มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

การสอบไล่ปลายภาคการศึกษาที่ 1 **ประจำปีการศึกษา 2548**

วันที่ 5 ตุลาคม 2548 **เวลาสอบ 09.00-12.00 น.**

วิชา 240-425 Computer and Information Security **ห้องสอบ A401**

คำสั่ง

ไม่อนุญาตให้นำเอกสารเข้าในห้องสอบ

ตอบคำถามทุกข้อ คะแนนเต็ม 170 คะแนน

โทษขั้นต่ำ ปรับตกในรายวิชาที่ทุจริต และพักการเรียน 1 ภาคการศึกษา

1 Basic Cryptography

1.1จาก ข้อความ ciphertext ต่อไปนี้ของ Rail Fence Cipher จงถอดรหัสให้เป็น Plaintext

AEUEO PTRYT MSCRC MUESS E (5 คะแนน)

1.2สำหรับระบบIntrusion Detection System

1.2.1 ในแง่ของการตรวจสอบการทำงานของ ผู้บุกรุกเข้ามาในระบบคอมพิวเตอร์ แล้ว ระบบฯที่ทำงานปกติ ในแง่ของ users และ processes จะมีคุณลักษณะสามข้ออะไรบ้าง (5 คะแนน)

1.2.2 คุณสมบัติที่พึงประสงค์สี่ประการของ Intrusion Detection System(IDS) มีอะไรบ้าง จงอธิบาย (5 คะแนน)

1.2.3 อธิบายการทำงานทั้งสามรูปแบบของ Anomaly Modeling เพื่อ Intrusion Detection คือ

-แบบThreshold metric

-แบบ Statistical moment

-แบบ Markov Model (10 คะแนน)

1.2.4 อธิบายการทำงานของ Misuse-based Modeling เพื่อ Intrusion Detection (5 คะแนน)

2 Identity

2.1 Level of trust of signature fields of PGP certificates ซึ่งทำกับ user name และ public key ทั้งสี่ระดับนี้ต่างกันอย่างไรในแง่ของ trustworthiness.

-Generic certification

-Persona certification

-Casual certification

-Positive certification (5 คะแนน)

2.2Cookies มีไว้เพื่อทำหน้าที่อย่างไรเพื่อระบุ Identity (5 คะแนน)

2.3 เปรียบเทียบการทำงาน ของ การไม่ระบุตัวตน(Anonymizer) ใน ไปรษณีย์อิเล็กทรอนิกส์ สามแบบต่อไปนี้ คือ
Pseudonymous remailer
Cypherpunk(type 1) remailer
และ Mixmaster Remailer(Type 2) ทำงานต่างกันอย่างไร (15 คะแนน)

3. Assurance
3.1 อธิบายความหมายของ
-Trustworthy
-Trust
-Security Assurance (5 คะแนน)

3.2 เก้าแหล่งที่มาของปัญหาที่ทำให้เกิดปัญหา ของระบบคอมพิวเตอร์ซึ่งจะนำไปสู่ปัญหาเรื่องความล้มเหลวของความมั่นคงปลอดภัย (Security Failures) มีอะไรบ้าง (10 คะแนน)
3.3.อธิบาย lifecycle assurance ของผลิตภัณฑ์ คือ
-Policy assurance
-Design assurance
-Implementation assurance
-Operational assurance (10 คะแนน)
3.4 จงอธิบายข้อแตกต่างระหว่าง
3.4.1Reference Monitor และ Reference Validation Mechanism(RVM) (5 คะแนน)
3.4.2 Security Kernel และ Trusted Computing Base(TCB) (5 คะแนน)

4. Evaluating Systems.
4.1จงอธิบาย Trusted Computer System Evaluation Criteria(TCSEC)
functional requirements
-Discretionary Access Control(DAC) requirements
-Mandatory Access Control(MAC) requirements
-Label requirements
-Audit requirements
-Trusted Path requirements (10 คะแนน)

4.2 อธิบาย การจำแนก ลำดับชั้นของ Trusted Computers ของ TCSEC
TCSEC Class A1(Verified Protection)
TCSEC class B3 (Security Domains)
TCSEC Class B2(Structured Protection)(10 คะแนน)

4.3 อธิบาย Security Level 4 ของ FIPS 140-2 (5 คะแนน)
4.4.อธิบายห้าระดับของ Capability Maturity Levels ของระบบ System Security Engineering-Capability Maturity Model(SSE-CMM) ดังต่อไปนี้
-Performed Informally
-Planned and Tracked
-Well-defined
-Quantitatively Controlled
-Continuously Improving (10 คะแนน)

5. Vulnerability
5.1จงอธิบายสี่ขั้นตอนต่อไปนี้ของ Flaw Hypothesis Methodology
-Information Gathering
-Flaw Hypothesis
-Flaw Testing
-Flaw Generalization
(10 คะแนน)
5.2 เขียน Diagram แสดง NRL Taxonomy : Flaw by Genesis โดยแสดงเฉพาะในส่วนที่เป็นแบบ Intentional (10 คะแนน)

6.ในระบบAuditing
6.1อธิบายองค์ประกอบของ Auditing System
-Logger
-Analyzer
-Notifier (5 คะแนน)
6.2 จงอธิบายการทำงานของ State-based auditing mechanism และ Transition-based auditing mechanism (10 คะแนน)
6.3 จงเปรียบเทียบข้อดีข้อเสียของการทำงานของ Audit Browsing Techniques ดังต่อไปนี้
-Relational database browsing
-Replay
-Graphing
-Slicing (10 คะแนน)
6.4 จงอธิบายการทำงานของ สองรูปแบบของ Pseudonymizing sanitizer (5 คะแนน)