มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

การสอบไล่กลางภาคการศึกษาที่ 1 **ประจำปีการศึกษา 2548**

วันที่ 2 สิงหาคม **2548** **เวลา** 09.00 - 12.00

วิชา 240-425 Computer and Information Security **ห้องสอบ** R201

ไม่อนุญาตให้นำเอกสารเข้าในห้องสอบ

ทุจริตในการสอบ มีโทษขั้นต่ำ คือ ปรับตกในรายวิชาที่ทุจริต และพักการเรียน 1 ภาคการศึกษา

1 Basic Cryptography

1.1 จาก ข้อความ ciphertext ต่อไปนี้ของ Rail Fence Cipher จงถอดรหัสให้เป็น Plaintext
IAESW CNURD CMIAI OQEE (5 คะแนน)
1.2 ในระบบรหัสแบบ VIGENERE จง encipher ข้อความ plaintext BOYHAS โดยใช้ key คือ VIG ให้ได้ ข้อความ ciphertext (15 คะแนน)

2 RSA Public Key Cryptography

2.1 หลักการในการทำงานในระบบ RSA Public Key Cryptography จะต้องมี conditions สามข้ออะไรบ้าง (5 คะแนน)
2.2 ในระบบ RSA cryptosystem ที่ค่า n=77
มีการติดต่อระหว่าง Alice กับ Bob โดยที่
Public Key ของ Alice = 17
Private Key ของ Alice = 53 (รู้เฉพาะ Alice คนเดียว)
Public Key ของ Bob = 37
Private Key ของ Bob = 13 (รู้เฉพาะ Bob คนเดียว)
ในระบบนี้ plaintext แต่ละตัวอักษรถูกแทนค่าด้วยตัวเลขระหว่าง 00 (คือ A) และ 25(คือ Z) และ 26 แทนด้วย ช่องว่าง

2.2.1 ถ้า Bob ต้องการส่งข้อมูลที่ Confidential ไปยัง Alice เป็นตัวอักษรคำว่า HELLO ซึ่ง plaintext จะมีค่าเป็น 07 04 11 11 14 ต้องเข้ารหัส เป็น ciphertext อย่างไร (ไม่จำเป็นต้องคำนวณค่าออกมา) (7 คะแนน)

2.2.2 Alice ได้รับ ciphertext แล้ว จะถอดรหัสเป็น Plaintext อย่างไร (3 คะแนน)

2.2.3 ถ้า Alice ต้องการส่งข้อมูลที่ Confidential และ Authenticate(เพื่อแสดงว่าข้อความถูกส่งไปจาก Alice) ไปยัง Bob เป็นตัวอักษรคำว่า HELLO ซึ่ง plaintext จะมีค่าเป็น 07 04 11 11 14 ต้องเข้ารหัสอย่างไร (ไม่จำเป็นต้องคำนวณค่าออกมา) (7 คะแนน)

2.2.4 Bob ได้รับ ciphertext แล้ว จะถอดรหัสเป็น Plaintext อย่างไร และจะ Authenticate อย่างไรว่า message มาจาก Alice (3 คะแนน)

3 Authentication

3.1 Information ที่จะต้องใช้เพื่อให้ entity ภายนอกสามารถยืนยัน identity ของตนเองในกระบวนการ Authentication มาจากแหล่งไหนได้บ้าง (10 คะแนน)

3.2 ห้าองค์ประกอบของระบบ Authentication System มีอะไรบ้าง ให้อธิบายโดยยกตัวอย่างในระบบที่ใช้ Password (10 คะแนน)

3.3 การรับมือกับ การ attack ด้วยการเดา Authentication Functions ในรูปแบบต่อไปนี้ทำอย่างไร
backoff
disconnection
disabling
jailing
(10 คะแนน)

4 Confidentiality Policy

4.1 อธิบายโครงสร้างพื้นฐานของ Bell-LaPadula model ในการแบ่งระดับชั้นของ Security Policy ในแง่ของ Security Classification และ Security Clearance ยกตัวอย่างให้เห็นชัด. (10 คะแนน)

4.2 การเพิ่ม categories เข้าไปใน Bell-LaPadula model มีผลกระทบอย่างไร (5 คะแนน)

5. Chinese Wall Model Hybrid Policy

5.1 Company Dataset (CD) และ Conflict of Interest (COI) class ต่างกันอย่างไร (5 คะแนน)

5.2 Sanitized Object คืออะไร (5 คะแนน)

5.3 ใน Simple Security Condition ถ้า Subject S จะอ่าน Object O ได้ ต้องมี ข้อแม้อะไรบ้าง (10 คะแนน)

5.4 ใน Star Property ถ้า Subject S จะเขียนไปที่ Object O ต้องมีข้อแม้อะไรบ้าง (5 คะแนน)

5.5 หลักการพื้นฐานของ Bell-LaPadula และ Chinese Wall Model ต่างกันอย่างไร (5 คะแนน)

6 Integrity Policy

6.1 Lipner requirement ห้าข้อของ Integrity Policy มีอะไรบ้าง (10 คะแนน)

6.2 อธิบายหลักการของระบบ ในระดับ operation ที่เน้น Integrity ซึ่งเป็นผลจาก Lipner requirement ในหัวข้อดังต่อไปนี้

-Separation of Duty
-Separation of function
-Auditing
(10 คะแนน)

6.3 ใน Clark Wilson Integrity Model จงอธิบาย Entity ต่อไปนี้ พร้อมยกตัวอย่างในกรณีบัญชีในธนาคาร

-Constrained Data Item (CDI)
-Unconstrained Data Item (UDI)
-Integrity Verification Procedure (IVP)
-Transformation Procedure (TP)
(10 คะแนน)

6.4 Certification Rules เป็นกฎเกณฑ์ที่องค์กรภายนอกต้องรับรองการทำงานว่าทำตาม Integrity Model มีห้าข้อมีอะไรบ้าง (10 คะแนน)

6.5 Enforcement Rule เป็นกฎเกณฑ์ภายในองค์กรที่ต้องปฏิบัติตามเมื่อใช้ Clark Wilson Model มีสี่ข้อมีอะไรบ้าง (10 คะแนน)

7 Clinical Information Systems Security Policy (CISSP)

7.1 หลักการเข้าถึงข้อมูล medical records ของระบบ Clinical Information Systems Security Policy (CISSP) สี่ข้อมีอะไรบ้าง จงอธิบาย (10 คะแนน)

7.2 จงอธิบายหลักการใช้งาน medical records ของระบบ Clinical Information Systems Security Policy (CISSP) มุมมองต่างๆดังนี้ Policy (CISSP)
Creation Principle
Deletion Principle
Confinement Principle
Aggregation Principle
Enforcement Principle (10 คะแนน)

8.จงอธิบายหลักการต่อไปนี้ของการออกแบบระบบ security ซึ่งเน้นในระบบคอมพิวเตอร์ (10 คะแนน)

หลักการของLeast Privilege

หลักการของFailsafe Defaults

หลักการของ Economy of Mechanism

หลักการของ Complete Mediation

หลักการของ Separation of Privilege

.....