13. MAC, DAC, RBAC의 차이점에 대해 서술하라.

○ DAC Model : 임의적 접근제어 모델
- needs-to-know 원리에 의해 정보를 보호
- data owners가 누가 resource에 접근할 수 있는지를 결정
- subject의 identity에 근거하여 접근을 승인하거나 거절.
  · identity는 user identity 또는 group membership이 될 수 있음
- DAC은 copy가 이루어지는 것을 막지 못하고 이에 대한 통제도 없다.
- 파일 소유주가 임의로 권한을 부여함에 따라 flexibility는 매우 높으나 엄격한 보안통제는 어렵다.

○ MAC Model : 강제적 접근제어 모델
- 어떤 sensitivity level에 접근하는 것이 허락되는 지를 정의하는 clearances를 user에게 할당함으로써 정보를 보호한다.
- MAC에서 users에게 부여된 clearances는 엄격히 준수된다.
  · DAC과는 달리 permissions이 user의 임의대로 전달될 수 없다.
- DAC과는 반대로 flexibility는 낮으나 엄격한 보안통제가 가능하다.
- Partial ordering으로 Lattice 구조를 만족한다.

○ RBAC(Role-Based Access Control) Model : 역할기반 접근제어 모델
- 회사 내에서 user가 보유하는 역할에 기반하여 resource에 대한 접근을 허락하는 모델
- MAC, DAC은 사람에게 권한을 부여하고 RBAC은 역할에 권한을 부여한다.
- User는 자주 바뀌나 역할은 자주 바뀌지 않으므로 사람에게 권한을 부여하는 것보다 에러가 적고 직관적이다.

【2013.2학기】 중간고사

1. Computer Security, Information Security, Information Assurance를 정의하고 비교하라

	Computer Security	Information Security	Information Assurance
Dates	1960s	1980s	1998
Subject of protection	Computers	Information and information systems	Business as a whole
Goals	Reliability	Confidentiality Integrity Availability	Confidentiality Integrity Availability Non-repudiation Accountability Possession Utility Authenticity Auditability Transparency Cost effectiveness Efficiency
Type of information	Electronic	Primarily electronic	All types
Approach	Strictly technical approach	technical approach가 주를 이룸. human factor, administration과 같은 면을 고려하려는 시도가 있었음	All-encompassing multi disciplinary systematic approach
Security Mechanisms	Technical	technical security mechanism에 주요 초점. organizational and human-oriented mechanisms을 처음 고려.	All available (technical, organizational, human-oriented, legal)
Role within a business	Supporting system	Supporting system, 종종 business에 대한 restriction을 부여	An integral aspect of business, business enabler
Responsible employees	Technical staff	Dedicated staff and technical staff	Senior management and dedicated staff
Involved employees	Technical staff	Senior management, dedicated staff and technical staff	All employees with an organization
Drivers	Technical-needs driven	Security-needs driven	Business-needs driven
Flow of security decisions	Bottom-Top (경영진은 security의 기술적 측면에 관심이 없음)	Bottom-Top (보안대책이 기술적 전문가에 의해 그들의 경험에 근거하여 성립되고, 승인을 위해 경영진에 보고됨)	Top-Bottom (보안대책이 경영진에 의해 risk analysis에 근거하여 성립되고, 관련 부서에 의해 구현됨)

2. Vulnerability, Threat, Attack을 정의하고 예를 제시하라.

- Assets : Software, Hardware, Data and Information, Reputation
  - 식별은 쉬우나 평가는 어려움
  - Data, Information, Reputation은 측정이 어려움
- Vulnerabilities : Weaknesses of a system that could be accidentally or intentionally exploited to damage assets
- Threats : Actions by adversaries who try to exploit vulnerabilities to damage assets
- Attack : attack이 성공하면 Threat이 구체화되어 실현된다.
  이를 위한 일련의 절차 · 단계를 말한다.

예) vulnerability : input에 대한 검증을 하지 않는 오류를 가진 프로그램
Threat : vulnerable한 프로그램에서 Cross-Site Scripting에 의해 cookie 유출
Attack : Attacker가 user들에게 악의적인 link가 담긴 e-mail을 보내는 절차 등을 시행하여 Threat을 실현

3. 2013.1 종합시험 1번 동일

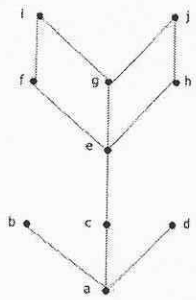
4. desktop의 standard password, iphone의 4 pin password, android pattern password의 암호체계를 분석 비교하고 개선 대책을 제시하시오

- Android의 pattern password는 사람의 지문 흔적 등이 기기에 남아있기 때문에 세 방법 중 공격에 가장 취약하다
- iphone은 4 pin이고 무선네트워크를 사용하므로 모든 경우에 대해 순서대로 전수조사하는 공격(Brute Force Attack), 패스워드로 많이 쓰이는 단어들부터 우선적으로 조사하는 공격(Dictionary Attack) 등에 있어서 desktop보다 더 취약하다.
- 기존 사용자 인증의 보조수단으로 Biometrics 등을 추가하고 인증수단을 강화하는 방법이 있다.

5. 2013.1 종합시험 13번 동일

6. 2013.1 종합시험 10번 동일

7.



■ (e.g.) Given two objects at different security levels b, c, what is the minimal security level a subject must have to be allowed to read both objects?

- lattice? No, because the pair {b, c} does not have a least upper bound

8, 9, 10. 2012.2학기 기말고사 1,2,3,4번 참조