정보보호론

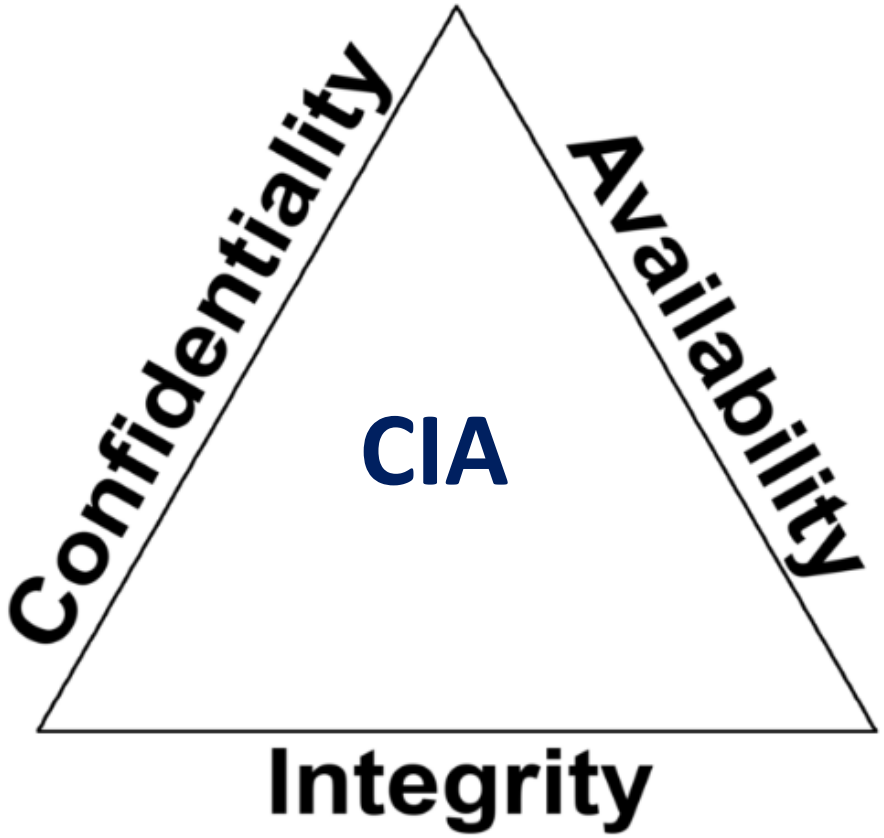
정보보호의 이해

한림대학교 소프트웨어융합대학 조효진

Contents

- 정보보호의 목표
- 고전 정보보호기술
- 현재 그리고 미래의 정보보호 기술
- 정보보호 기술의 필요성 및 이슈

정보보호의 목표



+

Authentication and Accountability

정보보호의 목표: 정보보호 용어

- 기밀성 (Confidentiality): 허락 되지 않은 사용자가 정보의 내용을 알 수 없도록 함
- 무결성 (Integrity): 허락 되지 않은 사용자가 정보를 함부로 수정할 수 없도록 함
- 가용성 (Availability): 허락된 사용자가 정보에 접근하려 하고자 할 때, 이것이 방해받지 않도록 함
- 인증 (Authentication): 허락 되지 않은 사용자인지 허락된 사용자인지 구분할 수 있도록 함
- 책임성 (Accountability): 정보보호사고 발생시, 사고의 원인을 파악할 수 있어야 함

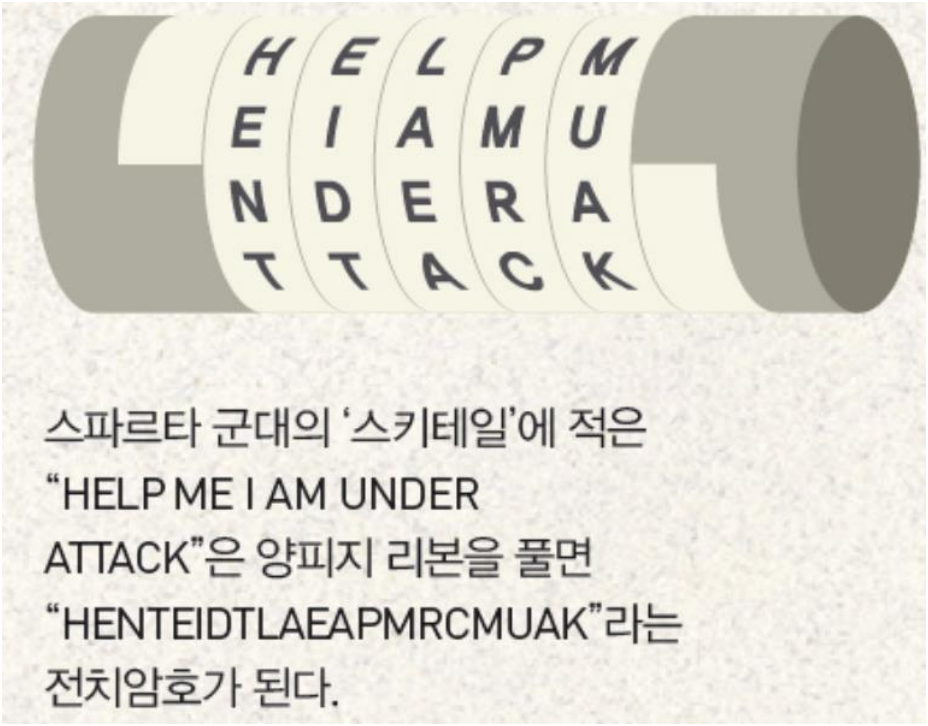
고전 정보보호 기술

기밀성: 스파르타 군대의 암호

(Source: http://m.blog.daum.net/picodrim/9873968)

기밀성: 스파르타 군대의 암호

❐ 스키테일 암호



스파르타 군대의 '스키테일'에 적은 "HELP ME I AM UNDER ATTACK"은 양피지 리본을 풀면 "HENTEIDTLAEAPMRCMUAK"라는 전치암호가 된다.

스키테일은 안전할까요?

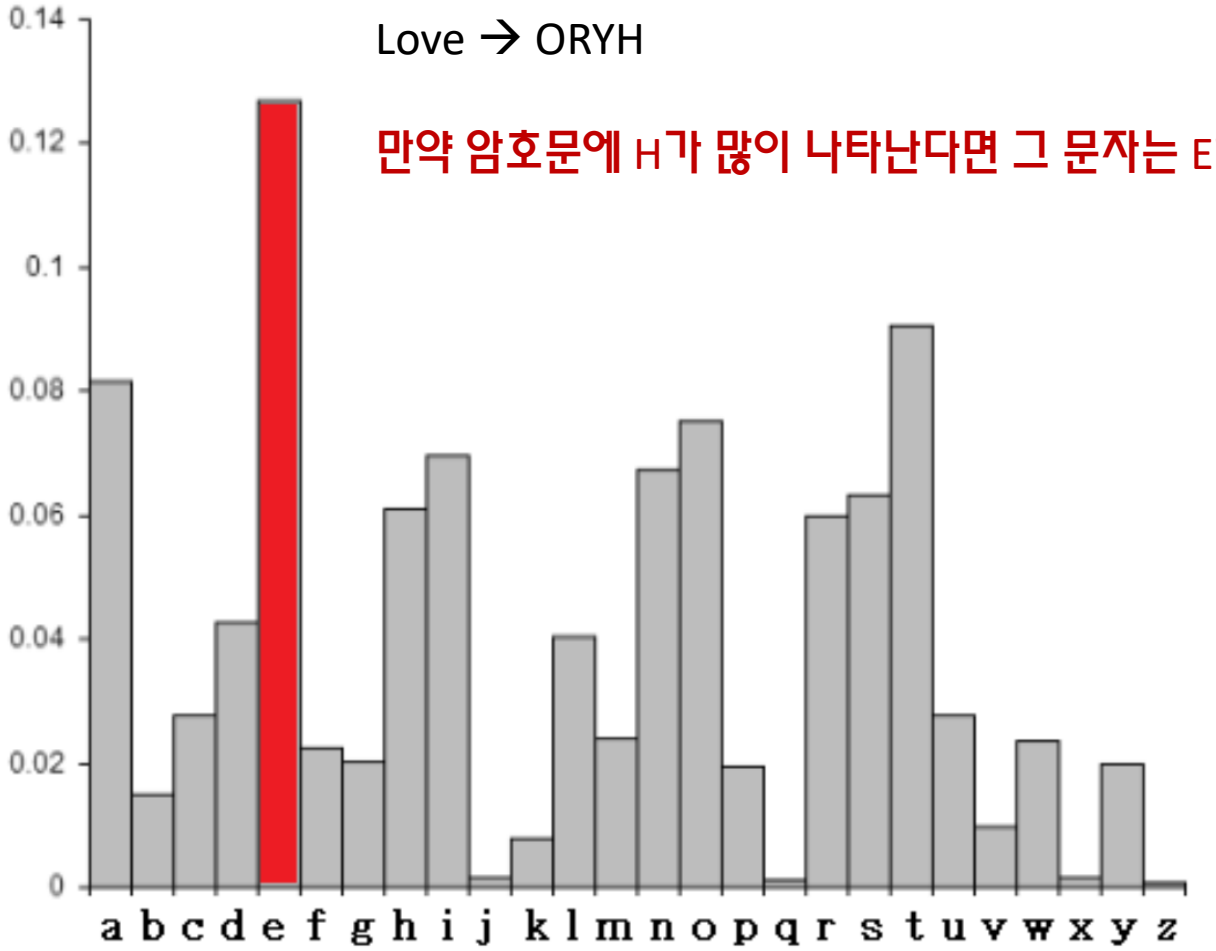
기밀성: 시저 암호

[시저 암호시스템]

Love → ORYH

시저암호는 안전할까요?

기밀성: 시저 암호

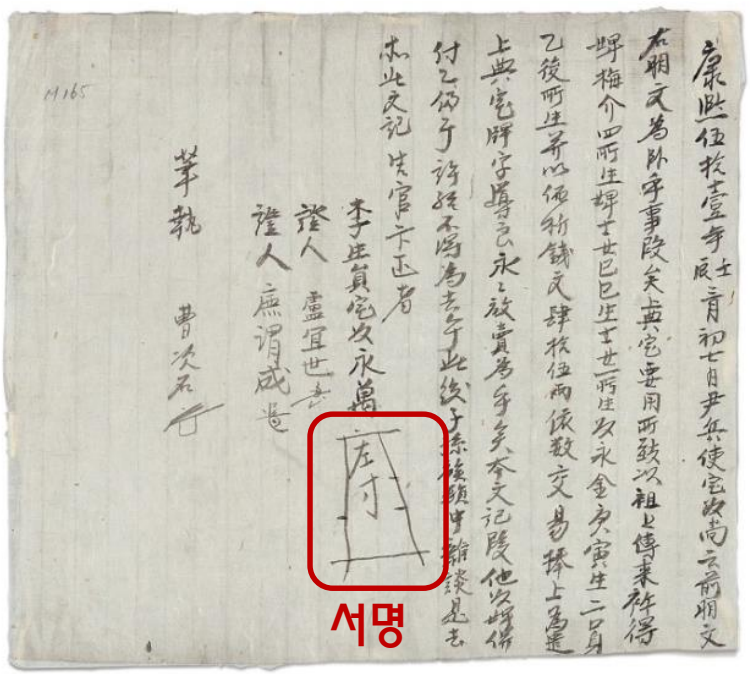


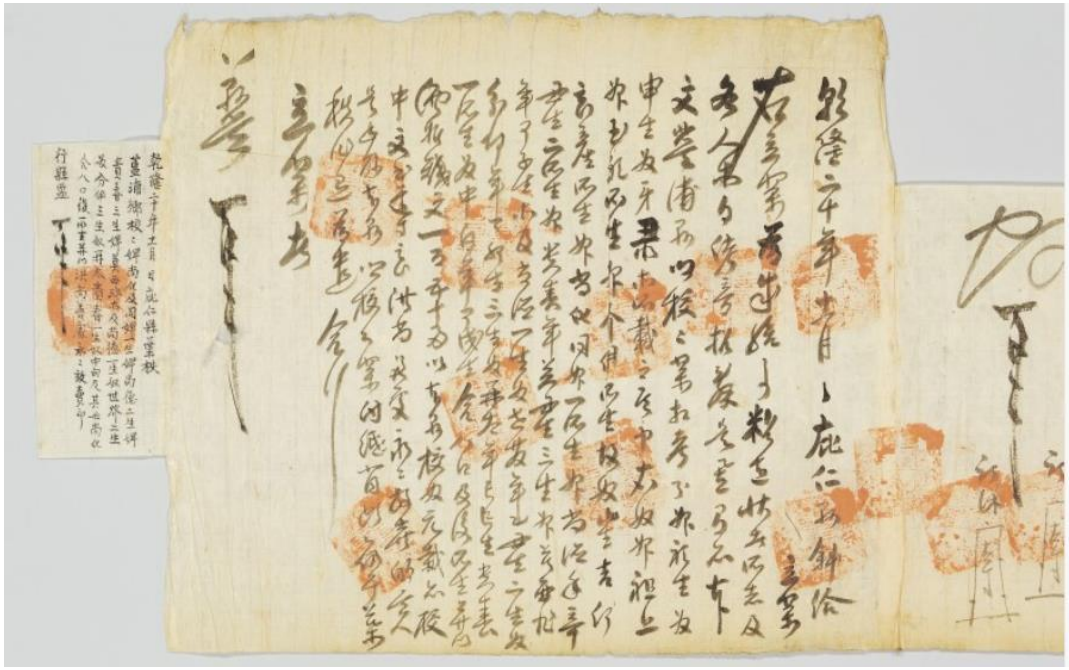
Love → ORYH

만약 암호문에 H가 많이 나타난다면 그 문자는 E일 확률이 높음!

무결성: 필체 + 서명 (인증) + 도장

- 조선시대의 노비매매 계약서





(Source: https://m.blog.naver.com/PostView.nhn?blogId=modusign&logNo=220782745717&proxyReferer=https%3A%2F%2Fwww.google.com%2F)

무결성: 필체 + 서명 (인증) + 도장

영화 <적벽대전>

무결성: 필체 + 서명 (인증) + 도장

항우

범증

전자문서 (한글, MS word 등)를 위한 무결성 및 인증 제공?

가용성: 전령의 보안 메시지 전달

전령이 적군에 잡히면?

(Source: http://magazine.hankyung.com/apps/news?popup=0&nid=01&c1=1012&nkey=2016061301072000191&mode=sub_view)

인증: 해님 달님

❒ 해님 달님 인증시스템

- 엄마가 맞는지 손을 내밀어 인증

(Source: https://ysbook.tistory.com/m/169)

(개체) 인증이 적절했다면?

책임성: 해님 달님

- 호랑이에게 속아 문을 열어준 동생!

(http://blog.naver.com/PostView.nhn?blogId=ahdtlf2010&logNo=220659274191&parentCategoryNo=8&categoryNo=&viewDate=&isShowPopularPosts=true&from=search)

책임은 누구에게? 엄마? 오빠? 동생?

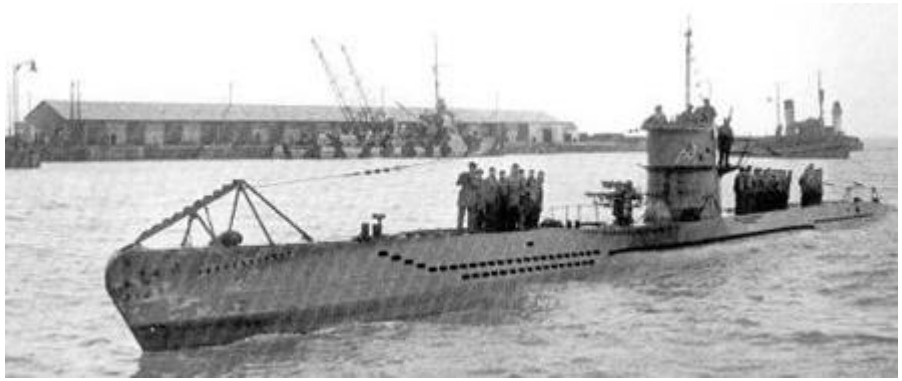
근대 정보보호 기술
(암호화 관점에서)

영화 이미테이션게임의 정보보호기술

영화 이미테이션게임의 정보보호기술

❒ 2차대전에서 독일군에 의해 사용된 잠수함 U-boat

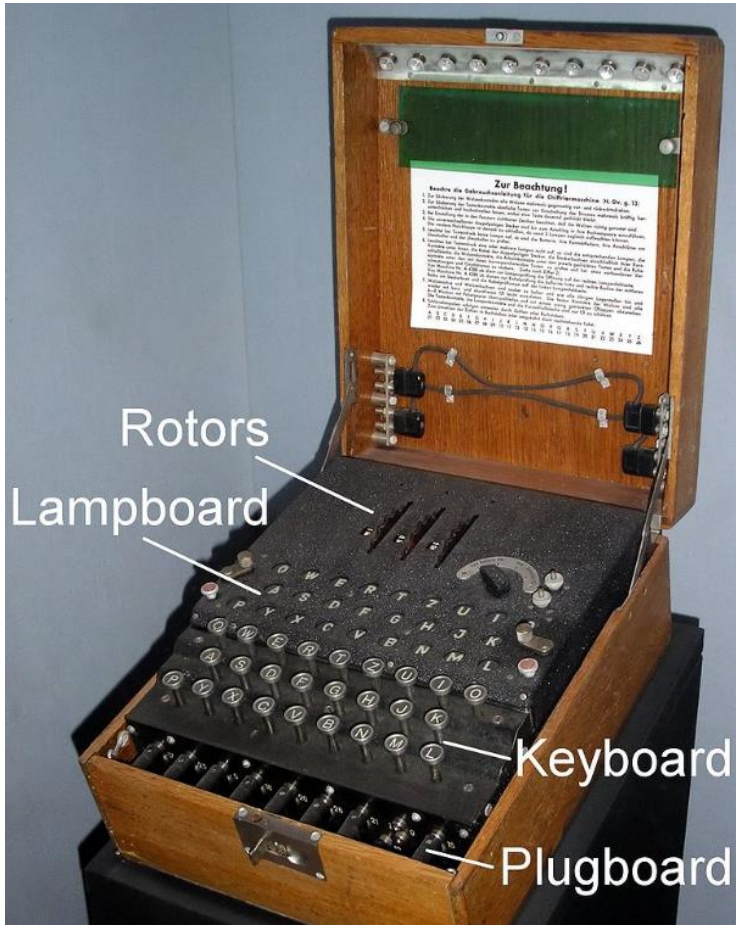
(Source: https://edition.cnn.com/2014/10/21/us/north-carolina-u-boat-wreck/)



(Source: https://blue-paper.tistory.com/1144)

영화 이미테이션게임의 정보보호기술

- 독일군의 암호시스템 "에니그마"



(Source: https://ko.wikipedia.org/wiki/%EC%97%90%EB%8B%88%EA%B7%B8%EB%A7%88%EC%9D%98_%ED%95%B4%EB%8F%85)

영화 이미테이션게임의 정보보호기술

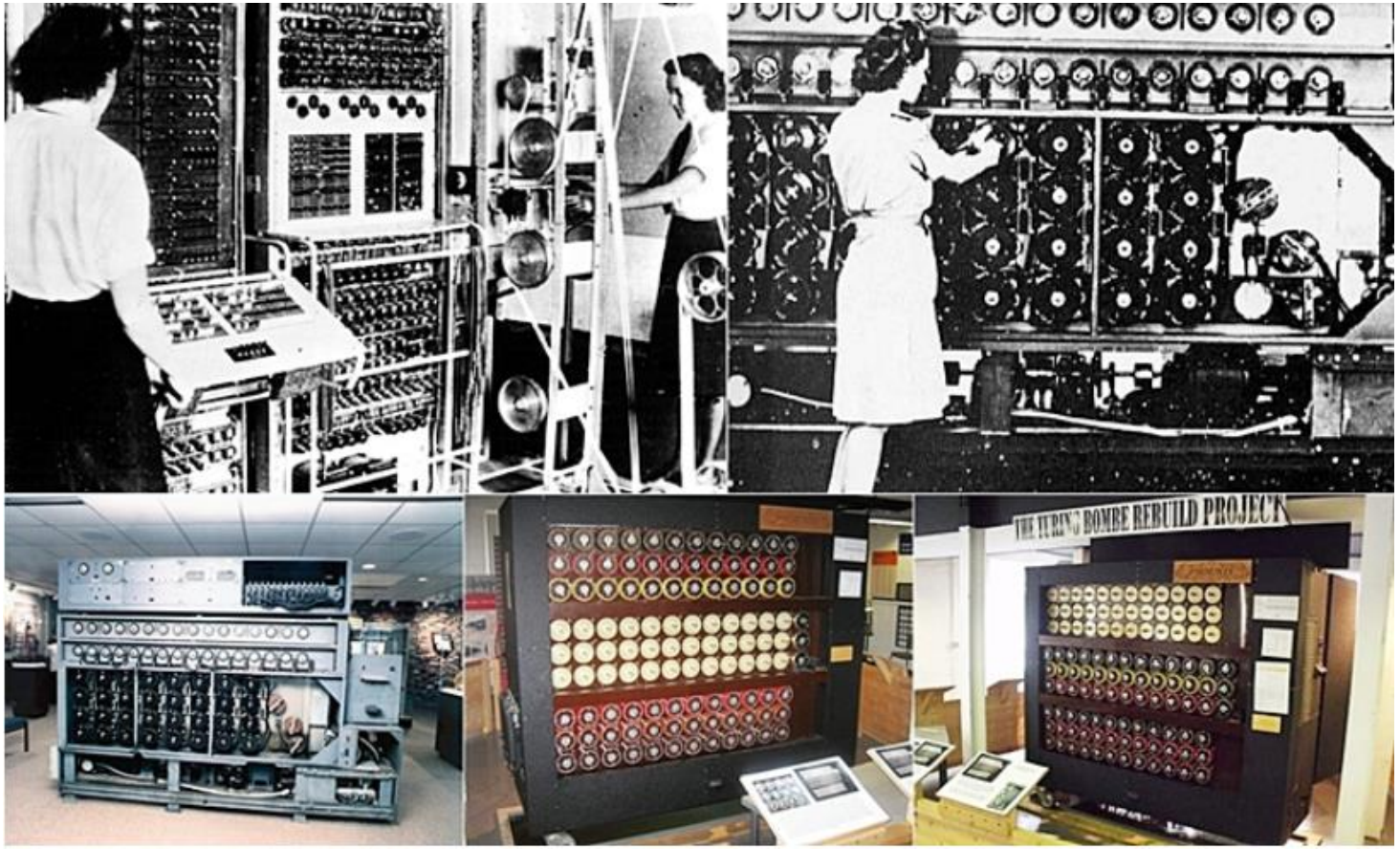
❒ 앨런 매티슨 튜링(영어: Alan Mathison Turing, OBE, FRS, 1912년 6월 23일 ~ 1954년 6월 7일)은 영국의 수학자, 암호학자, 논리학자이자 컴퓨터 과학의 선구적 인물이다. 알고리즘과 계산 개념을 튜링 기계라는 추상 모델을 통해 형식화함으로써 컴퓨터 과학의 발전에 지대한 공헌을 했다.

❒ ACM에서 컴퓨터 과학에 중요한 업적을 남긴 사람들에게 매년 시상하는 **튜링상**은 그의 이름을 따 제정한 것이다. 이론 컴퓨터 과학과 인공지능 분야에 지대한 공헌을 했기 때문에 **"컴퓨터 과학의 아버지"**라고 불린다.

영화 이미테이션게임의 정보보호기술

❒ 튜링 머신

영화 이미테이션게임의 정보보호기술



(Source: https://m.blog.naver.com/PostView.nhn?blogId=sw_maestro&logNo=220902590813&proxyReferer=https%3A%2F%2Fwww.google.com%2F)

역사학자들은 에니그마 해독이 전쟁을 2년 단축시켰고, 1400만명을 구했다고 함

현재 그리고 미래의 정보보호 기술

영화 스노든의 정보보호기술

영화 스노든의 정보보호기술

- 에드워드 조지프 스노든(Edward Joseph Snowden)은 중앙정보국(CIA)과 미국 국가안보국(NSA)에서 일했던 미국의 컴퓨터 기술자다.

- 2013년 스노든은 가디언지를 통해 미국내 통화감찰 기록과 PRISM 감시 프로그램 등 **NSA의 다양한 기밀문서를 공개했다.**

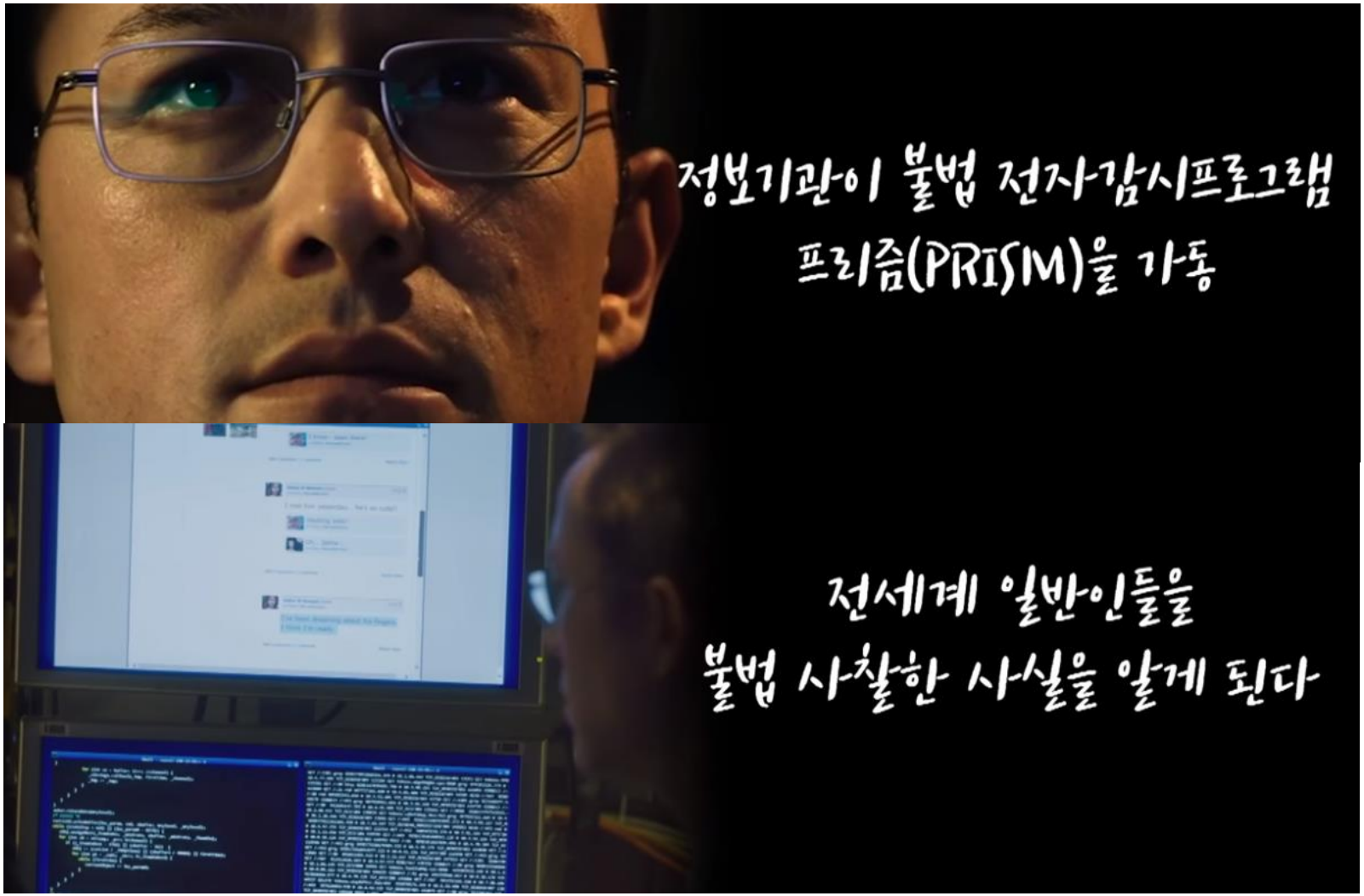
영화 스노든의 정보보호기술

(Source: https://www.youtube.com/watch?v=RXVMp0oMHIo)

영화 스노든의 정보보호기술

(Source: https://www.youtube.com/watch?v=RXVMp0oMHIo)

영화 스노든의 정보보호기술



(Source: https://www.youtube.com/watch?v=RXVMp0oMHIo)

영화 스노든의 정보보호기술

- https://www.youtube.com/watch?v=2bylpTuMrdA

영화 스노든의 정보보호기술

- 스노든은 어떻게 정보를 가져올 수 있었을까?

https://www.youtube.com/watch?v=2byIpTuMrdA

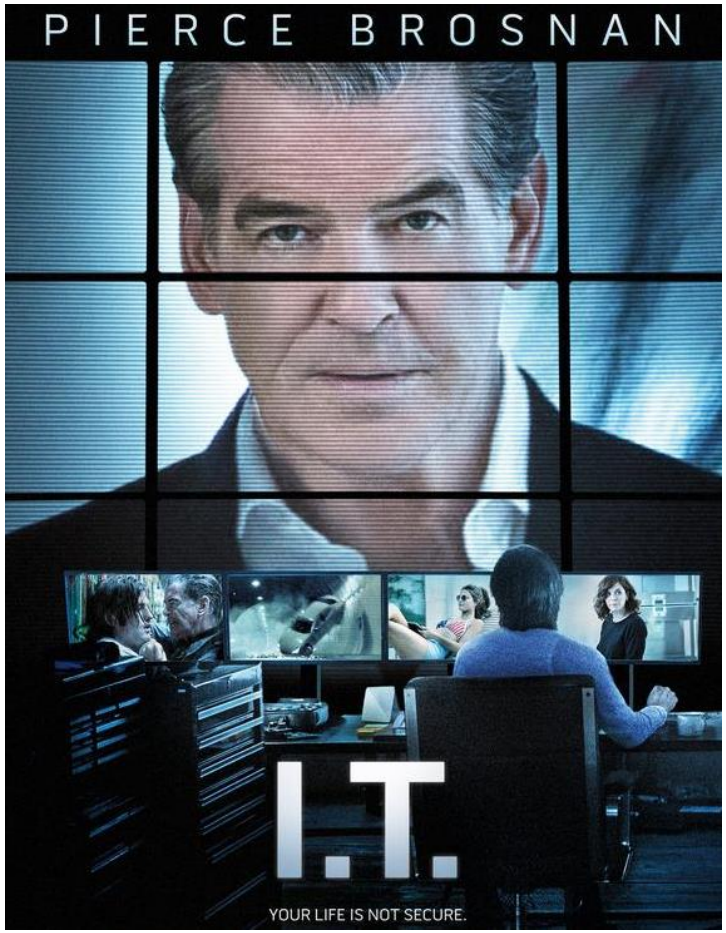
NSA에는 프리즘 프로젝트 보호를 위한 보안 SW 가 존재 했음 (기밀성, 무결성, 가용성, 인증, 책임성 제공)

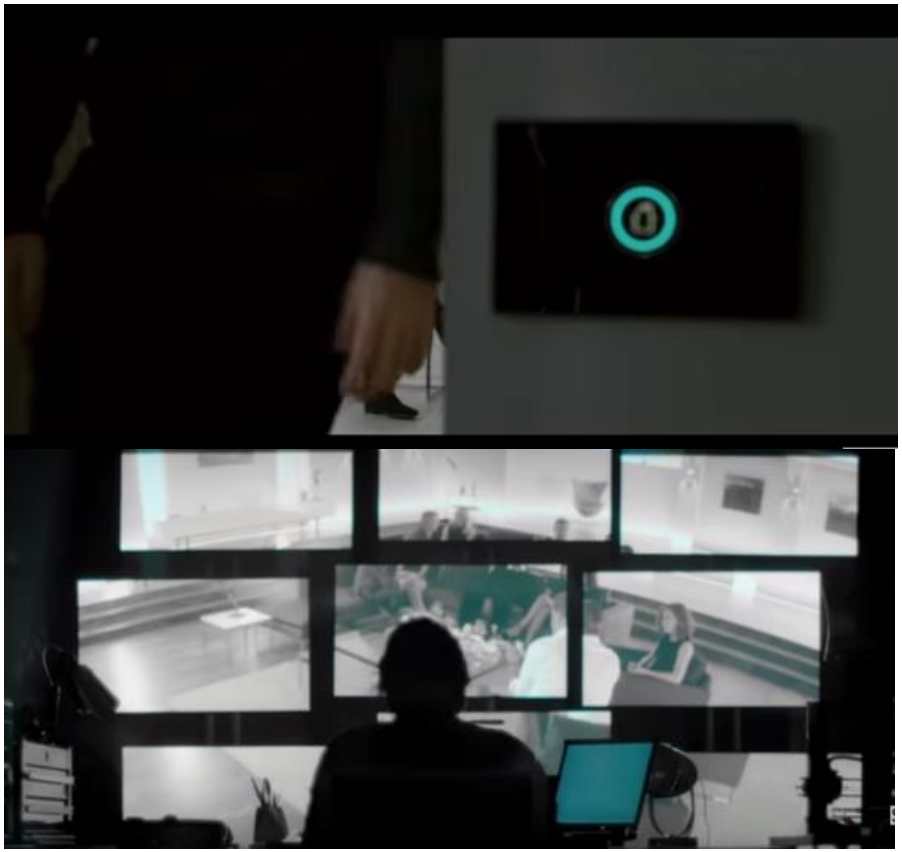
또한, 물리적인 보안 시스템도 존재 했음

하지만, Humane Error 및 Mistake를 적절히 관리하지 못한 보안 정책 및 모니터링 시스템에 문제가 있을 수 있음

영화 I.T의 정보보호기술

❒ 사생활 유출





Is it possible?

영화 I.T의 정보보호기술

반려동물용 **IP 카메라 해킹**해 주인 사생활 털었다
보안뉴스 - 2018. 11. 1.
[보안뉴스 원병철 기자] 집에서 키우는 반려동물을 위해 주인이 설치한 **IP카메라**를 **해킹**해 반대로 주인의 사생활을 엿본 피의자들이 검거됐다.

These smart TVs are open to hacks

USA TODAY
YouTube - 2018. 2. 7.

Here's How The CIA Is Hacking Your Smart TV

NowYouKnow
YouTube - 2017. 3. 8.

90% of Smart TVs Vulnerable to Hack

TWiT Netcast Network
YouTube - 2017. 4. 5.

왜 일어날까? 인증? 무결성? 기밀성? 책임은 누구?

영화 분노의 질주의 정보보호기술

- https://www.youtube.com/watch?v=bfoFmZhMXmA

Is it possible?

영화 분노의 질주의 정보보호기술

왜 일어날까? 인증? 무결성? 기밀성? 책임은 누구?

영화 스파이더맨의 정보보호기술

- https://www.youtube.com/watch?v=_EvOJfSHI9Y

영화 스파이더맨의 정보보호기술

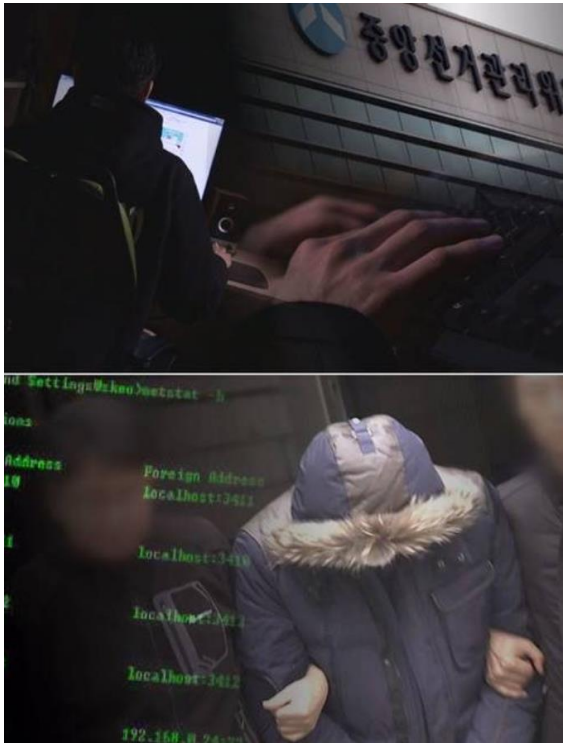
- 왜 일어날까? 인증? 무결성? 기밀성? 책임은 누구?

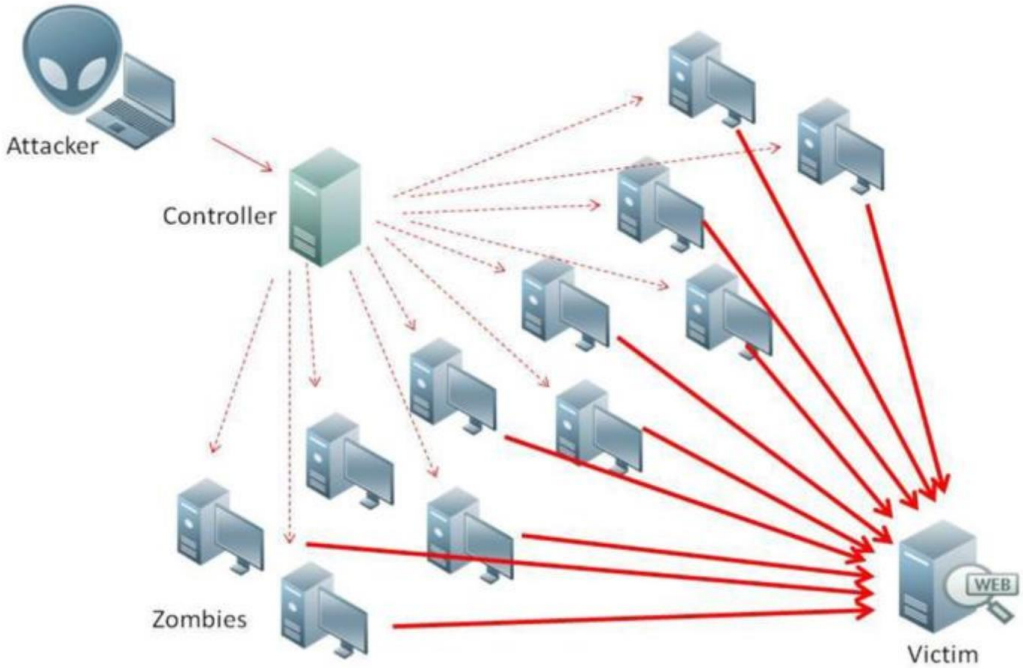
?

정보보호 기술의 필요성 및 이슈

정보보호기술의 필요성

❐ 투표소가 어디?





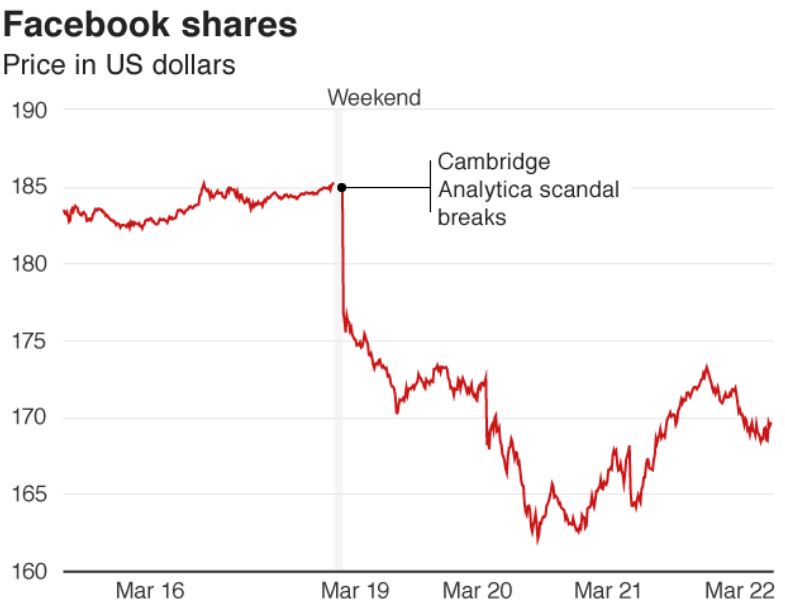
'그것이 알고싶다', 2011년 **선관위 디도스 공격**사건 파헤친다
2017.02.11 | 서울신문 | 다음뉴스

선관위, 선거날 또 **디도스 공격**을 받다
허핑턴포스트 - 2016. 4. 13.
중앙**선거관리위원회** 홈페이지가 20대 총선 선거당일인 13일 오후 **디도스**(**DDoS**.분산서비스거부) **공격**을 받은 것으로 확인됐다. **선관위**는 이날 ...

[단독] **선관위** 홈페이지 '**디도스**' **공격** 당해
조선일보 - 2016. 4. 13.

정보보호기술의 필요성

facebook.



하버스대 졸업식 축사

정보보호기술의 필요성

"인도 원전 사이버 공격에 북 **해킹**조직 흔적 남아"
자유아시아방송 - 2019. 11. 1.
앵커: 자국의 원자력 **발전소**에 대한 사이버 공격을 부인하던 인도(인디아) 원자력공사(NPCIL)가 원전 시스템에서 악성 코드가 발견됐다고 인정한 ...

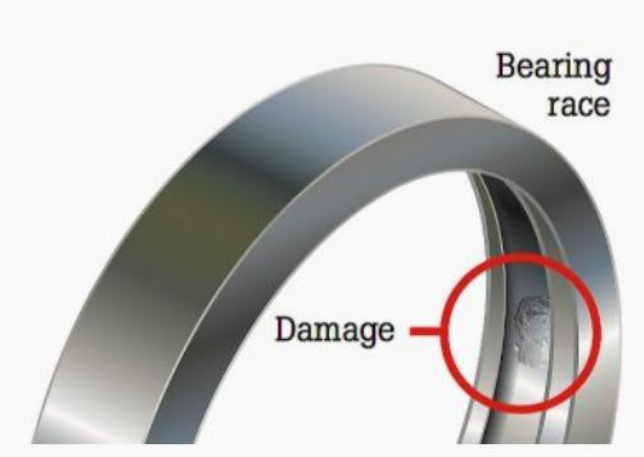
미국서 풍력·태양광 **발전소 해킹**으로 가동 중단
ZD넷 코리아 - 2019. 11. 1.
미국 재생에너지 **발전소**가 사이버공격을 받아 전력 생산이 중단됐던 것으로 밝혀졌다. 에너지 전문 매체 E&E뉴스는 미국 유타 주에 위치한 태양광· ...

[긴급] 인도 핵**발전소** 공격 악성코드, 라자루스 공격코드와 ...
보안뉴스 - 2019. 10. 31.
[보안뉴스 원병철 기자] 인도의 쿠단 쿨람 핵**발전소**(KKNPP)가 **해킹** 공격으로 인해 가동이 중단된 가운데, 공격에 사용된 악성코드가 지난 2009년 ...

인도 원자력 **발전소** 사이버 공격 공식 인정...'北 소행' 의심
전자신문 - 2019. 10. 30.
인도 원자력 **발전소 해킹**의혹이 결국 사실로 밝혀졌다. ... 를 통해 쿠단쿨람 원자력**발전소**(KKNPP) 행정망에서 악성코드가 발견됐다고 인정했다.

정보보호기술의 필요성

- Stuxnet periodically modifies the frequency of a target motor to 1,410 Hz and then to 2 Hz and then to 1,064 Hz; if there is no attack, the motor spins between 807 Hz and 1,210 Hz
  - Motor speed: High → Low → High → Low



Possible unexpected damage by continuous radical changes of the motor speed

정보보호의 이슈 (Privacy vs. Security)

Apple and Facebook pressured to reveal terror suspects' data

KAKAO TALK

Telegram

https://www.jumble.io/blog/2016/02/26/apple-vs-fbi-battle-encryption-privacy-security/

정보보호의 이슈 (Safety vs. Security)

- 자동차 도둑이 어떻게 스마트 키를 해킹 했을까?

정보보호 이슈 (보안 vs. 비용)

사건	유출건수	민사소송	행정소송
'08 옥션	1,800만 건	옥션 승(2013다43994)	-
'11 싸이월드	3,500만 건	싸이월드 승(2015다24904)	-
'12 KT 1차	870만 건	KT 승(2015나61155)	-
'14 KT 2차	1,170만 건	KT 승(2014가합49529)	KT 승(2014구합15108)
'16 인터파크	2,500만 건	진행 중	진행 중(방통위 2016.12. 5. 처분)
'17 여기어때	97만 건+숙박정보	진행 중	진행 중(방통위 2017. 9. 8. 처분)
'17 빗썸	3만 건 +비트코인	진행 중	진행 중(방통위 2017.12.12. 처분)

https://www.boannews.com/media/view.asp?idx=68756

국민 4천3백만 의료**정보 유출**·판매한 한국IMS헬스 **사건** 무죄 ...
참여연대 - 2020. 2. 20.
국민 4천3백만 의료정보 **유출**·판매한 한국IMS헬스 **사건** ... 이에 이번 **판결의** 의미와 한계, 의료정보 상업화와 **개인정보**보호법 개악이 초래할 문제 ...

빗썸 고객**정보 유출** 재판, 2심 간다
논객닷컴 - 2020. 2. 20.
[논객닷컴=이상우] 암호화폐 중개업체 빗썸**의** 고객 **개인정보 유출 사건**에 대한 형사 ... 1심 재판부는 피고인 측 혐의를 인정해 유죄 **판결**을 내렸다.

빗썸 고객 **개인정보 유출** 재판, 2심 간다
TokenPost - 2020. 2. 20.

法 "롯데카드, '**정보유출**' 고객 2500여명에 7만원씩 배상"
파이낸셜뉴스 - 2020. 2. 3.
카드사 **개인정보** 대량**유출 사건**은 지난 2014년 KB국민카드·농협은
와 함께 원고들에게 10만원씩 배상하라"고 원고 일부 승소 **판결**했다
대상에 포함된다고 볼 수 없다"며 "롯데카드 고객들이 정보 ...

페이스북 5조9000억원 벌금 낸다...전체 매출의 9%
조선일보 (풍자) (보도자료) - 2019. 7. 24.
페이스북이 개인정보 유출 등 사용자 프라이버시 침해를 이유로 미국 연방거래위원회(FTC)가 부과한 50**억달러**(약 5조9000억원)의 벌금을 내기로 ...

6兆 벌금 맞은 페북, 그래도 끄떡없다
한국경제 - 2019. 7. 24.

Assignment #1

- 정보보호 5가지 목표 (기밀성, 무결성, 가용성, 인증, 책임성)와 관련된 정보보호 사고 소개
  - 정보보호 (해킹) 사고 소개
  - 정보보호 (해킹) 사고의 원인 소개
  - 조사된 정보보호 (해킹) 사고 재발생을 막기위해 필요한 보안기술

- 2페이지 이내 (A4, 10 pt)
  - 3월 26일 오후 5시까지
  - 늦은 제출 시, 감점
  - 과제 copy 시, 관련된 과제들 모두 0점 처리
  - 제출양식: hwp or pdf

Thank you