【2012.2학기】 기말고사

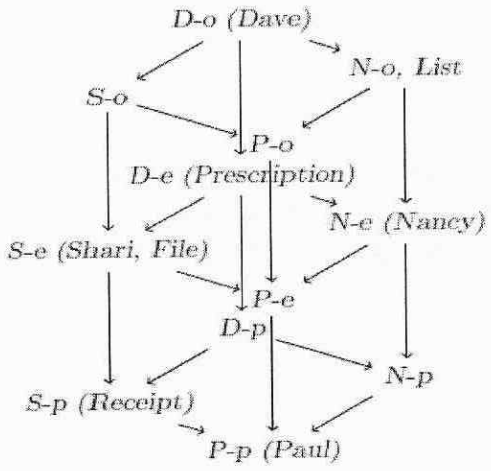
In a hospital we have 4 kind of users: Doctor, Nurse, Secretary, Patient. In this hierarchy, Doctors are superior to Nurse, Secretary and Patient, Nurse and Secretary are superior to Patient, but Nurse is neither superior nor inferior to Secretary. Medical information have several security levels for files, in decreasing order: Operating room, Emergency and Personal.

1. Draw a lattice of all the security clearances.

Suppose that Dave the surgeon has clearance (Doctor,Operating room), Nancy the nurse has clearance (Nurse, Emergency), Shari the secretary has clearance (Secretary, Emergency) and Paul the patient has clearance (Patient, Personal). A Receipt containing payment information has clearance (Secretary, Personal), a Prescription for antibiotics has clearance (Doctor, Emergency), the List of medical tools necessary for an operation has clearance (Nurse, Operating room) and the File containing the home address of patients in the hospital has clearance (Secretary, Emergency).

2. Place all these actors and documents (in bold in the paragraph above) on the preceeding lattice.

1, 2번 답)



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

a) Dave writes on the List. → no (write down 금지)
b) Nancy reads the File. → no (서로 관계가 없는 노드들, 어떤 것도 허용되지 않음)
c) Paul writes on the Prescription → yes (write up 허용)
d) Shari reads the receipt. → yes (read down 허용)

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

a) Dave writes on the List → yes (write down 허용)
b) Nancy reads the File → no (서로 관계가 없는 노드들, 어떤 것도 허용되지 않음)
c) Dave writes on the File → yes (write down 허용)
d) Shari reads the prescription. → yes (read up 허용)

5.

(a) In access control systems, what is a capability?

- ○ Access Control Matrix에서 행(rows)을 나타내며, 사용자를 중심으로 접근권한을 리스팅 함으로써 subject가 각 자원에 대해 어떠한 접근권한을 가질 수 있는지 나타냄
- ○ 자원에 접근할 수 있는 권한을 증명하는 데이터 소유의 부분임

(b) Explain an advantage of access control lists over capability lists.

Access control list는 administrator가 주어진 resource에 대해 누가 접근할 수 있는지를 파악하기가 capability보다 쉽다.

(c) Explain an advantage of capability lists over access control lists.

Capability는 유저들 간에 오프라인으로 이전될 수 있다. (이것은 access control list에서는 일반적으로 가능하지 않다.)

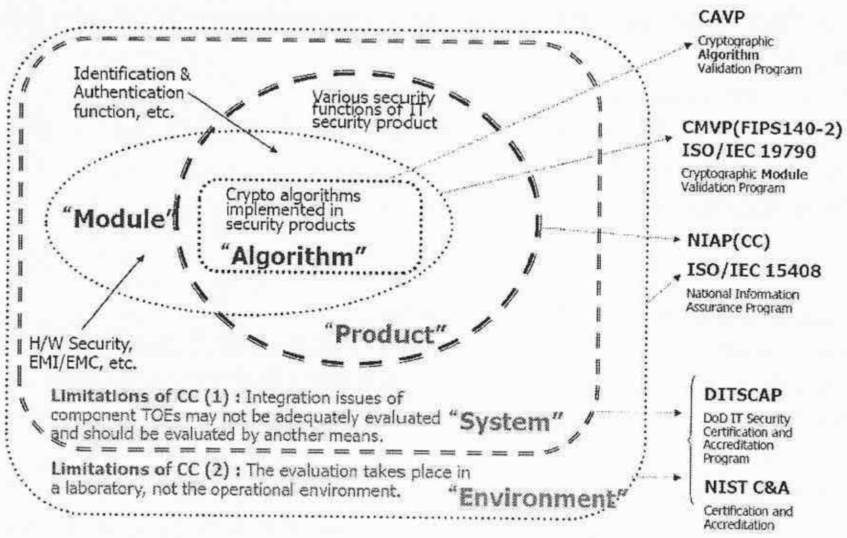
6. We consider that 1 and 0 are the two possible ballots for an elections. A server publishes his public RSA key (N; e). Each voter encrypt his vote, 0 or 1, as RSA(N,e)(0) or RSA(N,e)(1) respectively. At the end of the election the server decrypt all received messages and counts the votes. Show how an attacker eavesdropping on the network can learn everybody's vote.

공격자는 RSA(N,e)(0) 또는 RSA(N,e)(1)의 값을 미리 계산한 후 네트워크상에서 투표의 내용을 도청하여 그 값을 비교해 봄으로써 모두의 투표내용을 알아낼 수 있다.

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

ElGamal과 같은 IND-CPA 스킴을 사용하면 2개의 투표내용을 구별하는 것이 가능하지 않다. 랜덤 패딩을 통해 Polynomial Security(IND-CPA)를 충족시킨다. RSA-OAEP를 사용하면 Random Padding을 통해 Polynomial security, Semantic security를 충족하고 Fixed Padding을 통해 위변조를 방지할 수 있다.

8. Draw CAVP, CMVP, CC, C&A. 국내/국외의 정책을 비교


Identification & Authentication function, etc.
Various security functions of IT security product
Crypto algorithms implemented in security products
"Module"
"Algorithm"
"Product"
H/W Security, EMI/EMC, etc.
Limitations of CC (1) : Integration issues of component TOEs may not be adequately evaluated and should be evaluated by another means.
"System"
Limitations of CC (2) : The evaluation takes place in a laboratory, not the operational environment.
"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

<우리나라와 미국의 비교>

- ㅇ 미국의 경우에는 누가 개발했는지 상관없이 일정기준을 충족하면 CAVP 리스트에 등재가 되나 우리나라는 국정원장이 승인한 알고리즘만 사용하므로 CAVP가 없다
- ㅇ 미국의 CMVP는 CAVP를 통과한 알고리즘에 대해 암호모듈을 평가하나, 우리나라의 K-CMVP는 국정원장이 승인한 알고리즘에 대해 암호모듈을 평가한다.
- ㅇ 우리나라는 2006.5월 CCRA 인증서 발행국으로 협약에 가입하였으나 CC제도가 국내용과 국제용으로 이원화되어 있으며, 국내용의 경우 평가보증등급에서 요구하는 평가항목 중 보안기능과 취약성시험을 제외한 일부 항목을 표본추출하여 평가하므로 Assurance가 훼손될 수 있다.
- ㅇ 우리나라에는 C&A가 없다 : C&A는 CC, CMVP 등을 모두 포함하는 개념으로 산재된 모든 보안정책을 통합하여야 하나 현실적으로 불가능하다.

9. A hospital patient record system provides login accounts for nurses. It is desired to implement the following policy:

(i) When a nurse registers a new patient, the nurse is granted access to the patient's records for a period of 90 days.

(ii) A nurse possessing the right to access a patient record can give that right to another user (this facilitates staff shift changes). This may be done offline.

To implement this policy, the system works as follows. When a nurse registers a new patient, a capability to access the patient record for the following 90 days is generated. The nurse stores it on a USB stick, and may copy it onto other USB sticks to give to other users. When a user attempts to access patient records, she is prompted to upload the relevant capability. The capability has the following format:

patient-id, issue-date, hmac(K, (*patient-id, issue-date*))

where hmac(K,...) denotes a suitable keyed hash function with key K. The key K is a secret key known only to 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 within 90 days after *issue-date.*

a) Suppose nurse A registers a patient and receives such a capability. A passes it to B, B passes it to C, and C passes it to D. Is D able to use the capability?

Yes, 전달된 capability는 여전히 유효기간(validity period) 내에 있으므로 D는 capability를 사용할 수 있다.

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 records for 90 days, as before, but if she passes the capability to any other user, the validity should be 10 days from the issue date. Explain a new format for capabilities which would support this new policy.

capability format에 user id를 포함시키면 시스템은 그 해당 user에게 90일간 권한을 부여하고 그 외 다른 user들에게는 10일간 권한을 부여하도록 프로그램 될 수 있다.

new format : *patient-id, issue-date, user-id,* hmac(K, (*patient-id, issue-date, user-id*))