【2013.1】 종합시험

1. 무어의 법칙이 2050년까지 계속된다고 가정할 때 AES-128, 192, 256의 안전성은 2050년에도 유효한가?

→ 무어의 법칙은 반도체 집적회로의 성능이 18개월마다 2배씩 증가한다는 것이다.
2050년 - 2013년 = 37년, 37 × 12월 = 444 개월
444/18 = 24.6667이므로 2050년에는 2013년 현재보다 2^24배 성능이 증가한다.
즉, 2013년 현재 64비트 컴퓨터의 연산능력을 2^64라하면 2050년에는 2^88의 연산능력을 갖는다.
따라서, AES 키 값에 대한 전수조사 공격을 실시한다면 AES-128은 안전성이 깨질 수 있으며, AES-192, AES-256은 여전히 안전서이 유효하다.

2. 윈도우 서버를 운영할 때 로그인시 CTRL+ALT+DEL 키를 동시에 눌러서 로그인하는 이유는 무엇인가?

→ CTRL+ALT+DEL 키를 동시에 눌러서 로그인 하는 것은 보안설정의 한 방법으로 대화형 로그인이라고도 한다. 이를 통해 인증되지 않은 사용자나 악성 프로그램이 컴퓨터에 접근하는 것을 방지할 수 있다.

3. 2012.2학기 기말고사 8번 동일

4. BLP 모델

(1) b, m, f의 의미

○ The State Set
- A state : (b, M, f), includes
- Access operations currently in use b
  · List of tuples (s, o, a), s∈S, o∈O, a∈A
- Access permission matrix
  · M = $(M_{s,o})_{s\in S, o\in O}$, where $M_{s,o}\subset A$
- Clearance and classification f = (f_S, f_C, f_O)
  · $f_S : S \rightarrow L$ maximal security level of a subject
  · $f_C : S \rightarrow L$ current security level of a subject ($f_C \leq f_S$)
  · $f_O : O \rightarrow L$ classification of an object

○ Elements of Access Control
- a set of subjects S
- a set of objects O
- set of access operations A = {execute, read, append, write}
- a set of security Levels L, with a partial ordering ≤

(2) ss-property를 b, m, f를 이용하여 표현

○ Simple Security Property (SS-Property) : <Read down>
- A state (b, M, f) satisfies the SS-property if
  · ∀(s, o, a)∈b, such that a∈{read, write}
  · $f_O(o) \leq f_S(s)$
- 즉, subject는 더 낮은 classification의 object들만 observe할 수 있다.

(3) *-property를 b, m, f를 이용하여 표현

○ *-Property (Star-Property) : <Write up>
- A state (b, M, f) satisfies the *-property if
  · ∀(s, o, a)∈b, such that a∈{append, write}
  · $f_C(s) \leq f_O(o)$

and
  · if ∃(s, o, a)∈b where a ∈{append, write},
  · then ∀o', a' ∈ {read, write}, such that (s, o', a')∈b
  · fo(o') ≤ fo(o)
- subject는 더 높은 classification의 object들만 변경할 수 있으며, low-level object에 쓰고 있는 동안에는 high-level object를 읽을 수 없다.

(4) BLP의 특징 및 단점 3가지

○ 의의 : gave a formal, mathematical model of MLS
to provide higher policy assurance of correctness
- 시스템이 어떤 환경에서 어디까지 할 수 있는지를 명확히 알 수 있다.
- 정보가 아래에서 위로 흐른다.

○ problem
- integrity는 다루지 않고 confidentiality만 다룬다.
- 접근권한의 변경을 통제하는 policy를 가지고 있지 않다.
- covert channel을 통한 information flow를 다루지 않는다.

(5) 은닉 채널이란 무엇이며 BLP 모델에서의 은닉채널의 예로는 무엇이 있는가.

○ 은닉채널 : 설계자가 당초에 의도했던 입출력 통로가 아닌 다른 통로를 통해 정보를 끄집어내는 것 ex) 카메라로 찍기

○ Covert channel은 *-property로 막을 수 없다.

○ 모든 covert channel을 막는 것은 일반적으로 매우 어려운 일이며, covert channel의 bandwidth를 제한하는 노력을 할 수 있다.

○ Military는 covert channel을 통해 keys를 유출하는 트로이목마를 방지하기 위해 암호 component를 hardware로 구현할 필요가 있다.

○ (예) High User(subject)를 전염시킨 트로이목마로부터 Low User(subject)를 전염시킨 트로이목마로 정보가 유출된다.(High User는 정보가 유출된 사실을 알지 못한다.)

5. 2012.2학기 기말고사 5번 동일

6. 2012.2학기 기말고사 9번 동일

7. Vulnerability, Asset, Threat

- ○ 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

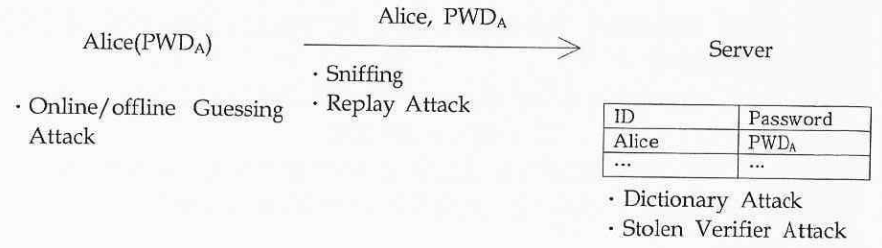
8. Confidentiality, Integrity, Availability

- ○ Confidentiality : *달성수단 Encryption(통신 중인 data), Access control(저장 중인 data)*
  - Prevent unauthorized disclosure of information
- ○ Integrity : *달성수단 MAC(대칭키 기반), 전자서명(공개키 기반)*
  - Prevent unauthorized modification of information
- ○ Availability
  - Services are accessible and useable (without undue Delay) whenever needed by an authorized entity
    · fault-tolerance가 필요

9. (LinkedIn, Facebook 해킹 salt와 관련된 문제) 패스워드가 유출되었을 때 다른 사이트에서도 활용가능한가?

salt는 불특정 다수에 대한 dictionary attack을 지연시키기 위해 사용하는 공개된 난수값이기 때문에 사용자별로 salt값은 다르며, 다른 사이트에서 password에 대한 guessing은 불가능하다.

10. password와 관련된 공격의 종류와 뜻



- ○ Password Guessing Attacks
  - Brute Force Attack : 모든 경우에 대해 순서대로 전수 조사하는 공격
  - Dictionary Attack : 패스워드로 많이 쓰이는 단어들부터 우선적으로 조사
  - (대응)
    · 에러의 발생 사실만 알려주고 자세한 에러의 내용은 알려주지 않음. 에러 정보를 가지고 공격 가능(Padding Oracle Attack)
    · 비정상적인 로그인 실패횟수를 탐지
    · 패스워드를 hash해서 저장(shadow file)
    · 'large salt values'*를 사용하여 여러 불특정 사용자들(multiple user)에 대한 공격을 방지
    * salt : 불특정다수에 대한 dictionary attack을 지연시키기 위해 사용하는 공개된 난수값
    · 'key stretching algorithms'(예 : PBKDF2)을 사용하여 패스워드에 Hash를 반복 적용함으로써 특정 사용자(single user)에 대한 집중 공격(chosen-victim attack)을 방지
- ○ Sniffing : 도청 및 패스워드 훔치기
  - (대응) 패스워드의 암호화를 통한 전송

Replay Attack : data packets을 가로채서 수신 서버에게 재전송하는 것과 관련된 중간자 공격(man in the middle attacks)의 일종이다. 패스워드를 재사용한다.
- (대응) 인증과정에서 nonce나 timestamp 값을 추가

Stolen Verifier Attack : 패스워드를 탈취한 후 해독하는 것이 아니라 전송하는 형식을 조금만 조작해서 서버에 전송하는 방법

11. 2012.2학기 기말고사 1,2,3,4번 동일

12. 2012.2학기 기말고사 6,7번 동일

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)