0001 모델옵스(ModelOps)

- 기계 학습* 모델의 생명주기를 효과적으로 관리하고 원활하게 해 주는 기계 학습 모델 관리 방법론이다.
- 기존에 수작업으로 수행했던 모델 학습과 배포 과정을 모두 자동화하여 체계적이고 고도화된 기계 학습 서비스를 제공한다.

• **기계 학습(Machine Learning)** : 컴퓨터가 마치 사람처럼 스스로 학습할 수 있어 정형화된 데이터를 입력받지 않고도 스스로 필요한 데이터를 수집·분석하여 고속으로 처리하는 기술

0002 확장 현실(擴張現實, eXtended Reality)

- 가상 현실(VR), 증강 현실(AR), 그리고 혼합 현실(MR)*을 모두 아우르는 개념으로, 광범위하고 다양한 수준의 초실감형 기술 및 서비스를 의미한다.
- 확장 현실이 진화하면 시야를 모두 가리는 헤드셋형 단말기 없이 안경 형태의 기기만으로 증강 현실이 필요할 때는 안경 위에 정보가 표시되고, 가상 현실이 필요할 때는 시야 전체로 정보를 보여주는 것이 가능해 진다.

• **혼합 현실(Mixed Reality)** : 가상 현실에서 현실에 실존하는 물건을 구현하거나, 현실에서 존재하지 않는 가상의 물건을 구현하는 등 기존의 가상 현실(VR), 증강 현실(AR) 등의 기술을 혼합한 것

0003 릴리즈 엔지니어링(Release Engineering)

- 안정적이고 신뢰성 있는 제품의 개발과 배포를 연구하는 소프트웨어 공학(Software Engineering) 분야를 의미한다.
- 소프트웨어 개발 생명 주기의 과정 중 구현, 시험, 배포, 유지보수와 관련이 있다.
- 모든 과정을 파이프라인 방식으로 구축하고 자동화한다는 특징이 있다.

0004 PEM(Privacy Enhanced Mail)

- 인터넷 표준화 조직인 IETF에서 1993년 제정한 전자 우편 보안 표준이다.
- 개인키를 이용한 암호화를 통해 비밀성, 무결성, 인증 등의 보안 기능을 제공하지만, 구조의 불편함으로 인해 PGP가 주로 사용되고 있다.

0005 PGP(Pretty Good Privacy)

- '아주 좋은 프라이버시'라는 의미를 가진 전자 우편 보안 시스템이다.
- 보안성이 비교적 떨어지지만, 구현이 용이하고 암호화 알고리즘의 안전성이 높아, IETF에서 제정한 표준인 PEM보다 전 세계적으로 더 널리 사용되고 있다.

0006 딥페이크(Deepfake)

- 인공지능(AI)을 기반으로 하는 딥 러닝(Deep Learning)* 기술로, 이미지를 합성하는 기술이다.
- 정치인, 연예인 등 유명인의 사진이나 동영상들을 딥 러닝을 통해 학습시킨 후 성인 비디오 배우의 얼굴에 이를 합성시키는 형태로 사용되어 많은 논란을 일으키고 있다.
- 기술이 날로 정교해짐에 따라 영상의 합성 여부를 판단하기 어려워 명예 훼손뿐만 아니라, 가짜 뉴스, 사기 행각 등에 활용될 우려가 있다.

• 딥 러닝(Deep Learning) : 인간의 두뇌를 모델로 만들어진 인공 신경망을 기반으로 하는 기계 학습 기술

0007 가상 머신(Virtual Machine)

- 특정한 프로그램이 실행될 수 있도록 실제 컴퓨터 시스템에 소프트웨어적으로 구성한 또 다른 가상의 컴퓨팅 환경을 의미한다.
- 하나의 컴퓨터 시스템에 다수의 가상 머신이 수행될 수 있으며, 각 가상 머신은 별개의 물리적 컴퓨터처럼 독립적으로 서로 다른 운영체제(OS)나 앱을 실행할 수 있다.

0008 하이퍼바이저(Hypervisor)

- 가상 머신을 생성하고 구동하는 소프트웨어로, 가상 머신 매니저(VMM) 또는 가상 머신 모니터(VMM)라고도 불린다.
- 가상 머신이 시스템 가용 리소스를 더 효율적으로 활용할 수 있도록 지원하며, 가상 머신 간의 제어 이동이 자유롭다.

0009 메타버스(Metaverse)

- 초월을 의미하는 메타(meta)와 현실 세계를 의미하는 유니버스(universe)의 합성어로, 현실 세계와 같이 사회, 경제, 문화 활동이 이뤄지는 3차원의 가상 세계를 의미한다.
- 언택트* 문화가 나타나고, 가상현실(VR)이나 증강현실(AR)에 대한 기술이 발전하자 메타버스에 대한 관심 또한 증가하고 있다.

- **언택트(untact)** : 판매자와 소비자의 만남 없이 물건을 구매하는 소비 현상

0010 디피-헬만 알고리즘(Diffie-Hellman Algorithm)

- 암호화되지 않은 통신망에서 비밀 정보를 공유하기 위해 고안된 암호화 알고리즘이다.
- 1976년 디피(Diffe)와 헬만(Hellman)이 발명하였으며, 이산대수의 복잡성을 활용한다는 특징을 갖고 있다.

0011 가상 울타리(Geo-fence)

- 위치 기반 서비스(LBS)*를 이용하여 특정 영역에 설치하는 가상의 경계를 의미한다.
- 경계가 설정된 영역에 대한 출입 현황을 확인할 수 있어, 이를 이용한 보안시설 및 금지구역에 대한 출입 관리, 어린이 보호, 치매 환자 보호 등이 가능하다.

- **위치 기반 서비스(LBS)** : 위성 위치 확인 시스템(GPS)이나 통신망을 활용하여 얻은 위치 정보를 바탕으로 제공되는 네비게이션, 지도, 게임 등의 다양한 서비스

0012 터널 링크 기술(Tunnel Link Technique)

- 웹상에 존재하는 라우터-라우터 간을 가상의 터널로 연결하여 패킷 통신로로 활용하는 기술이다.
- 데이터를 캡슐화하여 정보를 웹상에 안전하게 유통시킬 수 있는 기술이며, 외부에서는 그 터널 안 패킷이 보이지 않으므로 안전한 가상 사설 통신망(VPN)*이 구축될 수 있다.

- **가상 사설 통신망(VPN)** : 공중망 상에 사설망을 구축해 마치 사설 구내망, 전용망 같이 이용하는 통신망

0013 데브옵스(DevOps)

- 소프트웨어 개발 방법론의 하나로, 소프트웨어 개발과 IT 운영을 병행하고 협업하는 방식이다.
- 시스템 개발자와 운영을 담당하는 정보기술 전문가 사이의 소통, 협업, 통합 및 자동화를 강조하는 소프트웨어 개발 방법론이다.

0014 마이크로커널(Microkernel)

- 운영체제(OS)의 기본적인 기능을 제공하는 핵심부(커널)를 필수 기능만을 가진 형태로 소형화한 것이다.
- 주로 처리 제어나 장치 구동기 등 하드웨어에 의존하는 기능이나 실시간 처리에 필요한 기능만을 가지고 있다.

0015 멀티테넌시(Multitenancy)

- 모든 사용자가 웹을 통해 단일 데이터베이스 안의 정보를 관리하고 공유할 수 있게 하는 기술이다.
- 클라우드 컴퓨팅*에서는 서로 다른 고객이 서버 자원을 나누어 사용하는 공유 호스팅을 멀티테넌시라고 부른다.

• **클라우드 컴퓨팅** : 인터넷의 기술을 활용해 가상화된 정보 기술(IT) 자원을 서비스로 제공하는 컴퓨팅

0016 포스트 양자 암호(量子暗號, Post-Quantum Cryptography)

- 양자 컴퓨터(Quantum Computer)*가 등장한 이후 발생하는 해킹(Hacking)에 대응하기 위해 개발된 비대칭 키 암호 알고리즘이다.
- 양자의 특성을 활용한 양자 암호 방식과는 달리 기존의 암호 알고리즘처럼 수학적 난제를 활용하여 암호화를 수행한다.

• **양자 컴퓨터(quantum computer)** : 양자 역학의 원리를 응용한 컴퓨터

0017 템페스트(Transient ElectroMagnetic Pulse Emanation Surveillance Technology)

- 정보통신 기기에서 발생하는 기생 방사*나 고조파 방출*과 같이 원하지 않는 전자파 방출을 수신하고 복원·분석하여 정보를 도청하는 기술과 이를 방어하는 기술이다.
- 미국 국가안보국(NSA)에서는 템페스트의 표준 사양을 설정하고, 인증 시스템을 운영하고 있다.

• **기생 방사(parasitic emission)** : 필요 주파수 이외의 주파수가 방출되는 것
• **고조파 방출(harmonic emission)** : 기본 주파수의 n배에 해당하는 주파수를 방출하는 것

0018 루트킷 툴(Rootkit Tool)

- 자기 자신 혹은 다른 프로세스의 존재를 숨겨주는 소프트웨어이다.
- 커널에 숨어 동작하기 때문에 탐지 및 분석이 어려워 바이러스나 악성 코드들이 발각되지 않고 동작하는 데 도움을 주기도 한다.

0019 비비84 프로토콜(BB84 protocol)

- 양자가 가진 특징을 기반으로 무조건부 안전성*이 증명된 최초의 양자 암호키 분배(Quantum Key Distribution)* 프로토콜이다.
- 이 프로토콜은 송신자와 수신자 간 암호키 분배 과정 중에 도청이 있을 경우 양자 역학의 원리에 의해 도청 여부가 드러날 뿐만 아니라 도청자도 정확한 정보를 얻을 수 없는 보안성을 가진다.

- **무조건부 안정성** : 도청자의 능력과 무관하게 암호 해독이 불가능한 안정성
- **양자 암호 키 분배(QKD; Quantum Key Distribution)** : 양자 통신을 위해 비밀키를 분배·관리하는 기술

0020 앱 추적 투명성(ATT; App Tracking Transparency)

- 특정 앱이 사용자의 개인정보를 무분별하게 수집하는 것을 막기 위해 사전 동의를 의무화한 애플의 개인정보보호 정책이다.
- 이로 인해 사용자 모르게 개인정보를 수집하여 표적 광고를 노출시켰던 앱들은 처음 실행 시 앱 추적 동의 여부를 묻는 팝업 창을 띄우게 되었다.

0021 동형 암호(同型暗號, Homomorphic Encryption)

- 데이터를 암호화한 상태로 복호화하지 않고 처리 또는 사용하게 해 주는 암호화 방식이다.
- 동형 암호는 2011년 미국 매사추세츠공대(MIT)가 선정한 미래 10대 유망기술 중 하나로 꼽혔다.
- 정보의 유출은 데이터를 분석하기 위해 암호화를 하고 이를 다시 푸는 과정에서 발생하기 때문에 동형 암호를 활용하게 되면 정보 유출 위험을 훨씬 낮출 수 있다.

0022 뱅쿤(Bankun)

- 모바일 환경의 악성코드로, 스마트폰에 설치된 정상 은행 앱을 삭제한 후 악성 은행 앱 설치를 유도하는 모바일 악성코드다.
- 뱅쿤 앱은 설치할 때 동일한 아이콘뿐만 아니라 '구글 플레이 스토어(Google Paly Store)'라는 유사한 앱의 이름을 사용하고 있으므로 주의 깊게 살펴보지 않으면 예기치 않게 악성 앱을 설치하기 쉽다.

0023 청색 폭탄(青色爆彈, Blue Bomb)

- 자신과 통신하고 있는 사람의 윈도 운영체제(OS)를 충돌 또는 중단되게 하는 수법이다.
- 운영체제가 수행할 수 없을 정도로 많은 양의 정보를 포함한 패킷으로 인하여 운영체제가 충돌되거나 중단된다.

0024 비무장 지대(非武裝地帶, Demilitarized Zone)

- 웹상에 공개하는 서버에 부정 접속을 방지하기 위한 침입 차단(Firewall) 기능이다.
- 외부 인터넷 측과 내부 통신망 측 사이에 비무장 지대(DMZ)를 설치하고 침입 차단 시스템을 운용하여 외부로부터 오는 신호를 여과 처리함으로써 부정 접속을 방지한다.

0025 립프로그 공격(Leapfrog Attack)

목표 호스트를 공격하기 전 추적을 불가능하게 하기 위해 불법적으로 얻은 ID와 암호 정보를 이용하여 하나 이상의 호스트를 경유하는 것을 의미한다.

0026 Nmap(Network Mapper)

- IP 패킷을 이용하여 원격 컴퓨터의 정보를 조회하는 보안 스캐너이다.
- 주요 기능에는 호스트 탐지, 포트 탐지, 버전 탐지*, 운영체제 탐지가 있다.

• **버전 탐지 :** 원격 컴퓨터에서 실행 중인 서비스의 버전을 확인하는 기능

0027 SET(Secure Electronic Transaction)

- 안전한 전자상거래를 보장하기 위한 프로토콜 규격이다.
- 디지털 인증서와 전자서명을 조합하여, 구매자와 판매자, 그리고 거래 은행 사이에서 기밀을 보장한다.

0028 CSRF / XSRF(Cross Site Request Forgery)

- 사용자의 요청을 위조하여 전달하는 공격 기법이다.
- 사용자가 로그인한 상태에서 위조 코드가 삽입된 웹페이지를 열면 위조된 요청이 사용자가 보낸 것처럼 공격 대상인 웹사이트에 전달되는 방식이다.

0029 개방 보안 환경(Open Security Environment)

시스템이 작동하기 전 혹은 작동하는 중 발생하는 악의적인 행위로부터 응용 프로그램 및 장비를 보호할 수 있는 환경이 충분히 갖춰지지 않은 것을 의미한다.

0030 커버로스(Kerberos)

- 분산 컴퓨팅 환경에서 대칭키 암호를 사용하여 상호 인증 서비스를 제공하는 암호화 프로토콜이다.
- MIT에서 개발하였으며, 커버로스 프로토콜로 생성된 메시지는 인증 메커니즘으로 인해 여러 형태의 공격을 막을 수 있다.