개발한 소프트웨어 프레임워크. 인터넷 익스플로러(Internet Explorer) 브라우저를 위해 고안되었다. (일반 응용프로그램과 웹을 연결시키기 위해 제공되는 기술)

* i-PIN (internet personal identification Number, 인터넷 개인 식별 번호)

: 웹 사이트에 주민 등록 번호 대신 이용할 수 있는 사이버 신원 확인 번호로서 인터넷상에서 주민 등록 번호가 유출되어 도용되는 부작용을 막기 위해 만든 서비스.

[신기술 - 시스템 관리2]

* G-PIN (Government-Personal Identification Number, 정부 개인 식별 번호) → 공공 i-PIN
: 정부가 추진하고 있는 주민 등록 번호 대체 수단.

* MY-PIN
: 주민등록번호를 대신할 수 있는 무작위 13자리 번호. 인터넷이 아닌 일상생활에서 사용할 수 있는 본인확인 수단

* SMishing (스미싱)
: SMS와 Phishing의 결합어로 문자메시지를 이용 피싱하는 방법. 이 기법을 사용하는 해커는 핸드폰 사용자에게 웹사이트 링크를 포함한 문자메시지를 보내고 휴대폰 사용자가 웹사이트에 접속하면 트로이목마를 주입해 인터넷 사용이 가능한 휴대폰을 통제할 수 있게 된다.

* spear phishing (스피어 피싱)
: 조직 내에 신뢰할 만한 발신인으로 위장해 ID 및 패스워드 정보를 요구하는 일종의 피싱 공격.

* SQL 주입 공격 (SQL injection)
: 웹 클라이언트의 반환 메시지를 이용하여 불법 인증 및 정보를 유출하는 공격. 웹 응용 프로그램에 강제로 SQL 구문을 삽입하여 내부 데이터베이스(DB) 서버의 데이터를 유출 및 변조하고 관리자 인증을 우회할 수도 있다.

* Key Logger Attack
: 컴퓨터 사용자의 키보드 움직임을 탐지해 ID나 패스워드, 계좌 번호, 카드 번호 등과 같은 개인의 중요한 정보를 몰래 빼 가는 해킹 공격.

[신기술 - 시스템 관리2]

* Spyware
: 사용자의 동의 없이 또는 사용자를 속여 설치되어 광고나 마케팅용 정보를 수집하거나 중요한 개인 정보를 빼가는 악의적 프로그램.

* Worm virus (웜 바이러스)
컴퓨터 바이러스 종류의 하나. '컴퓨터에 근거지를 둔 지렁이와 같은 기생충'이란 의미의 부정 프로그램이다. 보통 'worm'이라고 한다. 컴퓨터 바이러스와 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해서 널리 퍼진다.

* Cracking
: 허가받지 않은 시스템에 강제로 침입하여 정신적인 피해나 물리적인 피해를 주는 것 (Hacking: 순수 연구 목적)

* Hoax (가짜 바이러스)
: 공신력 있는 기관을 사칭하거나 복잡한 기술 용어를 사용하여 사용자를 속이는 바이러스. 전자 우편, 인터넷 메신저, 문자 메시지 등의 통신 수단에 거짓 정보 또는 유언비어, 괴담 등을 마치 사실인 것처럼 사용자를 속이는 바이러스를 말함. (ex. 행운의 편지)

* Dropper
: 자기 자신을 복제하는 바이러스 코드는 없지만 실행할 때 바이러스를 불러와 전파할 수 있는 악성 실행 파일. 컴퓨터를 쓰는 사람이 알 지 못하는 순간에 바이러스나 트로이 목마 프로그램을 사용자 컴퓨터에 설치하는 악성 프로그램이다. 한 번 감염되면 악성 코드 수십 개를 생성하는 '멀티 드로퍼(Multi Dropper)'로 악화되고 있어 주의해야 한다.

[신기술 - 시스템 관리2]

* Dyre malware (다이어 악성코드)
: 사용자 컴퓨터에 악성코드를 설치하는 트로이목마(계속적인 비합법적 침투가 가능하도록 시스템 내에 코드를 놓음)의 한 종류. 주로 윈도우(Windows) 운영 체제를 사용하는 금융 기관을 대상으로 전자우편(이메일) 첨부 파일을 통해 악성코드를 유포한다. 첨부 파일을 실행시키면 악성 프로그램이 설치되거나 가짜 웹사이트로 접속되어 금융 정보가 유출된다.

* Memory Hacking
: 메모리에 상주한 데이터를 위·변조하는 해킹. 기존의 해킹 방법은 외부에서 계좌 비밀 번호를 빼내는 방법에 초점을 맞춘 반면, 메모리 해킹 방법은 비밀문 같은 프로그램을 설치하고, 컴퓨터 메모리에 있는 비밀 번호를 빼내는 것뿐 아니라 데이터를 조작하여 받는 계좌와 금액까지 변경할 수 있는 해킹 방법이다.

* rootkit
: 시스템 침입 후 침입 사실을 숨긴 채 차후의 침입을 위한 백도어, 트로이목마 설치, 그리고 원격접근, 내부 사용흔적 삭제, 관리자권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램들의 모음.

* grayware
: 정상 소프트웨어와 바이러스 소프트웨어의 중간에 해당하는 일종의 악성 소프트웨어.

* Honey pot (허니팟)
: 해커를 잡기 위해 유인하는 시스템. 해커를 향한 달콤한 유혹이라는 뜻에서 꿀단지라고도 한다. 해커를 유인하기 위한 위장 서버와 추적 탐지용 소프트웨어로 구성된다.

[신기술 - 시스템 관리2]

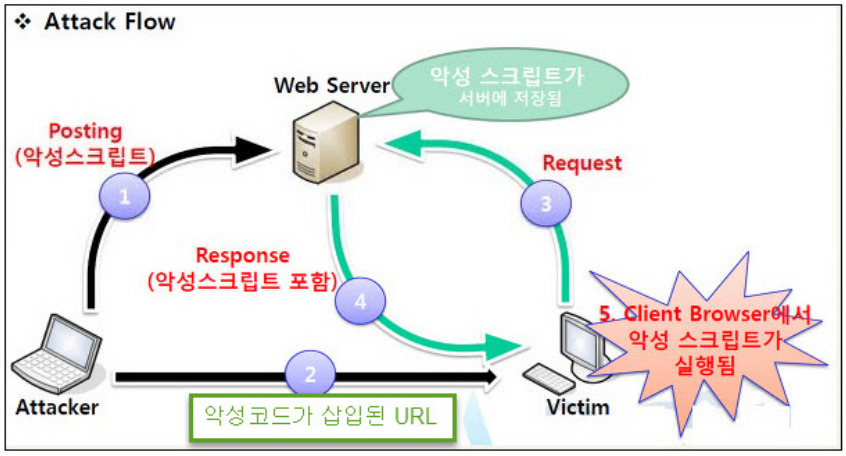
* CERT (computer Emergency Response Team, 침해 사고 대응팀)
: 인터넷의 보안에 관한 문제와 보고를 실시하는 공식적인 비상 대응팀. 일종의 파괴 프로그램인 웜(worm)으로부터 급습 사고가 있은 직후인 1988년 11월에 미국국방부고등연구계획국(DARPA)에서 구성되었으며, 인터넷의 보안에 관한 공동의 인식을 증진시키고 사고 처리 및 예방을 위한 정책 수립 등을 수행하는 한편, 지속적으로 공공 인식 캠페인과 보안 시스템을 개선·연구하고 있다. 미국 피츠버그의 카네기 멜론 대학에 있다. 이와 같은 업무를 하기 위한 우리나라의 대표적인 침해 사고 대응팀(CERT)은 인터넷 침해 사고 대응 지원 센터(KrCERT/CC)가 있다.

* 익스플로잇 공격 (exploit) → 취약점 공격
: 컴퓨터나 컴퓨터 관련 전자제품의 보안 취약점을 이용한 공격 방법.
취약점 공격에는 보안 취약점의 종류에 따라 BOF 취약점 공격, CSRF 취약점 공격, XSS 취약점 공격 등이 있다.

* BOF (buffer overflow)
: 메모리를 다루는 데에 오류가 발생하여 잘못된 동작을 하는 프로그램 취약점이다. 이로 인해 잘못된 프로그램 동작이 나타날 수 있으며, 메모리 접근 오류, 잘못된 결과, 프로그램 종료, 또는 시스템 보안 누설이 발생할 수 있다.

[신기술 - 시스템 관리2]

* XSS (Cross Site Scripting)
: 게시판, 웹 메일 등에 삽입된 악의적인 스크립트에 의해 페이지가 깨지거나 다른 사용자의 사용을 방해하거나 쿠키 및 기타 개인 정보를 특정 사이트로 전송시키는 공격.



* CSRF (Cross Site Request Forgery)
: 세션 쿠키, SSL 인증서, 윈도 도메인 인증과 같이 자동으로 입력된 신뢰 정보를 기반으로 한 웹 애플리케이션에서 사용자의 신뢰 정보 내에서 사용자의 요청을 변조함으로써 해당 사용자의 권한으로 악의적인 공격을 수행하는 것.
웹 2.0 환경에서 전통적인 교차 사이트 스크립팅(XSS) 기반의 공격과 함께 매우 효과적인 공격 기법.
→ CSRF 스크립트가 서버에서 실행됨

[신기술 - 시스템 관리2]

* 막대형 컴퓨터 (PC-on-a-stick)
: 유에스비(USB) 메모리 장치 같이 생긴 작은 막대형 컴퓨터. 고화질 멀티미디어 인터페이스(HDMI) 포트가 지원되는 모니터만 있으면 막대형 컴퓨터(스틱 컴퓨터)를 바로 연결하여 인터넷, 동영상 재생, 문서 작성 등 간단한 작업을 할 수 있다.

* UASP (USB Attached SCSI Protocol)
: 유에스비(USB) 3.0 표준 규격에 스카시(SCSI) 프로토콜이 탑재되어 데이터 이동 속도가 개선된 컴퓨터 프로토콜.
- SCSI: 소형 컴퓨터의 입출력 버스 인터페이스.

* 모바일 광개토 플랜
: 이동통신 주파수를 추가 확보하기 위한 우리나라의 모바일 광대역 계획. 모바일 광개토 플랜은 2011년 방송통신위원회가 우리나라의 모바일 광대역을 위하여 2020년까지 이동통신용으로 600 메가헤르츠(MHz) 대역폭을 추가로 확보하려는 계획이다.

* SCO (Synchronous Connection Oriented link, 동기식 접속 지향 링크)
: 블루투스 데이터 링크의 하나. 두 장비 간에 음성과 같이 지정된 대역폭 통신을 위한 전용 회선의 동기식 접속 방법이다.