มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์

ข้อสอบกลางภาค ภาคการศึกษาที่ 1 : ปีการศึกษา : 2549

วันที่ : 1 สิงหาคม เวลา : 09.00 – 12.00 ห้อง : A201

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

คำสั่ง:

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

ข้อ 1 (15 คะแนน)

1Data Forensics(16 marks)

1.1.Describe sanitization problem in Data Forensics for hard disks

1.2.Describe 5 levels of a sanitization taxonomy.

2Mitigating Wireless Network Design Flaw (16 marks)

2.1 describe WEP data encryption and encapsulation in Figure 2.1.

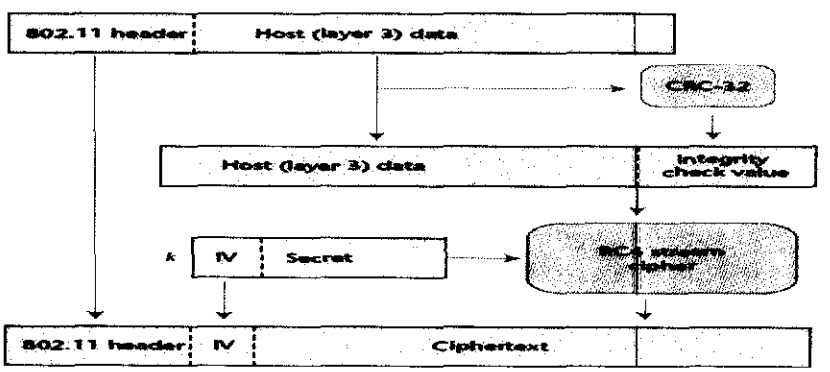

Figure 2.1.

2.2 Explain IEEE 802.11 WiFi wired equivalent privacy(WEP) protocol design flaws

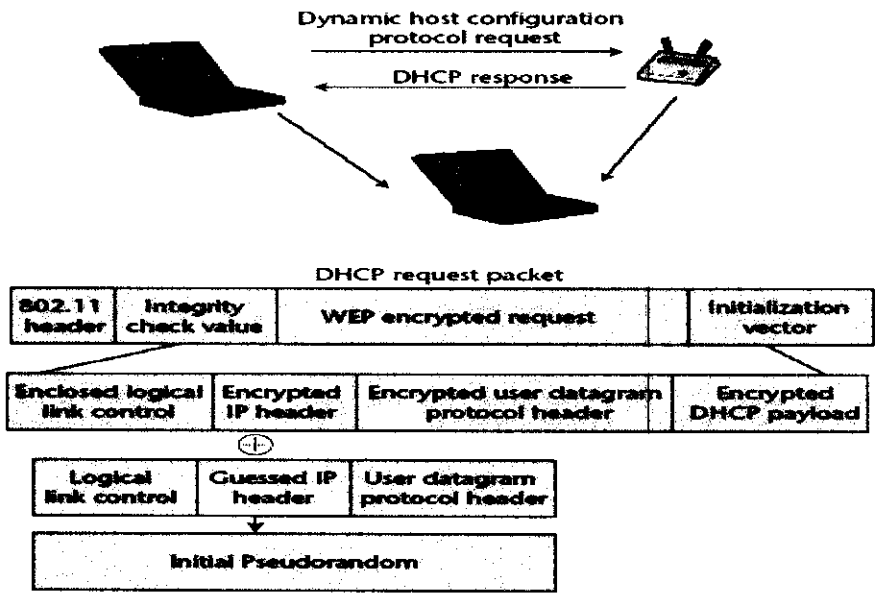

Figure 2.2

2.3Describe Recovery of an initial pseudorandom stream from a dynamic host configuration protocol (DHCP) request in Figure 2.2 ..

3 Describe the vicious circle Cybercrime in figure 3(16 marks)

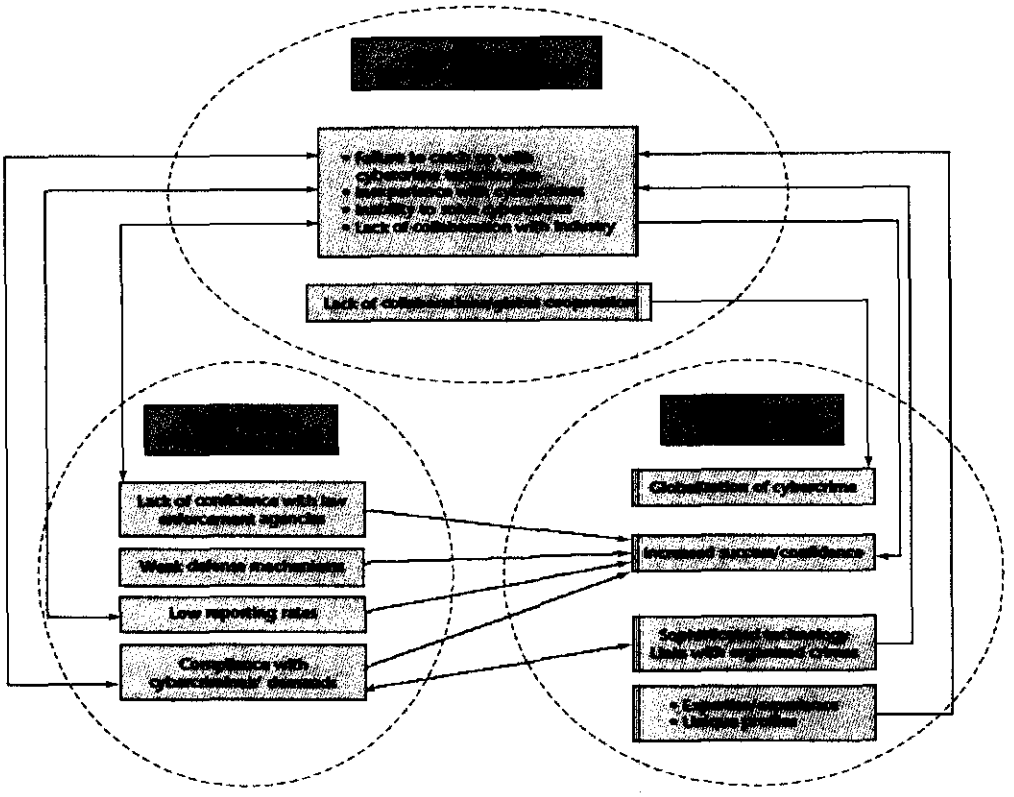

Figure 3.1. The vicious circle of cybercrimes. The proposed framework outlines how the characteristics of cybercriminals, law enforcement agencies, and cybercrime victims shape the cybercrime landscape.

4 Secure Authentication (20 marks)

4.1Describe Offline credential-stealing attack scenarios. User credentials are attacked via interception on the client PC or by tricking the user into revealing them to a fake server in Figure 4.1..

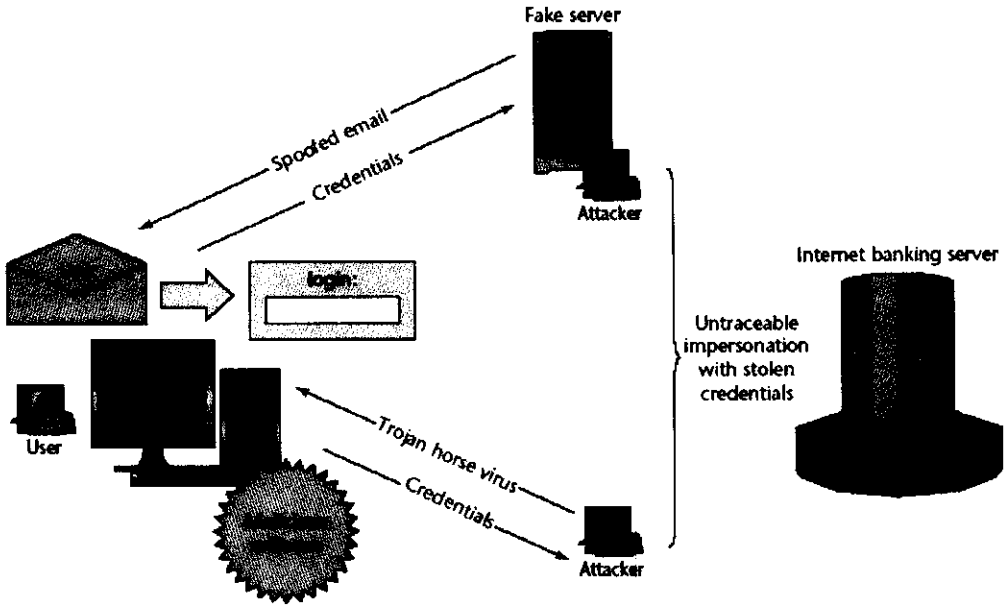

Figure 4.1..

4.2 Describe Online channel-breaking attack scenarios. Session credentials (such as session cookies) are attacked via interception as they move between the client PC and the banking server in Figure 4.2..

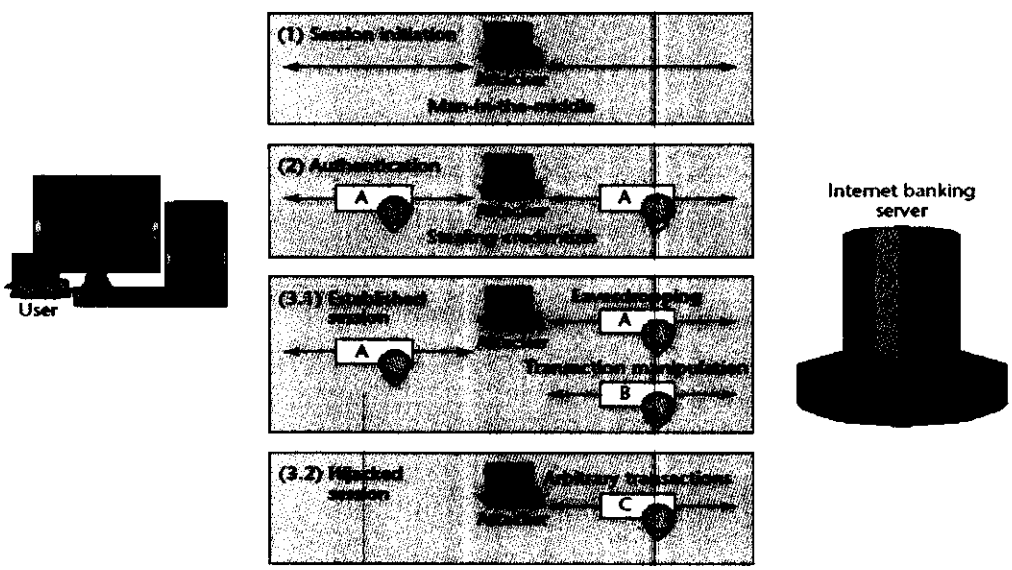

Figure 4.2

4.3.Describe Taxonomy of Internet banking authentication methods. Methods are classified according to their resistance against offline credential-stealing and online channel-breaking attacks in Figure 4.3..

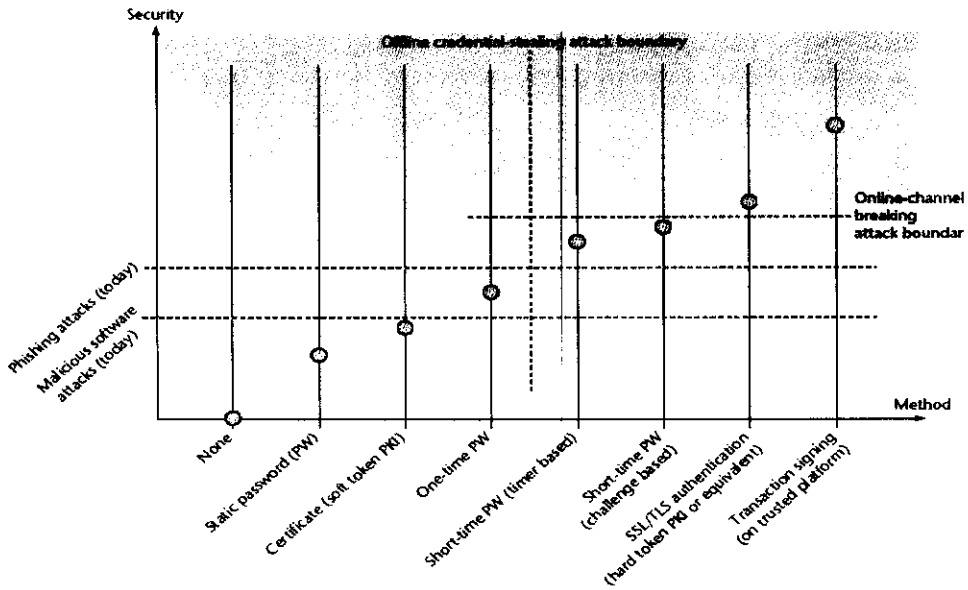

Figure 4.3

4.4 Describe the short-time password solution. This authentication scheme uses an offline card reader and a smart card to produce short-lived passwords on demand in Figure 4.4.

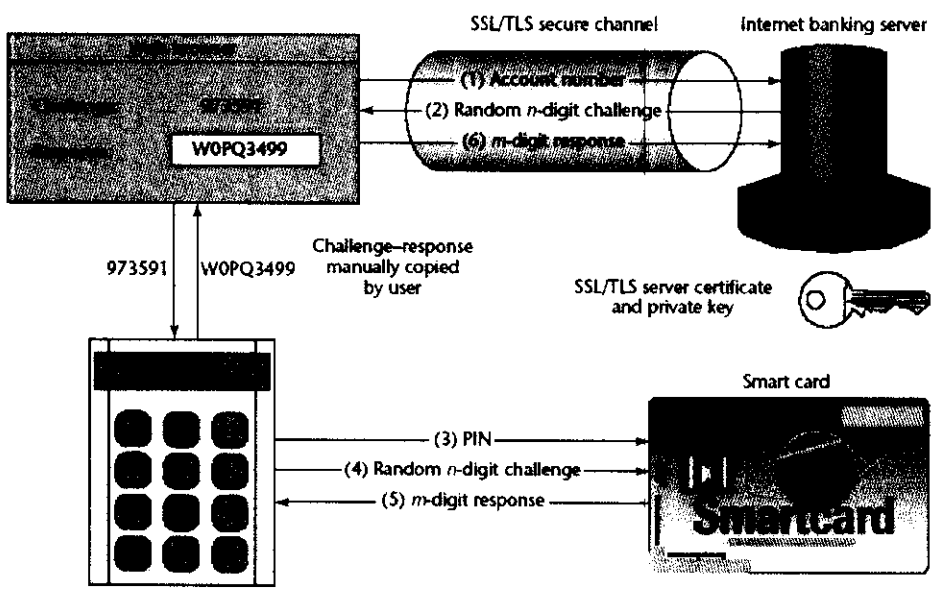

Figure 4.4

4.5 Describe the certificate-based solution. This authentication scheme uses a secure online card reader, the FINREAD card reader, and a smart card to sign SSL/TLS challenges on demand shown in Figure 4.5.

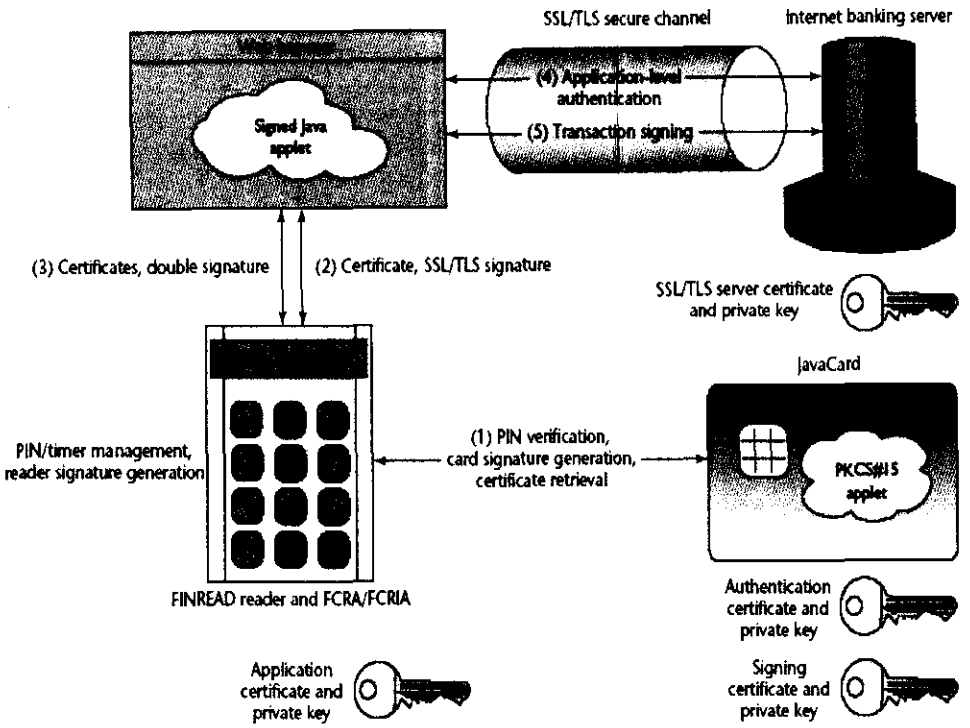

Figure 4.5

5A contextual framework for combating identity theft(16 marks)

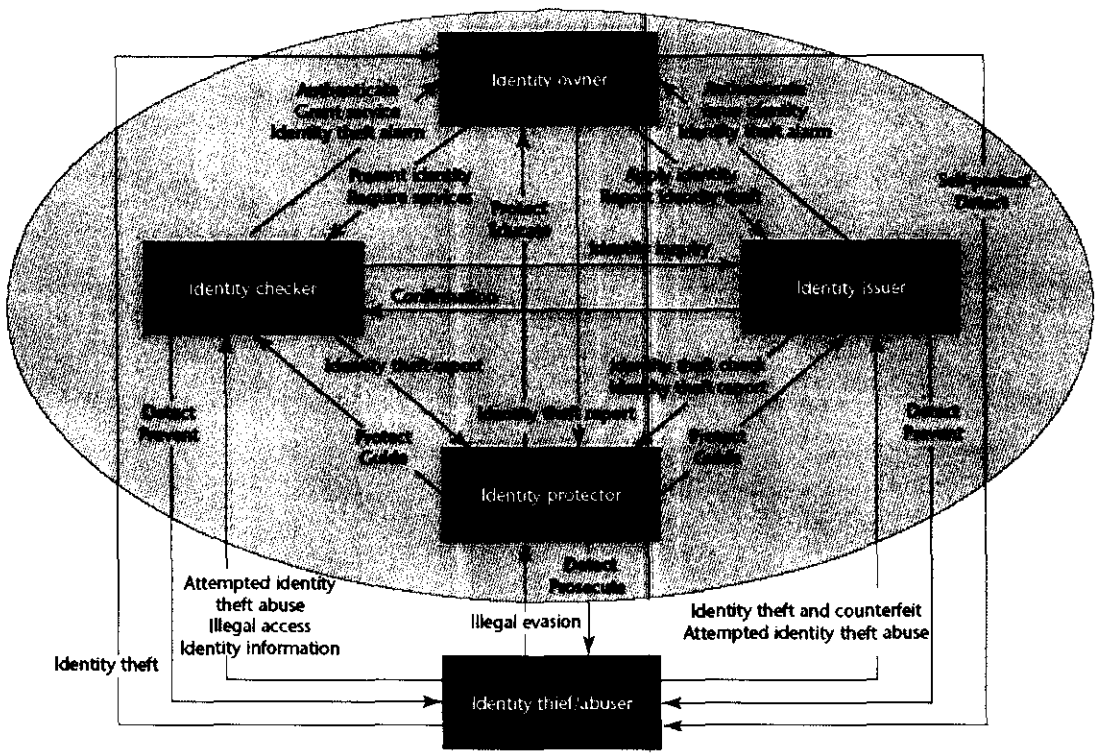

Figure 5.1..

5.1 Describe The contextual framework for combating identity theft. In the graph, nodes represent the major stakeholders, and arrows indicate their interactions and information flows. Red lines indicate the activities taken by identity thieves/abusers. Green arrows indicate activities by other stakeholders in Figure 5.1..

5.2 Describe Identity theft Prevention technologies.

6 Securing Embedded Systems(16 marks)

6.1 Explain Embedded security pyramid as per figure 6.1

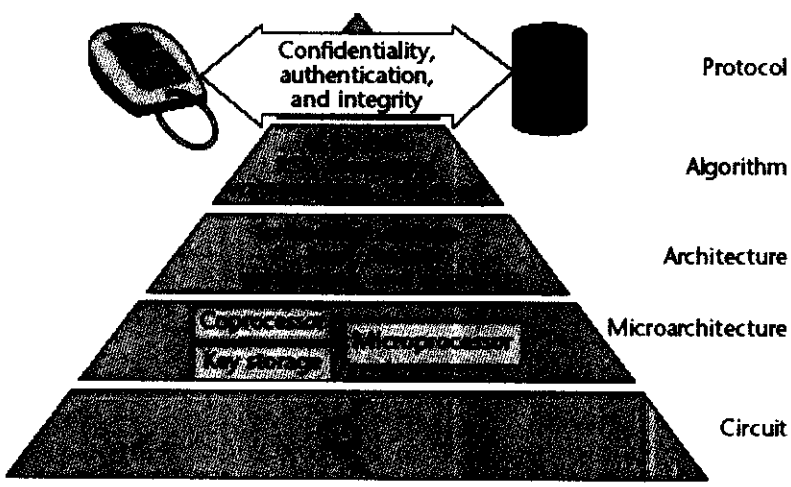

Figure 6.1. Embedded security pyramid. To ensure security in an embedded system, we must address the problem in all abstraction layers.

6.2Describe Biometric authentication. (a) In a server-based fingerprint authentication scheme, the server matches a user's fingerprint with a previously stored template. (b) In a device-based scheme, a user authenticates directly with the embedded device as in Figure 6.2.

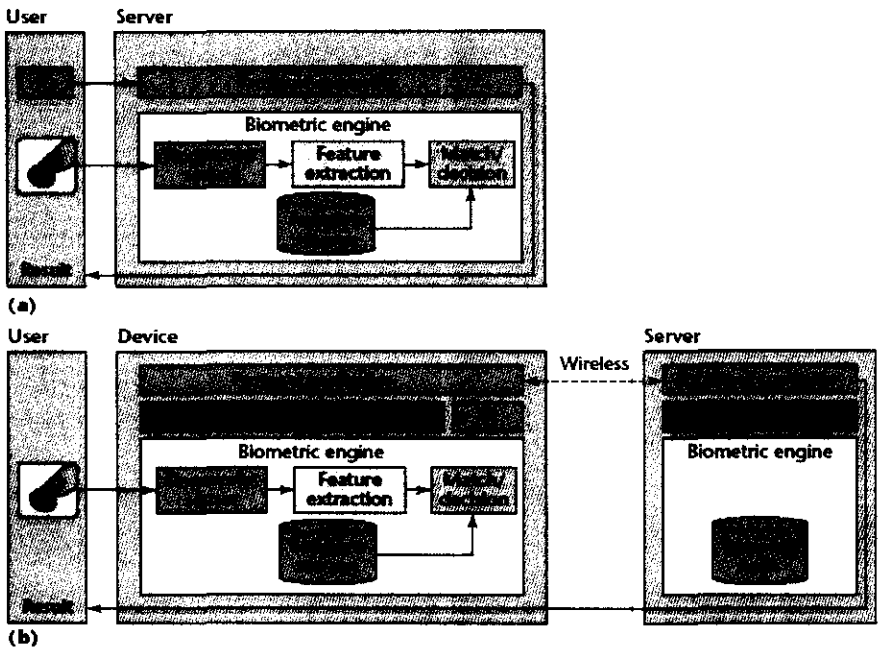

Figure 6.2

6.2Describe Biometric authentication. (a) In a server-based fingerprint authentication scheme, the server matches a user's fingerprint with a previously stored template. (b) In a device-based scheme, a user authenticates directly with the embedded device as in Figure 6.2.