

มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

การสอบไล่ปลายภาคการศึกษาที่ 2

ประจำปีการศึกษา 2547

วันที่ 2 มีนาคม 2548

เวลา 09.00 – 12.00 น.

วิชา 240-526 Computer and Information Security ห้องสอบ A201

ไม่อนุญาตให้นำเอกสารเข้าในห้องสอบ

ทฤษฎีในการสอบ

โทษขั้นต่ำ ปรับตกในวิชานี้ และ พักการเรียน 1 ภาคการศึกษา

โทษสูงสุด ให้ออก

1. ในระบบชีวมาตร

1.1. เปรียบเทียบการทำงานของ ระบบชีวมาตรที่ทำงานเป็นแบบ Identification system และ Verification system ว่าแตกต่างกันอย่างไร (3 คะแนน)

1.2 เปรียบเทียบการทำงานของ การประยุกต์ใช้งานระบบชีวมาตรแบบ positive recognition และ negative recognition พร้อมยกตัวอย่าง (3 คะแนน)

1.3 จงอธิบายการประยุกต์ใช้งานระบบชีวมาตร ในลักษณะแบบ cooperative และ non-cooperative และการประยุกต์ใช้งานในลักษณะแบบ covert และ overt (4 คะแนน)

1.4 จงอธิบายคุณสมบัติสำคัญเจ็ดข้อ เพื่อช่วยในการเลือก ระบบ ชิวมาตร ที่จะนำไปใช้ (4 คะแนน)

1.5 จุดอ่อนสามข้อในการใช้ ดีเอ็นเอ เป็นระบบ ชิวมาตร (3 คะแนน)

1.6 จงอธิบาย คุณลักษณะของระบบชีวมาตร ต่อไปนี้ (3 คะแนน)

-Failure To Capture (FTC) rate

-Failure To Enroll (FTE) rate

-Failure To Match (FTM) rate

2. ระบบลายพิมพ์นิ้วมือ

2.1 อธิบายโดยสรุปถึง เทคนิคทั้งสามวิธีใน การทำ matching สำหรับระบบลายพิมพ์นิ้วมือ คือ

-correlation-based matching

-minutiae-based matching

-ridge feature-based matching (3 คะแนน)

2.2 จงอธิบาย ลักษณะ fraud ที่มีลักษณะ สี่อย่างคือ repudiation, coercion, contamination, และ circumventionว่า เกี่ยวข้องกับ การ รักษา Integrity ของ

fingerprint recognition อย่างไร และมีประเด็นเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย (security issues) อะไรบ้าง (4 คะแนน)

2.3ยกตัวอย่างการใช้ fingerprint recognition ในการประยุกต์ใช้งานทั้งสามด้าน คือ การประยุกต์ใช้ด้าน Forensic , ด้าน Government และด้าน Commercial (3 คะแนน)

3 ในระบบตรวจจับผู้บุกรุก(Intrusion detection system)

3.1จงอธิบายเปรียบเทียบการทำงานและ ข้อดีและข้อเสีย ระหว่าง misuse detection and anomaly detection.(6 คะแนน)

3.2.อธิบาย การจำแนกวิธีการทำงานของ Intrusion detection systems ตามแหล่งที่มาของข้อมูล (4 คะแนน)

4 สำหรับความเสี่ยงและ Business security pattern

4.1จงอธิบายหารูปแบบความเสี่ยงที่เกิดขึ้นกับองค์กรธุรกิจ (Risks to the Institution) ของระบบ Business security patterns ดังต่อไปนี้ asset risk, identity risk, infrastructure risk, custodial risk, และ compliance risk. (4 คะแนน)

4.2.ทางเลือกของการจัดการความเสี่ยง(risk management options),มีอะไรบ้าง (4 คะแนน)

4.3ความคุกคาม(major threats) สำหรับ Business to consumer business security pattern คืออะไรบ้าง (4 คะแนน)

4.4 มาตรการป้องกัน(countermeasures) และการลดความเสี่ยง ใน Business-to-Business security pattern มีอะไรบ้าง (4 คะแนน)

4.5 คุณลักษณะพิเศษของ High assurance system มีอะไรบ้าง (4 คะแนน)

5 Securing workstations และ network servers.

5.1 อธิบาย recommended password policy for securing workstations, ในส่วนที่เกี่ยวกับ length, complexity, aging, reuse, and authority (4 คะแนน)

5.2. จงอธิบาย สิ่งประเด็นหลักในการที่จะทำให้ network servers มีความ secure (3 คะแนน)

5.3.ในระบบที่มี network logging เราใช้ประโยชน์จากข้อมูลใน log file เพื่อทำอะไรบ้าง (3 คะแนน)

6 Denial of services attack

6.1Denial of services attack คืออะไร (4 คะแนน)

6.2 attacks ต่อไปนี้เกิดขึ้นได้อย่างไรและวิธีแก้ไขโดยสังเขปอย่างไร (8 คะแนน)

-Smurf network flooding

-TCP SYN flood

-UDP flood attack

-Distributed Denial of Service (DDoS) attack