

มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์

ข้อสอบปลายภาค ภาคการศึกษาที่ 1 :

ปีการศึกษา : 2549

วันที่ : 4 ตุลาคม 2549

เวลา 9.00 - 12.00

ห้อง วิศวกรรม

รายวิชา : 240 – 425 ความปลอดภัยของคอมพิวเตอร์และสารสนเทศ (Computer and Information Security)

คำสั่ง:

- ข้อสอบทั้งหมดมี 6 ข้อใหญ่ (รวมทั้งหมด 100 คะแนน) ทำทุกข้อ
- เวลาในการทำข้อสอบทั้งสิ้นรวม 3 ชั่วโมง
- ไม่อนุญาตให้นำเอกสารหรือสิ่งพิมพ์ใดๆ เข้าห้องสอบ
- ไม่อนุญาตให้ใช้เครื่องคำนวณ หรืออุปกรณ์อื่นใด ประกอบการทำข้อสอบ

Answer can be in either Thai or English.

1 From a paper “SecureComm 2005: Implications of Unlicensed Mobile Access (UMA) for GSM security” (20 marks)

1.1 Explain the UMA solution for security as shown in Figure 1.1

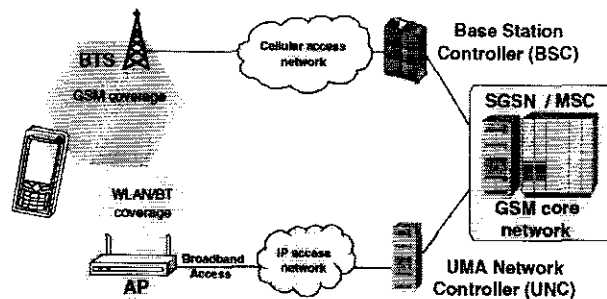


Figure 1.1

1.2. Explain UMA security mechanisms as shown in Figure 1.2

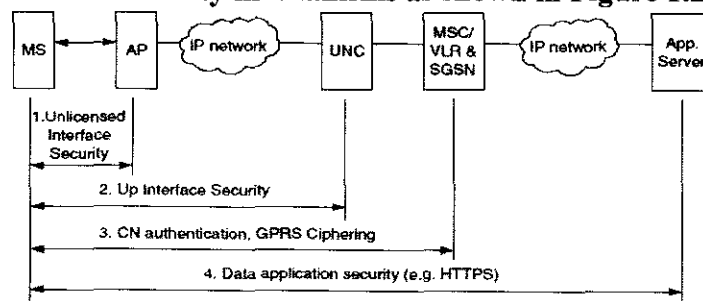


Figure 1.2

1.3 Explain that a Trojan horse in the victim's PC can access the phone and SIM card over Bluetooth as shown in Figure 1.3

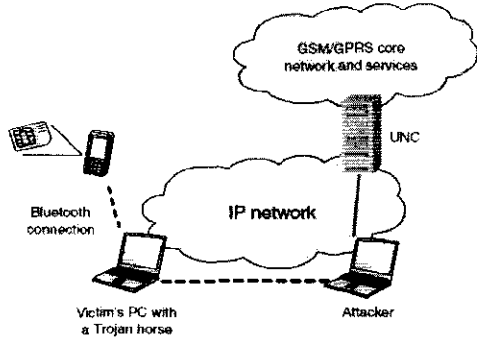


Figure 1.3

2 (16 marks)

2.1 From a paper "SecureComm 2005: Spread-Identity mechanisms for DOS resilience and Security" explain Denial of Service (DOS) attack resilient architecture as shown in Figure 2.1

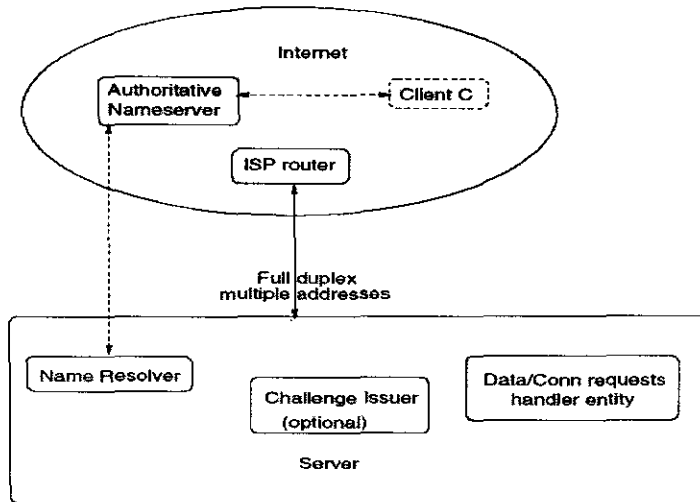


Figure 2.1

2.2. From a paper SecureComm 2005: "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems", explain NFCIP devices vs. Smartcards Devices as shown in Figure 2.2

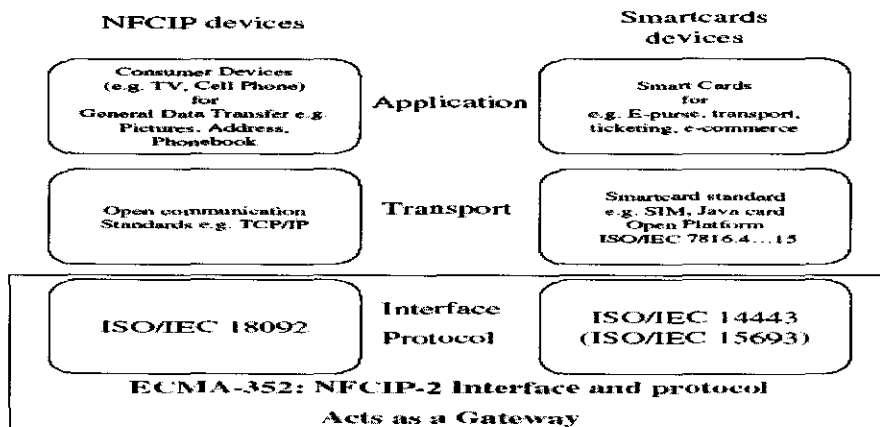


Figure 2.2

3. (16 marks)

3.1 From a paper "SecureComm 2005: Improving Cross-domain Authentication over Wireless Local Area Networks Authentication architecture as shown in Figure 3.1

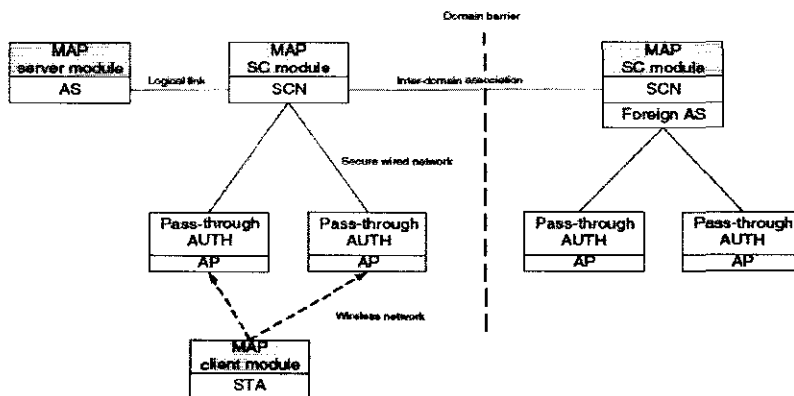


Figure 3.1

3.2 From a paper "SecureComm 2005A Signal Fingerprinting Paradigm for General Physical Layer and Sensor Network Security and Assurance explain a system-level view of the a Signal Fingerprinting Paradigm as shown in Figure 3.2

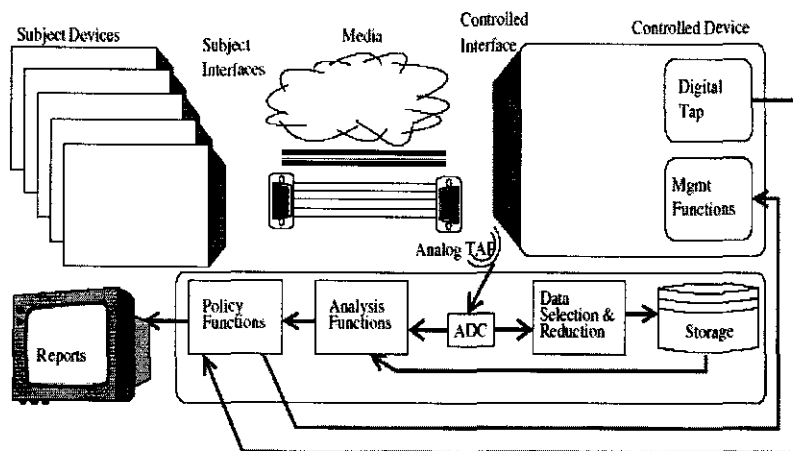


Figure 3.2

4 (16 marks)

4.1 From a paper "SecureComm 2005" A Solution for Wireless Privacy and Payments based on E-cash" explain WLAN Authentication using EAP-E-Coin as shown in Figure 4.1

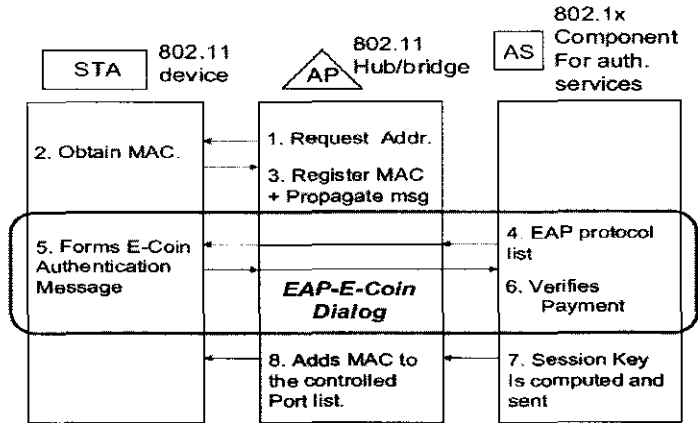


Figure 4.1

5 (16 marks)

5.1 From a paper "SecureComm 2005: An RFID Distance Bounding Protocol" explain the challenge-response scheme used in the distance-bounding protocol as shown in Figure 5.1

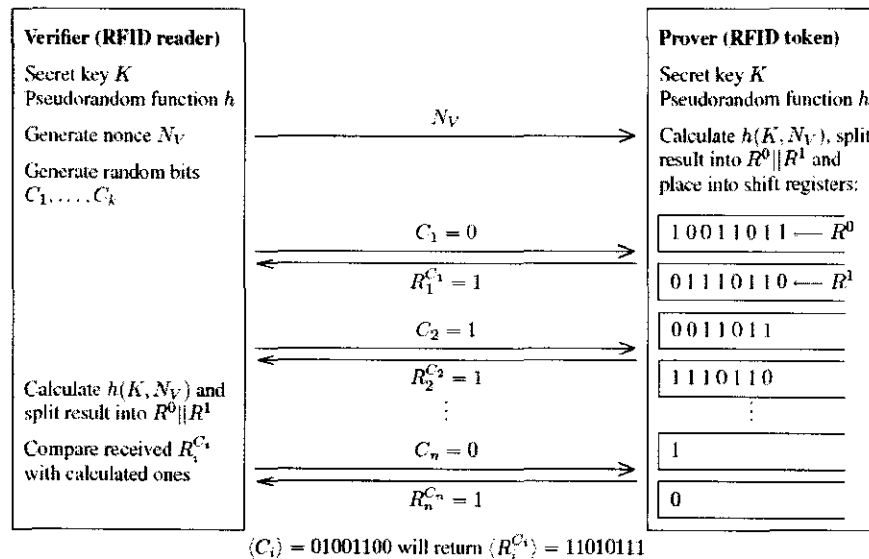


Figure 5.1

5.2 From a paper "SecureComm 2005: Towards a Location-Aware Role-Based Access Control Model" explain the Relationship of RBAC entities with Location as shown in Figure 5.2

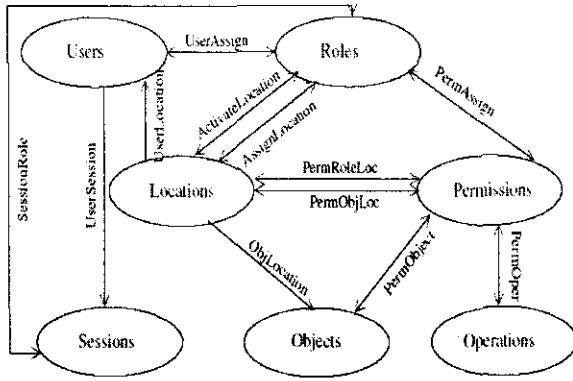


Figure 5.2

6 (16 marks)

6.1 From a paper “SecureComm 2005A Privacy Service for Context-aware Mobile Computing” explain the Context Privacy Service (CoPS) Architecture as shown in Figure 6.1

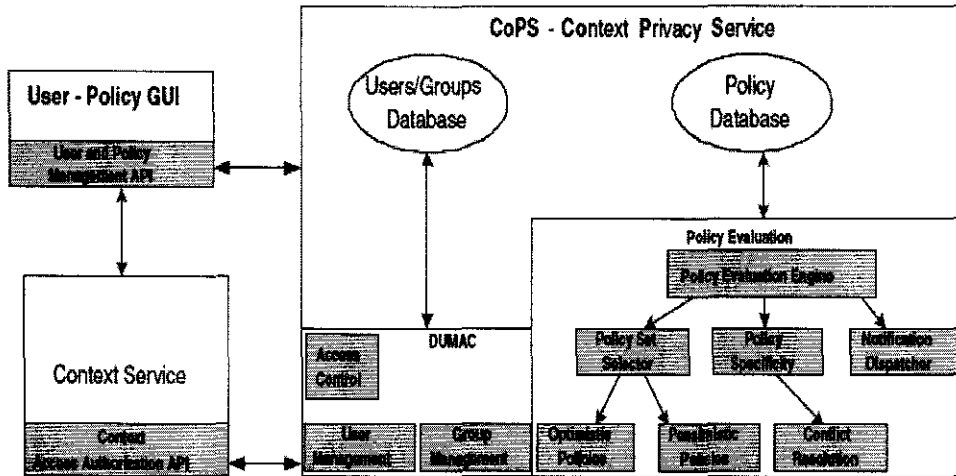


Figure 6.1