보안공학 종합시험 2013. 3. 합격선 70 (ack)

1. 무어의 법칙이 2050년까지 계속된다고 할 때 AES-128, 192, 156bit의 안전성은 어떻게 변화하는가? (10/10)

2. CAVP, CMVP, CC, C&A, DITSCAP 및 국내와 미국 평가제도 비교설명(5/10)

용어 정의와 뜻을 각각 다 써야함. 그림을 다 그리고, 각 용어가 무엇인지, 한국과 미국은 어떻게 다른지 자세히 기술해야 함
나는 용어만 쓰고, CAVP, CMVP, CC 가 무엇인지 그림만 그리고 뜻을 쓰지 않아서 점수가 깎임

3. BLP모델

(1) b, m, f의 의미(0) formal method

b : Access operations currently in use b, List of tuples (s, o, a), s∈S,

m : Access Permission matrix, M=(Ms,o)s∈S, o∈O, where Ms,o⊂A

f : clearance and classification f = (fs, fc, fo), fs : S → L ..... 등...

(2) ss-property를 b,m,f를 이용하여 표현(0) formal method

(3) *-property를 b,m,,f를 이용하여 표현(0) formal method

(4) BLP의 특징 및 단점 3가지(7/10) --> 비효율적 X

① 오로지 기밀성에만 초점을 두고 있음 → Biba는 무결성을 다룸 〈 전반적인 예제 〉

② 접근제어 권한이 중간에 변경되었을 때의 문제를 다루고 있지 않음

③ 은닉채널에 의한 정보흐름의 문제를 다루고 있지 않음

(5) 은닉채널이란 무엇이며, BLP모델에서의 은닉채널의 예로는 무엇이 있는가?

은닉채널이란 당초의 보안 메커니즘 설계자가 의도하지 않은 통신채널,

BLP에서 *-property로만 완벽히 막는 것은 불가능함, 그러므로 은닉채널을 통해 유출되는 정보의 양(Band width)을 줄이는 연구가 중요함

BLP에서 중간에 접근 권한이 변경될 경우 정보의 흐름이 위에서 아래로 흐르는 것이 깨지게 된다.

4. a. What is a capability? ★★
b. advantage of access control list over capacity? ,ACL(Access Control List)
c. advantage of capacility over access control list? ,CL(Capacitiy List)

5. 간호사 문제
(1) 90일간 유효한 티켓을 다른 사람에게 주어도 유효한가?
(2) 나에게는 90일 유효, 다른 간호사에게는 10일 간만 쓰게 하는 새로운 정책 선언 ★★

6. V, A, T의 정의

7. C, I, A의 정의: 기밀성은 접근제어를 통해서도 달성 가능

8. Salt와 관련된 문제, pw가 유출되었을 때 다른 사이트에서도 활용가능한가?

salt는 공개된 난수 값이기 때문에 사용자별로 salt값은 다 다르며, 다른 사이트에서 password에 대한 guessing이 불가능하다.

9. password와 관련된 공격의 종류와 뜻

가. guessing attack : brute forcing, dictionary attack --> large salt value, key stretching algorithm 활용

나. sniffing
다. replay attack
라. stolen verify attack

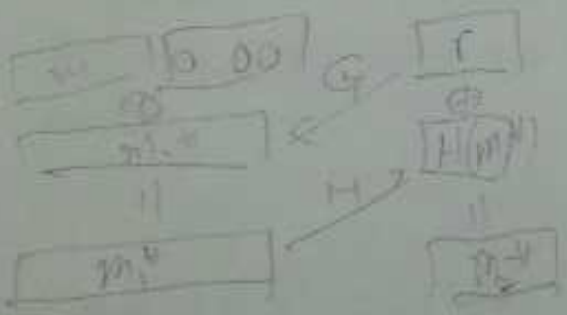
10. ~~Lattice 문제~~

Security Goal

11. RSA 전자투표 시스템 안전한가? 안전하지 않은가?

RSA-OAEP를 사용하면 됨(NM - Fixed Padding, IND - Random Padding)

12. MAC, DAC, RBAC의 차이점에 대해 서술하라



45
+
25
11
70