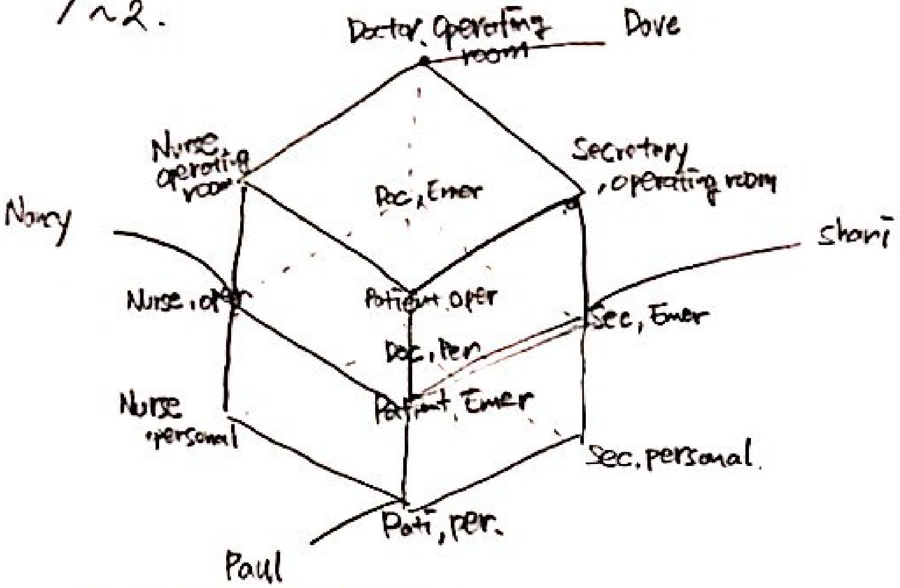
1~2.



1. 그림그리기
2. File, receipt, prescriton, List 그리기

3. BLP에서 각각 어떻게 되는지

· BLP Property
- SS-property : No-Read Up (Subject는 낮은등급의 object만 관찰할수 있다)
- *-property : No-write Down (subject는 낮은등급의 object에 쓸수 없다)

· Dave writes on the List
· Paul writes the prescription

- Nancy reads the File
- Shari reads the receipt

4. BIBA Model에서 각각 어떻게 되는지

· BIBA Property
- SS-property : No-Read Down(
- *-property : No-write up

5. a) what is a capability? Subject S_j와 object O_j의 교점으로 만나는 Matrix의 권한을(접근) 가능한 것을 의미 (≒permission)

· 분산 환경에서 접근제어를 구현할수 있는 방법 중에 하나로서.

$$\begin{array}{cc} & \text{object } O_j \langle \text{방화벽, 라우터} \rangle \\ \text{Subject } S_i \langle \text{안드로이드, Kerberos} \rangle & \begin{bmatrix} & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{bmatrix} \end{array}$$

b) advantage of access control List over capacity?

- ACM에서 열(columns)을 중심으로 접근권한을 Listing함
- 자원별로 주체의 권한을 각각 설정하여 저장함. 자원별로 주체의 접근권한을 설정 가능
- 윈도우 NTFS나 F/W, Router 등에서 많이 사용,

c) advantage of capability over access control list?

- ACM에서 행(Rows)을 중심으로 접근권한을 Listing함
- 주체가 각 자원에 대해 어떠한 접근권한을 가질수 있는지 설정가능
- Kerberos, Android 등이 대표적.

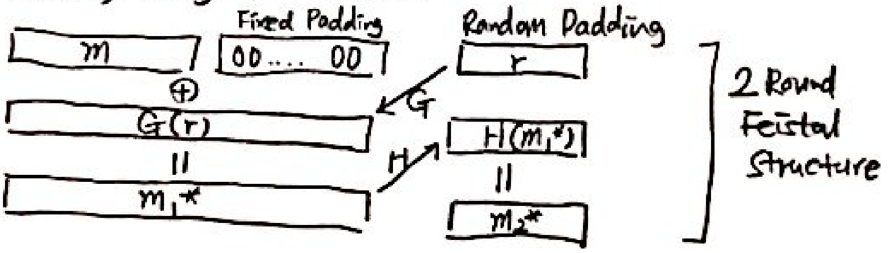
6. 전자투표. $m = \begin{cases} 0 \\ 1 \end{cases}$, $RSA_{(N,e)}(0) / RSA_{(N,e)}(1)$, 서버는 전송받은후 복호화하여 counting

이때 가능한 공격자의 공격방법은, NM(Non-Mellability), IND(Indistingushability) 가 존재 할수 있다.

IND 라는 Security Goal은 암호문을 보고 공격자가 평문 m을 어떤것이 였는지 구별 불가능해야 한다는 속성이지만 IND-CCA 공격을 통해 (임의의 난수 값을 추가하여 연산) 얻어진 C 값으로 평문을 유추할 수 있게된다.

또, NM 이라는 Security Goal은 공격자가 C에 대한 변조를 불가능하게 하여야 한다는 속성이지만 C 값에 임의의 값을 추가로 연산함으로서 전자투표의 무결성을 해칠수가 있게 된다. (조작)
예를 들어 0을 곱하게 하여 변조

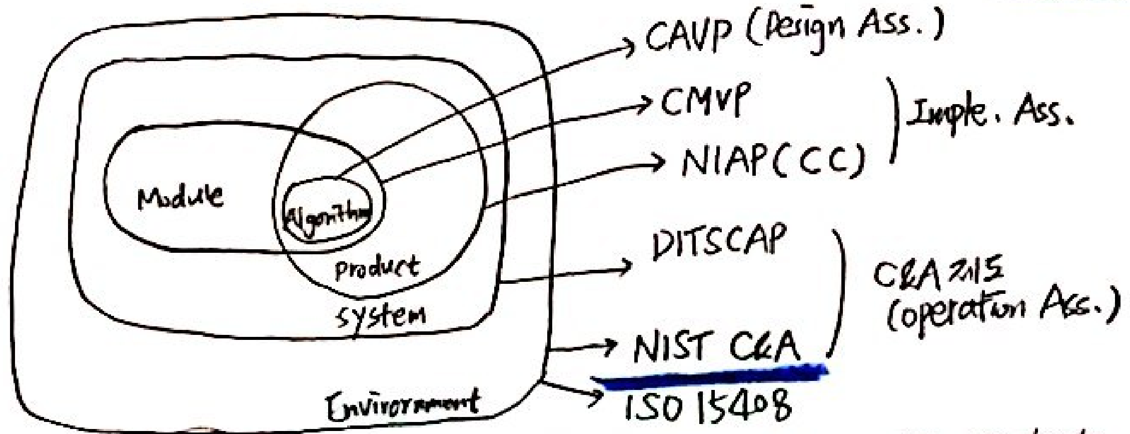
7. 위 공격에 대한 대응방안으로서 RSA-OAEP에 기반한 메세지 패딩을 하면 보다 안전한 Security Design이 가능하다.



$C = f(OAEP(m, r)) = (m_1^* \| m_2^*)^e \bmod n$ 일때,

Fixed Padding은 NM을 보장 할수 ~~(보충)~~ 있고, Random Padding은 IND 속성을 보장할 수 있다.

8.



한국: 사용영역이 민간인가, 공공인가로 구분하여 평가. , ~~또한 CC 인증간~~

미국: 제품과 자료(Data)의 가치로 구분하여 평가.

또한 CC 인증에서 차이를 갖음. 국내용 CC 인증제도는 보안기능과 취약성 시험을 제외한 평가항목 중 일부만 포함축소, 국제용 CC는 CCRA 수준으로 제품평가하여 EAL 1~4 단계까지 CCRA 회원국간 상호인정하고 있다.

9. Patient ID, Issue-date, hmac(K, (patient-id, issue-date))

a) A가 D까지에게 파일이 이전된 이후에도 Issue-date에 의해 90일간 접근권한이 유지되므로 D는 사용가능하다

~~Nu~~ Nurse-Generator-id → hmac(K, (nurse_G-id))

b) Nurse ID, Patient ID, Issue-date, hmac(K, (patient-id, issue-date, ~~nurse-id~~))로 설정후 if (~~Nurse-id == Nurse_Generator-id~~ hmac(Nurse-id) == hmac(G-id)) { 90일 사용가능 } else 10일 사용가능

1,2 번은 저번 중간고사랑 똑같은거 그리는 Lattice 문제 나왔고, 3, 4번은 그걸 보고 푸는 문제. Lattice 모양은 저번처럼 정육면체 두 개 쌓은 모양이야.

Dave : (Doctor, Operating room)
Nancy : (Nurse, Emergency)
Shari : (Secretary, Emergency)
Paul : (Patient, Personal)

Place

→ SS → * 상하관계

NRU NWD

3. In the Bell-Lapadula model, say if the following actions are allowed, explaining each time why that is? → NRU ., NWD

a) Dave writes on the List o
b) Nancy reads the File
c) Paul writes the Prescription
d) Shari reads the receipt

* SS
NRD NWU

각각 어 그런지?

4. In the BIBA model, say if the following actions are allowed, explaining each time why that is?

a) Dave writes on the List
b) Nancy reads the File
c) Paul writes the Prescription
d) Shari reads the receipt

① Directory-based Access Control , ② 행(ACM)
③ key . 디렉토, 도 관련대로. 사용자 정보저장?

ACM → 권한

5. a) In access control system what is a capability? b)Explain an advantage of ~~access control list over capability~~? c) Explain an advantage capability of over access control list ?

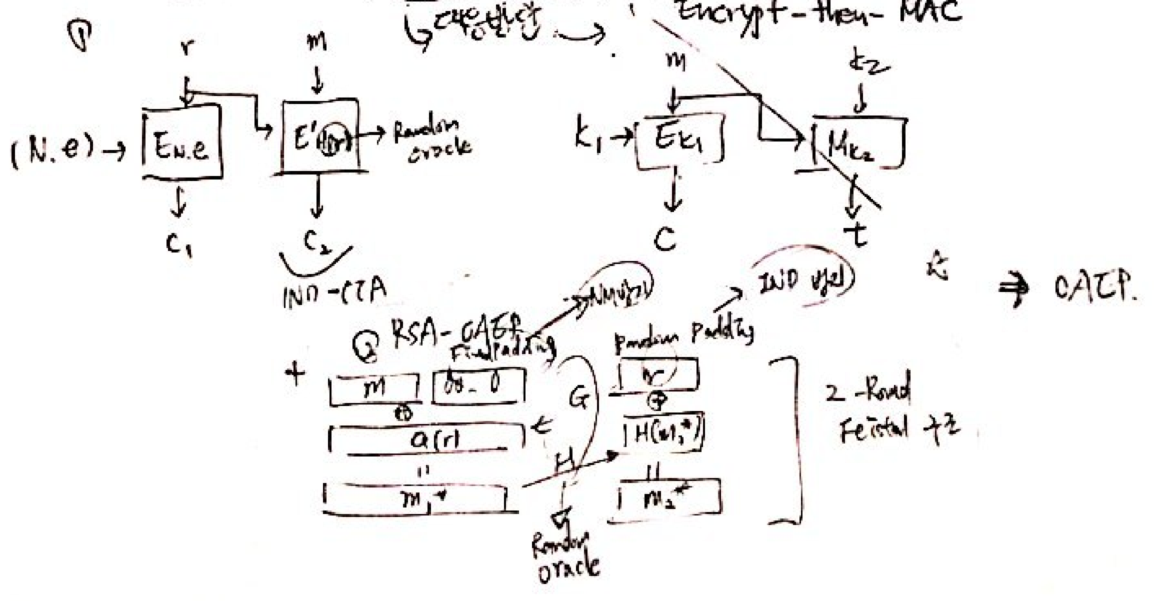
열 ← 객체에 기반

행 가로 주체의 능력

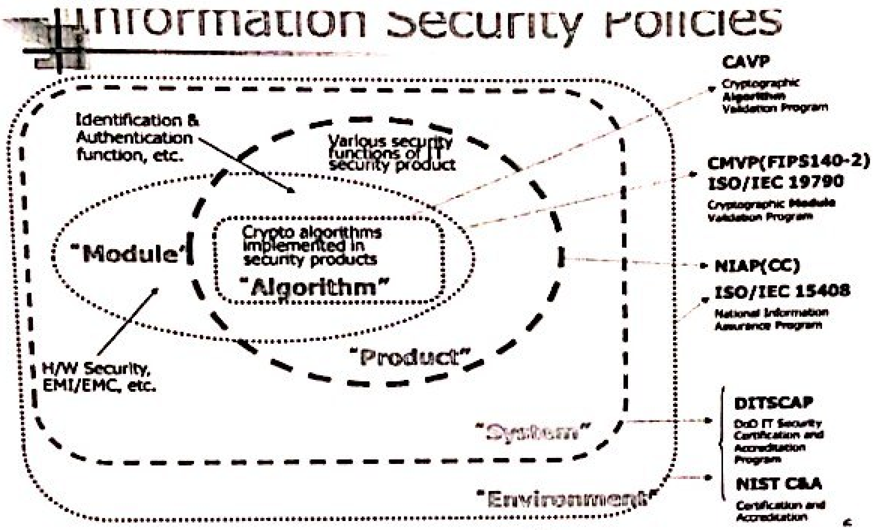
m

6. 전자투표를 하는데 투표자가 0, 1 을 선택하고 이것을 RSA 공개키를 사용해서 암호화해서 서버에 전송한다. $RSA_{(N,e)}(0)$ / $RSA_{(N,e)}(1)$ $m = \{0, 1\}$
서버는 이것을 전송받으면 복호화해서 count한다. 이때, 공격자가 중간에 가로채서 훔쳐보는 방법을 써라 NM? 임의의 변수 $C = m^e \bmod n$
→ 도청공격 (CCA? 임의의 변수 $= C^d \bmod n$ IND, CC NM

7. above attack의 솔루션을 써라.(위의 공격)
↳ 대응방안 →



8. 아래의 그림을 그리는 것이 답. 그리고 각각을 설명하고 국내/국외의 정책을 비교하시오.


Information Security Policies
Identification & Authentication function, etc.
Various security functions of IT security product
"Module"
Crypto algorithms implemented in security products
"Algorithm"
"Product"
H/W Security, EMI/EMC, etc.
"System"
"Environment"
CAVP
Cryptographic Algorithm Validation Program
CMVP(FIPS140-2)
ISO/IEC 19790
Cryptographic Module Validation Program
NIAP(CC)
ISO/IEC 15408
National Information Assurance Program
DITSCAP
DoD IT Security Certification and Accreditation Program
NIST C&A
Certification and Accreditation

9. 엄청나게 긴문제인데....

간호사가 환자 차트를 저장하는데... 한번 저장하면 90일 동안 접근 권한이 있는데, 이 접근 format이

patient-id, issue-date, hmac(k, (patient-id, issue-date))

이것이다.

key를 갖고있다면 - 사용가능.

a) A 간호사가 위의 파일을 USB에 담아와서 B에게 주고, B가 다시 C에게 주고, C가 D한테 주면, D는 사용가능한가? 90일간 사용가능? 이유?

b) 서로 쓰는 것을 막기 위해서 만약 다른 사람에게 전달하면 90일 동안 ~~열람 가능~~한게 아니라, 10일 동안만 가능하게 바꾸고자 한다. Explain a new format for capabilities which would support this new policy. timestamps,

ACL vs

patient-id, issue-date, hmac (k, (patient-id, issue-date ~~timestamps~~)), timestamps

* Nurse ID를 통해 인증대상을 거친다.

if ~~환자의~~ 간호사 id = 간호사(90일) else (10일))

※ 이해 안되거나 확인하고 싶은거 있음 언제든 전화해서 묻고, 일단 화욜날 오면 한번 연락줘~ 다들 힘내서 100점 맞아!!

답은........확실치 않아서 ㅋㅋ

Attributed -

2012. 기말

1. 헤티스 그림그리기

In hospital we have 4 kind of user: Doctor > Nurse= secretary > Patient

Medical information have security levels for files, in decreasing order : Operating room> emergency > personal

2. Suppose that a receipt containg payment information has security level(secretary, personal),

A prescription for antibiotics has security level(Doctor, Emergency) The list of medical tools necessary for an operation has security level(Nurse, Operating room) and the file containing the home address of patients in the hospital has security level(secretary, emergency). Place all these coduments (in the paragraph above) on the preceeding lattice.

< 3~4 가정 >

Dave- the surgen has clearance (Doctor operation room)
Nancy- Nurse has clearance(Nurse, emergency room)
Shari- the secretary has clearance(Secretary, emergency)
Paul - the patient has clearance(Patient, personal)

3. 벨 라파듈라, if the follwing actions are allowed, explaining each time why that is.

(a) Dave writes on the list
(b) Nancy read the files

(c) paul writes on the prescription

(d) shari read the receipt

4. 비바모델

(a) Dave writes on the list

(b) Nancy read the files

(c) Dave writes on the file

(d) shari read the prescription

5. (a)접근제어에서 capability란?

(b) explain an advantage of access control list over capability lists

(c) Explain an advantage of capagility list over access control list

6. We consider 1 and 0 the two possoble ballots for an election.
A server publishes his public RSA key (N,e).

Each voter encrypt his vote 0 or 1, as RSA(N,e) 0 or RSA (N,e) 1 , respectively.

At the end of the eletion the server decrypt all received message and count the votes.

Show how an attacker eavesdropping on the network can learn everybody vote.

7. Propose a solution in order to avoid the above attack

8.Draw CAVP, CMVP, CC & C&A

9. Hospital patient record system provide login account for nurse. It is desire to implement the following policy:

1) When a nurse register a new patient, the nurse is granted access to the patient records for a period of 90 days.

2) A nurse passing the right to access a patient record anc give that right to another user. This may be done office.

The implement this policy, the system works as follow, when an nurse register new patient, a capability to access the patient record for the following 90 days in generated.
The nurser stores it on a usb stick, and may copy it onto other usb stick to give to other user.
When a user attempt to access patient records, she is promoted to upload the relevant capability.
The capability has the following format

F , O

patient- id, issue-date, hMAC(k, patient-id, issue-date)

Where HMAC(k,...) denote a suitable keyed hash function with key K. The key K is a secret key.
Known only the patient record system, Any user in possession of this capability is able to access the records of the patient with patient-id, provided the date is with in 90 days after issue date

(a) Suppose nurse register a patient and receives such a capability. A passes it to B, B passes it C, ans C passes it to D. Is D able to

복사여부.

issudate, F, , ~~[illegible]~~ expi_date, use the capability?

(b) In order to stop long-lived capabilities being distributed widely, the hospital decides to adopt the policy that the nurse that initially registers the patient will have access to the record for 90 days, as before, if she passes the capability to any other user. the validity should be 10 days from it issue-date.

Explain a new format for capability which would support this new polocy.