# 1 기본 요소

## 1 패스워드

- 가장 널리 사용되는 기본적인 사용자 인증 방식
  (아이디 - 1중 보안, 아이디/패스워드 - 2중 보안)

## 2 안전한 패스워드 만들기

### [패스워드를 만들 때 고려할 사항]

| 속성 | 설명 | 예시 |
|---|---|---|
| 길이 | 세 종류 이상의 문자 구성으로 여덟 자리 이상 | abc123!@ |
| | 두 종류 이상의 문자 구성으로 열 자리 이상 | angel12345 |
| 형태 | 특정 명칭을 예측이 어렵도록 가공 | '인터넷해킹과보안'의 경우 홀수번째 문자인 '인넷킹안'을 영문으로 입력한 'dlsxptzlddks' |
| | 노래 제목이나 명언, 속담, 가훈 등을 가공 | '백설공주와 일곱 난쟁이'를 '백설+7난장'으로 줄인 후 영문으로 입력한 'qortjf+7skswkd' |
| | 패스워드 길이를 증가시키기 위해 알파벳 문자 중간에 특수문자나 숫자 삽입 | Security1을 'Se1cu@@rity'로 가공 |
| | 기본 패스워드 문자열을 설정한 뒤 사이트별 특정 규칙 적용 | 기본 문자열을 i486U로 설정하고 사이트 이름을 앞뒤에 추가한 'da+i486U+um'이나 'na+i486U+ver' |

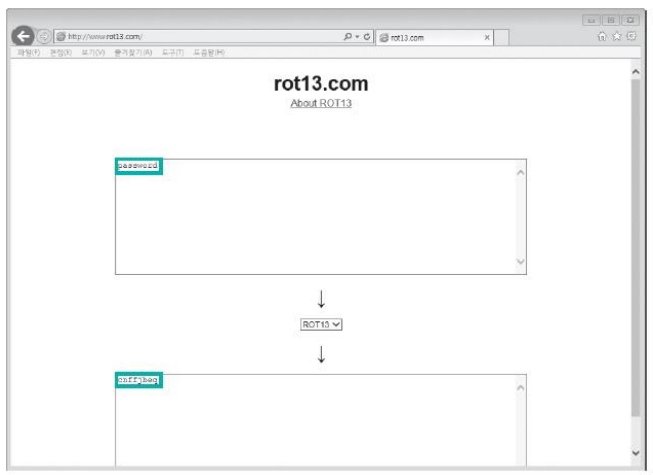
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 1 패스워드 변형

- http://www.rot13.com

[패스워드를 ROT13 방식으로 디코딩한 경우]




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 1 패스워드 변형

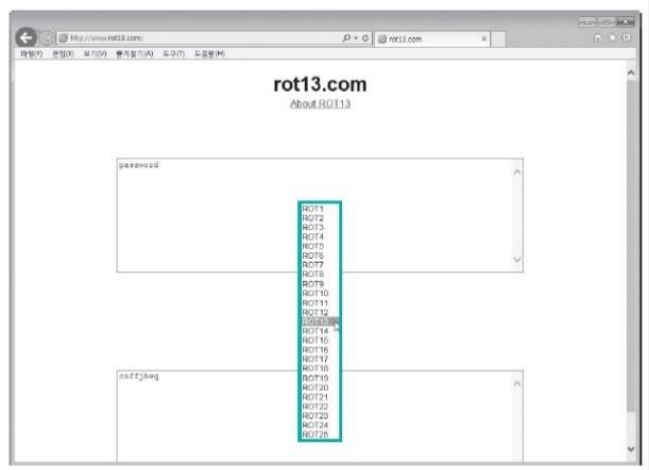
- ROT13 방식
  : 영어 알파벳을 열세 글자씩 밀어서
  암호로 만드는 방법
- ROT1부터 ROT25까지 다양한 방식의
  인코딩/디코딩 선택 가능

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 1 패스워드 변형

- http://www.rot13.com

[다양한 방식의
인코딩/디코딩 선택 가능]



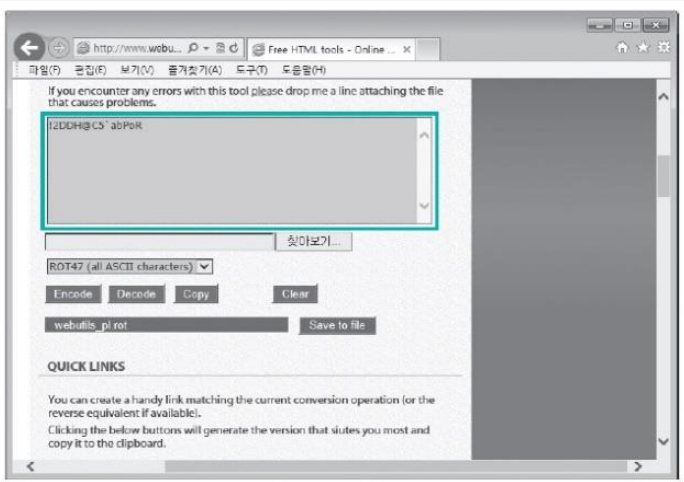

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 1 패스워드 변형

- http://www.webutils.pl/ROTencode

['Password123!@#'를 ROT47로 치환]




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

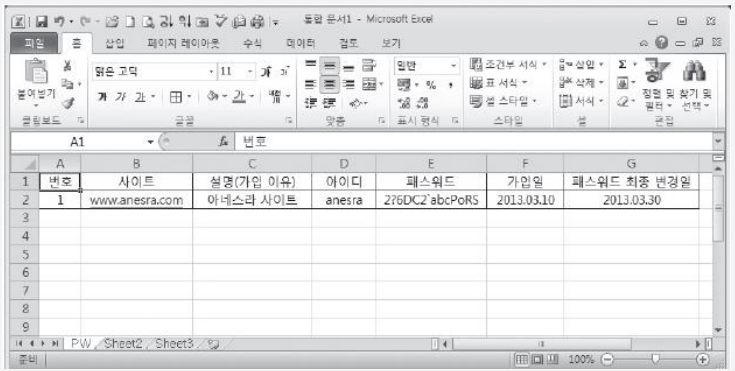
1. 패스워드 변형
   - ROT5, ROT13, ROT18, ROT47 방식의 인코딩/디코딩 선택 가능
   - ROT18은 모든 문자, 숫자를 치환할 수 있고, ROT47은 모든 ASCII 치환 가능

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 2 패스워드 보관 파일의 암호화

- 액셀 파일에서 보안을 강화하려면 패스워드가 입력된 시트의 이름 부분에서 마우스 오른쪽 버튼을 누르고 [숨기기(H)] 선택

**[엑셀 파일에 사이트 가입 정보 저장]**



| 번호 | 사이트 | 설명(가입 이유) | 아이디 | 패스워드 | 가입일 | 패스워드 최종 변경일 |
|---|---|---|---|---|---|---|
| 1 | www.anesra.com | 아네스라 사이트 | anesra | 226DC2`abcPoRS | 2013.03.10 | 2013.03.30 |

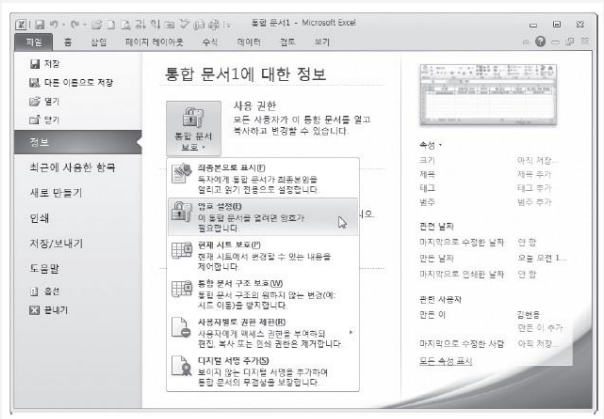
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 2 패스워드 보관 파일의 암호화

- Excel 2010의 경우에는 [파일]-[정보]-[통합 문서 보호]-[암호 설정]에서 패스워드를 설정할 수 있음

**[엑셀 파일에 패스워드 설정]**




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

3 외부 저장장치와 컴퓨터 하드디스크에 이중 보관

- 패스워드와 파일을 안전하게 보관해 놓으면 파일이 유출되더라도 패스워드까지 노출되는 위험을 줄일 수 있음(패스워드를 따로 안전하게 보관)

# 2 사용자 인증 수단

# 2 | 사용자 인증 수단

## 1 공인인증서

- 전자 서명의 검증에 필요한 공개키에 소유자 정보를 추가하여 만든 일종의 전자 신분증(증명서)
- 패스워드 인증 메커니즘보다 한 단계 강화된 사용자 인증 방식(입금 메시지)
- 공개키와 비밀키의 쌍을 이용하여 사용자를 인증하는 공개키 기반 구조(Public key infrastructure) 메커니즘 이용
- 공인인증서에 들어가는 정보는 ITU-T의 X.509 표준에 기술되어 있음 (http://www.itu.int/rec/T-REC-X.509/en)

# 2 | 사용자 인증 수단

## 1 공인인증서

- 공인인증서(公認認證書)는 전자 서명의 검증에 필요한 공개 키(전자서명법에는 전자서명검증정보로 표기)에 소유자 정보를 추가하여 만든 일종의 전자 신분증(증명서). 공개 키 증명서, 디지털 증명서, 전자 증명서 등으로도 불림. 공인인증서는 개인 키(전자서명법에는 전자서명생성정보로 표기)와 한 쌍으로 존재(사용자 - 공인인증서 - 은행)

# 2 | 사용자 인증 수단

## 1 공인인증서

- 공인인증서는 OpenSSL의 ssl-ca나 수세 리눅스의 gensslcert와 같은 도구를 포함한 유닉스 기반 서버용으로 작성, 비대면 온라인 방식의 전자상거래에서 상대방과의 계약서 작성, 신원확인 등에 전자서명이 필요하며 동시에 공인인증서로 해당 전자서명을 생성한 자의 신원을 확인함(부인 방지)

# 2 | 사용자 인증 수단

## 1 공인인증서

- 공개키 기반 구조 (PKI) 는 전자서명을 생성하고 검증하는데 사용되는 개인키와 공개키를 안전하게 나누어주는 역할을 담당하는 신뢰된 제3자(인증기관)의 존재를 전제로 하고 있음(등록기관)

- 한국의 공인인증서 제도 역시 공개키 기반구조에 입각한 제도임, 공개키 기반구조에 입각한 인증서는 서버의 신원을 확인하는데 사용되는 서버인증서와 이용자의 신원을 확인하는데 사용되는 개인인증서로 나누어 볼 수 있음(서버인증서, 개인인증서)

# 2 | 사용자 인증 수단

## 1 공인인증서

- 한국의 공인인증서도 이 두가지 용도에
  모두 사용될 수는 있지만, 한국의 공인인증서를
  서버인증서로 사용할 경우, 파이어폭스 웹브라우저는
  그러한 서버인증서를 신뢰하지 않으므로 현실적으로
  서버 신원 확인 용도로 한국의 공인인증기관이
  발급한 서버인증서를 사용하기는 무리가 따름,
  한국의 공인인증서는 따라서 개인인증서로
  주로 사용되고 있음(서버인증서 - 외국)

# 2 | 사용자 인증 수단

## 1 공인인증서

- 한국의 공인인증서 및 개인키 역시 파일 양식 자체는 국제표준을 따르고 있지만, 그 파일들이 보관, 저장되는 위치와 방법이 독특하여 웹브라우저로는 사용이 불가능하며, 그 결과 한국의 공인인증서를 이용하려면 이용자가 추가프로그램을 반드시 설치 해야만 함(불편함)

# 2 | 사용자 인증 수단

## 1 공인인증서

- 인증서는 원래 금융거래에만 사용되는 것이 아니라, 모든 전자적 거래(금전적이건 비금전적이건)에서 당사자의 신원을 확인하거나, 전자서명을 하는 용도로 사용될 수 있고, 한국의 공인인증서도 물론 그런 다양한 용도로 사용될 수 있음,

  그러나 현실적으로 공인인증서는 전자금융거래에서 주로 사용되고 있음 (사용자 - 공인인증서 - 은행)

  금융위원회는 전자금융거래에 “공인인증서 등”을 사용하도록 강제하고 있다가 의무사용 폐지됐음 (년 내 폐지 예정)

## 2 공인인증서에 포함되는 정보

| 속성 | 설명 |
|---|---|
| 일련번호 | 증명서를 개별 인증할 때 사용한다. |
| 주체 | 사람의 이름이나 증명자이다. |
| 서명 알고리즘 | 서명을 만드는 데 사용하는 알고리즘이다. |
| 발행자 | 정보를 검증하고 증명서를 발행하는 주체이다. |
| 유효 기간(시작) | 처음 효력이 발생한 날짜이다. |
| 유효 기간(끝) | 효력 만기일이다. |
| 키 이용 목적 | 공인키의 사용 목적(예: 서명, 인증 서명 등)이다. |
| 공인키 | SSL 목적이다. |
| 지문 알고리즘 | 인증서를 해시하는 데 사용하는 알고리즘이다. |
| 지문 | 증명서가 개봉되지 않았음을 증명하는 해시 자체이다. |

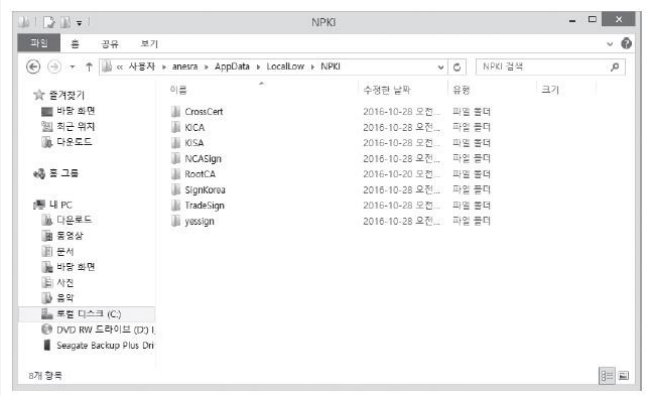
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 1 공인인증서가 있는 폴더 탐색

- 윈도우 7 이후부터는 공인인증서 파일이 C:₩Users₩사용자계정₩AppData₩LocalLow 폴더에 저장

**[공인인증서가 저장된 폴더]**




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

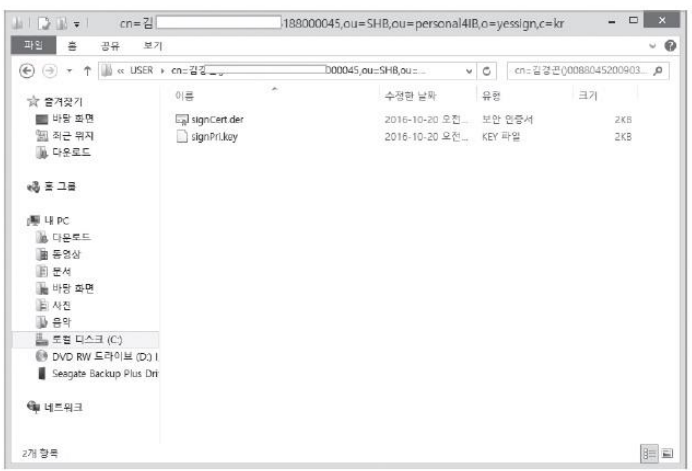
2 yessign 폴더에서 개별 인증서 선택

- 개인 공인인증서 파일은 User 폴더 안에 있음
- signCert.der이 DER 암호화된 인증서 파일임
  더블 클릭하면 인증서에 대한 일반적인 내용을
  볼 수 있음

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 2 yessign 폴더에서 개별 인증서 선택

[개인 공인인증서 파일]

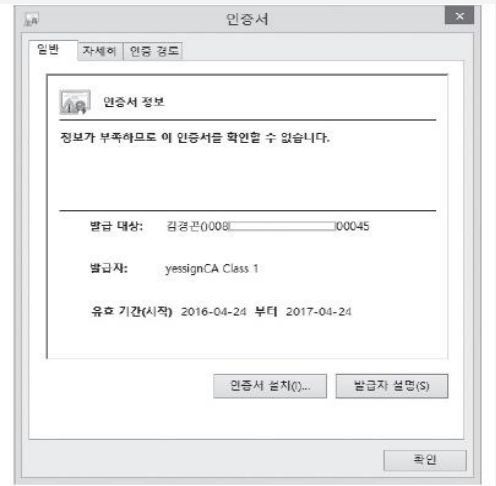



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 2 yessign 폴더에서 개별 인증서 선택

[공인인증서 파일 내용]



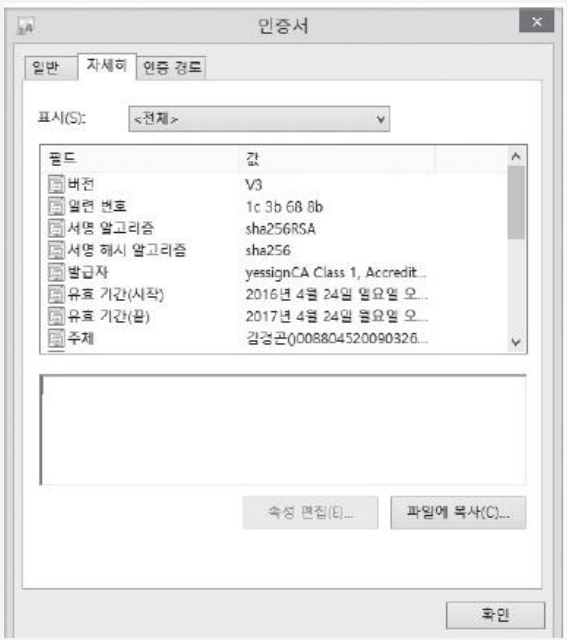

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 나만의 방식으로 안전하게 패스워드 관리하기

### 3 공인인증서 상세 보기

- 공인인증서 파일에서 [자세히] 탭을 클릭하면 공인인증서에 포함된 내용 및 구조를 살펴볼 수 있음

**[공인인증서 파일 상세 정보]**




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 생체 인증 방식

- 사용자를 인증하는 현존 방식 중 가장 강화된 것
- 모바일 시대가 열리면서
  생체 인증 방식이 도입되는 추세
- 얼굴, 음성, 지문, 홍채, 망막, 손 모양,
  손등 정맥, 귀 모양, 걸음걸이, 서명, DNA 등
- 가장 대중적으로 사용되는 것은 지문 인식
  (특징, 인식률)

## 4 생체 인증 방식

[생체 인식 기술 관련 동영상의 한 장면]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 5 생체 인증

- 신체인식은 통상 템플릿이라고 불리는 정보를 사전에 채취 및 등록해서 인증 할 때, 센서로 취득한 정보와 비교함(특징 추출)
- 단순히 이미지의 비교로 인증하는 방식부터 생체반응을 검출하는 방식까지 여러 가지 수준이 있음
- 비밀번호나 물건에 의한 인증방식은 망각이나 분실, 비밀번호 노출, 도난의 우려가 있음

## 5 생체 인증

- 생체정보의 경우에는 그런 위험성이 낮고, 비밀번호를 입력하거나 열쇠를 휴대하는 것이 불필요하며, 제삼자가 인증하는 것이 방지 가능한 수단으로(도용 방지), 공동주택의 입구, 신용카드나 생체 여권(입출국 시)의 인증수단으로 사용되고 있음

## 5 생체 인증

- 하지만 널리 사용될수록 상처, 병, 선천성 결손 등에 의해 생체인식이 불가능한 사람을 위한 대안이 필요함

  또한 복제되거나 신체기관의 노화로 인해 인식이 불가능해지는 경우가 있음(화장을 안하면?)

  생체정보는 비밀번호처럼 임의로 갱신하는 것이 불가능하기 때문에 한번 복제되면 안전성을 회복하는 것이 불가능할 수도 있는 치명적인 문제를 가지고 있음(영화 - 생체 복제)

## 6 지문

- 개인의 고유한 생체 정보로 일생 동안 변하지 않음
- 표피 면에서 위로 돌출된 융선과
  그 사이의 공간인 골로 구성
- 지문 등록(Enrollment)
  : 지문 센서로부터 입력 받은 고유한 특징을
  추출하여 데이터베이스에 저장하는 과정(특징 추출)
- 지문 인증(Verification)
  : 재입력된 지문으로부터 특징을 추출한 후 입력된
  데이터베이스의 내용과 비교하여 사용자를 인증
  (특징 추출)

## 6 지문

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 7 손 모양

- 손을 폈을 때 손가락의 길이와 굵기 등의 요소를 인증에 사용
- 비교적 간편하고 인증 데이터의 크기도 작은 편이어서 빠르게 인증 수행 (면적과 비례하지 않음)
- 인증 수준이 낮고 고무 인형 같은 것으로 손 모양 조작 가능

## 7 손 모양

- 적외선으로 손의 표피 가까이에 있는 정맥 모양을 촬영하여 인증하기도 함
  - 손 모양을 이용하는 것보다는 보안 수준이 높지만 장비가 크고 비싸다는 것이 단점(효용성?)

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 8 망막

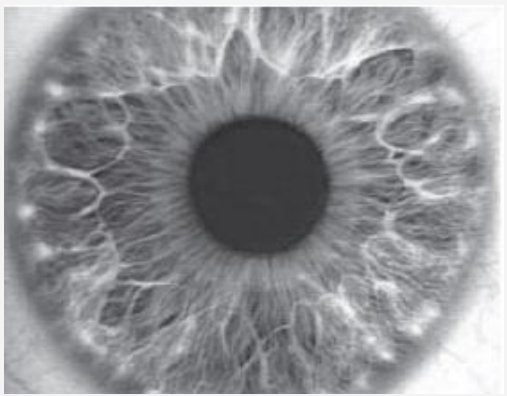
- 눈 뒷부분에 있는 모세혈관의 형태를 확인하여 인증
- 정확도가 매우 높은 편이지만 한 사람을 검사하는 데 10~15초 정도의 시간이 걸림(효용성?)
- 기계장치에 오랫동안 눈을 갖다 대고 초점을 맞춰야 하며 안경을 쓴 상태에서는 수행할 수 없음

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 9 홍채

- 홍채의 패턴을 수학과 통계학 알고리즘으로 구분하여 개개인을 식별하는 방식(스마트폰, 은행)
- 많은 국가에서 자동 통관 시스템에 홍채 인식을 적용
- 망막을 이용한 것보다 정확도가 높고, 50cm 정도 거리에서도 인증 가능
- 홍채 인식 기술이 망막 인식 기술로 대체되는 추세

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017



## 10 서명

- 외국에서는 서명을 사용하는 경우가 훨씬 많은 편이어서 서명을 이용한 인증장치도 있음

- 장비를 이용하여 서명의 진위를 확인하는 방식은 보안 수준이 낮은 편 (쉽게 복제 가능)

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 11 목소리

- 원격지에서 전화로 본인인지 확인할 수도 있고 사용 방법을 따로 익힐 필요도 없어 편리
- 사용되는 장비의 가격이 저렴
- 환경이나 감정에 따라 변할 수 있고 다른 사람이 쉽게 흉내 낼 수도 있기에 보안 수준은 낮은 편 (쉽게 복제 가능)


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

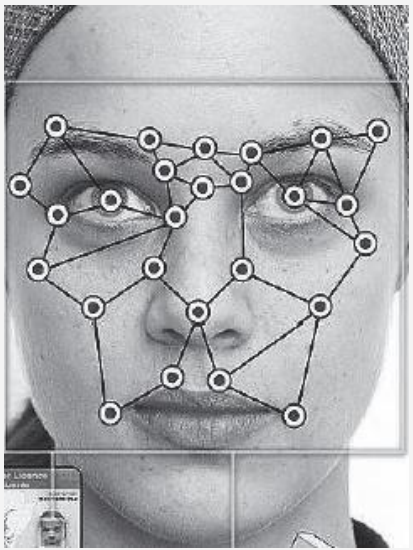
## 12 얼굴

- 얼굴 인증(Facial scan)은
  현재의 기술로는 무표정한 얼굴만 인증 가능

- 2012년 6월 페이스북은 이스라엘의 얼굴 인식
  기술 업체인 페이스닷컴을 1억 달러(약 1300억 원)에
  인수하여 타임라인에 사진을 올리면 사진 속에 있는
  사람의 얼굴을 자동으로 인식하여 태그를 달 수 있게
  함(아이폰)

## 12 얼굴

[얼굴을 통한 인증]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 13 뇌파

- 2012년, 영국 옥스퍼드대학교의 이반 마티노빅 박사는 뇌파(EEG)를 이용하여 마음을 읽을 수 있는 방법에 대한 보고서를 발표

- 2013년 4월 8일 미국 UC버클리의 연구 팀이 뇌파를 인식하는 헤드셋을 이용하여 패스워드를 입력하는 방법 개발(뇌파 - 패스워드)

## 13 뇌파

[뇌파 센서를 이용하여 본인 인증을 하는 모습]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

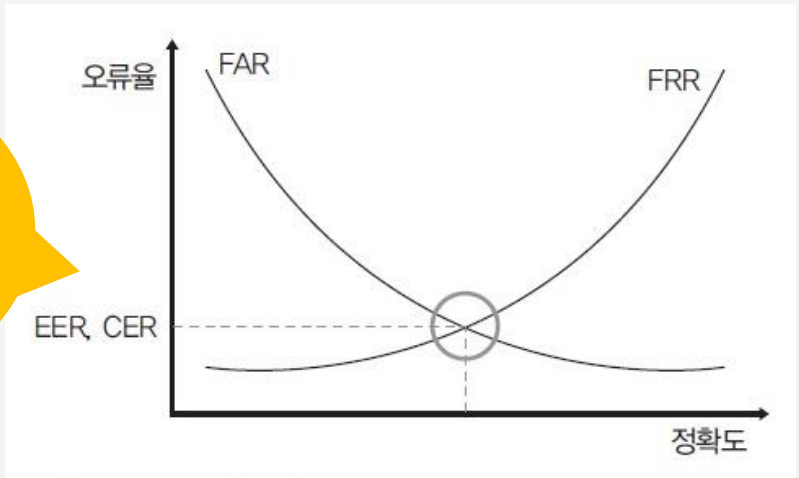
## 14 생체 인증의 측정 기준

- FRR(False rejection rate, Type I Error)
  - 권한이 있는 사람이 인증을 시도했을 때 실패하는 비율
- FAR(False acceptance rate, Type II Error)
  - 권한이 없는 사람이 인증을 시도했을 때 성공하는 비율
  - FRR이 높은 것보다 FAR이 높은 것이 더 심각한 문제가 될 수 있음
- EER(Error equal rate)
  - FRR과 FAR이 그리는 곡선의 교차점

## 14 생체 인증의 측정 기준

[EER과 CER]

좋은 생체 인증 방식은 FAR과 FRR이 만나는 지점인 EER이 낮은 것




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 15 성능 척도

- 다음은 생체인식 시스템의
  성능을 평가하는 지표로 사용됨

- 오인식률(FAR:False acceptance rate)
  : 본인의 것이 아닌 생체인식 정보를 본인의 것으로
  잘못 판단할 확률을 의미함

- 오거부률(FRR:False Rejection Rate)
  : 본인의 생체정보를 본인이 아닌 것으로
  잘못 판단할 확률을 말힘

## 15 성능 척도

- ROC(Receiver Operating Characteristic) 곡선
  : ROC곡선은 오인식률과 오거부률 간의 트레이드 오프를 시각적으로 나타낸 그래프임,
  일반적으로, 본인의 생체정보가 타인의 생체정보로 잘못 인식될 확률이 내려가면 오거부률은 내려가지만, 한편으로 이것은 본인의 생체정보로 판단하는 기준을 느슨하게 한다는 의미를 가지기도 하기 때문에, 오인식률은 올라가게 됨. 반대로, 타인의 생체정보를 본인의 생체정보로 인식하는 확률이 내려가면 오인식률은 내려가지만, 오거부률은 올라감
  (트레이드 오프)

## 15 성능 척도

- 동일 오류율(EER:Equal Error Rate)
  : 오인식률과 오거부률이 같아지는 비율을 말함,
  EER의 수치는 ROC 곡선으로부터 쉽게 얻을 수 있음,
  EER은 다른 ROC 곡선을 가지는 장치의 정확도를
  비교하기 위한 빠른 방법이며, 일반적으로 가장 낮은
  EER을 가지는 장치가 가장 정확함.(비교 - EER)

- FTE(Failure To Enroll rate)
  : 사용자가 시스템에 생체정보를 등록하려는 시도가
  실패하는 확률을 의미하며, 대부분은 생체정보의
  입력이 잘못되어 일어남(등록 실패)

## 15 성능 척도

- FTC(Failure To Capture rate)
  : 자동화시스템에서 올바르게 입력된
  생체정보를 시스템이 감지하지 못 할 확률(인식 실패)

- 주형용량 : 시스템에 저장 가능한 데이터의 수

## 16 실용 사례

- 현재, 이용건수가 많은 것에는 지문, 눈동자 속의 홍채를 들 수 있음, 금융기관이 ATM에 사용하고 있는 것으로 손바닥이나 손가락의 혈관의 모양을 읽는 정맥인증도 이용이 늘고 있으며, 그 외에도 음성, 얼굴, 필적 등에 의한 인증방법이 실용화되어 있음 (스마트폰, 은행)
- 인증할 때에는 전용 인식기를 이용해서 생체정보를 기계에 읽어 들이는 것으로 사전에 등록한 본인의 확인을 하며, 생체인식으로만 하는 것이 아닌 카드나 비밀번호 등과 맞추는 경우가 많음 (복합 인증 - 멀티 팩터)

## 16 실용 사례

- 전산기등을 이용할 때, 또는 전자제어 출입구에
  미리 등록된 본인을 확인하는 목적으로 행해지고 있음

- 개인 컴퓨터에 로그인할 때,
  작은 기기를 이용하여 지문인식을 사용함

- 휴대전화를 사용할 때, 휴대전화의 일부를
  손가락 끝으로 문질러서 인증하는 제품이 있음(인식률)

- 은행의 ATM에서 비밀번호와 같이 손바닥의
  정맥의 형태를 읽어 들여 본인을 확인하는 것도 있음

## 16 실용 사례

- 국가나 기업에서는 개인정보나 극비정보가 포함된 방에 들어가기 위해서 망막인식을 이용하고 있음
- 일본적십자에서는 헌혈자의 본인 확인을 위해 (2014년 05월 14일, 홋카이도부터 순차적으로) 손가락 정맥인식을 채용하고 있음

## 17 참고 요소

- 생체인식을 위해 이용될 수 있는
  인간의 물리적, 화학적 행동적 특성은 다양함,
  특정한 상황에 적용해야 할 생체인식정보의
  선택은 다음과 같은 요소들을 참고로 할 수 있음

## 17 참고 요소

- 보편성
  : 시스템을 이용하는 모든 사람들이 인증하는데
  사용되는 생체정보를 지니고 있어야 함을 의미함

- 영구성
  : 생체정보가 시간에 따라 변하는 정도와 관련이 있음,
  높은 영구성을 가진 생체정보는 시간이 지나도 거의
  변하지 않음(나이가 들면 변화는 것은 안됨)

## 17 참고 요소

- 측정성(정확성)
  : 생체정보가 얼마나 간단히 획득되고 측정되는지와 관련이 있음, 추가로 데이터는 얻어진 후에 가공되거나 추출될 수 있는 형태로 얻어져야 함

- 성능성
  : 사용되는 기술의 정확도, 속도, 견고함과 관련이 있음

## 17 참고 요소

- 수용성
  : 개인들이 자신들의 생체정보의 획득과 수집을 허용하도록 얼마나 사용자들이 생체인식을 거부감 없이 수용하는지와 관련이 있음(거부감)

- 우회성
  : 생체정보가 인공물 따위의 것으로 얼마나 잘 모방될 수 있는지와 관련이 있음(복제)

## 18 표준화 동향

- 생체인식에 관계되는 국제 표준화 규격은 ISO/IEC JTC 1/SC 37가 전문으로 심의하고 있음
- 현시점에서, BioAPI(인터페이스), CBEFF(데이터구조) 등의 규격이 국제표준으로 발행이 완료
- 그 외에, ISO/IEC JTC 1/SC 17(IC카드 기술), ISO/IEC JTC 1/SC 27(보안 기술), ISO/TC 68(금융분야),ITU-T/SG17(통신기술),ICAO(IC여권) 등의 국제 표준화기관도 생체인식에 관련한 규격화 작업이(SC 37에 관계해서) 진행되고 있음

## 19 안정성

- 오인식률을 0에 수렴하게 하려면 오거부률이 높아져 버리기 때문에, 일반적으로 실용화 되어 있는 생체인식은 오인식률이 0이 아닌 상태이며, 생체인식 자체가 보안이 강한 시스템이라고는 말할 수 없음, 그 때문에 은행 ATM등에서는 생체인식과 비밀번호를 병용해서 양쪽의 입력을 요구하는 것으로 높은 보안을 확보하고 있음(복합 인증 - 멀티 팩터)

## 19 안정성

- 음성이나 필적 등은 사용자의 그날 상태에 의존하는 인식방법인 반면, 지문, 정맥, 홍채 등은 그렇지 않다는 점에서 정확도가 높다고 하지만, 현시점에서는 비밀번호 등의 방법을 병용하는 것이 안전하고 확실한 수단이라고 말할 수 있을 것임(멀티 팩터)

## 19 안정성

- 몇 천 원 정도의 비용으로 생체보안을 무력화 시키는 방법도 여러 가지 알려져 있음, 젤라틴으로 만든 인공 손가락으로 많은 지문인식시스템을 통과 가능하다는 것이 알려져 있고, 종이로 만든 홍채로 인공 홍채 시스템 또한 통과 가능할 가능성이 있다는 것까지 지적되고 있음, 정맥인식시스템은 무로 만든 인공손가락을 등록 할 수 있는 장치가 있다는 것이 실험에 의해 확인 되어 있음, 이런 문제에는 장치의 정확도를 올리는 것 등의 대응을 하고 있는 중임 (정확도를 올리는 것은 굉장히 힘듦)

## 19 안전성

- 지문인식의 경우

  : 잔류지문을 젤라틴으로 얻어서 인공손가락을 만들어, 그 인공손가락으로 인식을 통과시키는 것이 성공한 사례가 있어 안정성에 굉장한 의문이 남음, 실제로 손가락에 특수한 테이프를 붙여서 지문을 변조한 사건도 발생하고 있음(인공손가락, 테이프)

## 19 안전성

- 홍채인식의 경우

  : 홍채이미지를 인쇄한 종이로 위조가 가능했다는 연구도 발표되고 있음(홍채이미지)

## 19 안전성

- 정맥인식의 경우

  : 2005년에 인공 손가락을 데이터로 등록해서 인식을 통과했다고 하는 실험만으로는 위험성이 있다고 잘라 말할 수는 없음. 하지만, 내부범이 부정으로 데이터를 등록할 가능성을 부정할 수는 없고, 이 같은 경우로 인공손가락의 데이터를 등록해서 결과적으로 인공손가락으로 인식을 통과해버릴 수 있기 때문에 역시 안전성에 의문이 남음(인공손가락)

## 19 안정성

- 이런 방법들은 일반적으로 정해진 방법과는 다른 부자연스러운 행동을 조건으로 하므로, 인증 절차 때의 모습을 감시하는 것으로 막을 수 있는 경우도 있음(인공손가락 - 부자연스러움)

## 19 안정성

- 또한, 생체인식에는
  다음과 같은 안정상의 문제점이 지적되고 있음
  - 상처나 병에 의해, 인식을 하지 못하는 위험이 있음
  - 대상자가 성장기에 있는 경우,
    크기 자체가 바뀌어 오거부률이 올라가 버림
  - 생체정보는 평생 바꿀 수가 없기 때문에,
    한번 복제하는 것으로 보안에 치명적인 약점이 되어
    버리기 때문에, 평생 안정성을 회복하는 것이 불가능
    (복제 가능)

## 19 안정성

- 또한, 생체인식에는
  다음과 같은 안정상의 문제점이 지적되고 있음
  - 생체정보는 평생 바꿀 수가 없기 때문에,
    탈퇴 등을 할 때 무효화가 불가능함
  - 모든 시스템에서 같은 정보를 쓸 수밖에 없음
  - 그렇게 때문에 어떤 시스템의 시스템관리자는
    등록된 정보를 사용하여 시스템의 인식을 통과하는
    것이 가능해져 버릴 가능성이 있음(오용, 악용)

## 19 안정성

- 또한, 생체인식에는
  다음과 같은 안정상의 문제점이 지적되고 있음
  - 도둑이 보안된 물건들을 훔치려 할 때,
    도둑들이 접근권을 얻기 위해, 물건의 소유자를
    추적하여 습격 할 수 있음, 만약 물건이 생체인식
    장치로 보안이 되어 있다면 소유자들에 대한 피해는
    되돌릴 수 없을 수도 있고, 잠재적으로 보안된 물건
    보다 더 많은 비용이 발생할 수 있음,
    예를 들어 2005년, 말레이시아의 메르세데스
    벤츠 S클래스의 차주는 차를 훔치려던 도둑들에게
    손가락이 잘렸음 (이중 삼중 피해 발생)

## 19 안정성

- 또한, 생체인식에는
  다음과 같은 안정상의 문제점이 지적되고 있음
  - 하지만, 이런 지적들은 반드시 모든 생체인식 기술에 해당하는 것이 아님, 방식에 따라서 근본적으로 문제가 되지 않는 것들이나 가볍게 해결책이 개발되는 것들도 있음
    (아직까지는 멀티 팩터를 해야함)