มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

การสอบไล่กลางภาคการศึกษาที่ 2 **ประจำปีการศึกษา 2546**

วันที่ 27 ธันวาคม 2546 **เวลา 13.30- 16.30น**

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

ให้ตอบคำถามทุกข้อ แต่ละข้อคะแนนเท่ากัน

ไม่อนุญาตให้นำเอกสารเข้าในห้องสอบ

1 Intrusion Detection

1.1For Intrusion detection compare advantages and disadvantages of the two strategies, namely, misuse detection and anomaly detection.

1.2.For misuse detection strategy, explain the following approaches:

-Expert System

-Signature Analysis

1.3.For Anomaly detection strategy, explain the following approaches

-Statistical analysis

-Data Mining

1.4.Explain how Machine-Learning Methods are used with degree of attack guilt to detect novel attacks while maintaining sufficiently low numbers of false alarms.

2. Explain the following :

-Public-key cryptography

-Secret-key cryptography

-Advantages and disadvantages of public-key cryptography compared with secret-key cryptography

-A hash function

-Message Authentication Codes

-Digital signature

-Authentication

-A digital envelope

3 Cryptanalysis;

3.1 Describe the attacks on symmetric block ciphers namely,

-differential cryptanalysis,

-linear cryptanalysis,
-the exploitation of weak keys,

3.2 Explain following basic types of cryptanalytic attack based on the kind of information the cryptanalyst has available to mount an attack.

-A ciphertext-only attack
-A known-plaintext attack
-An adaptive-chosen-plaintext attack
-An adaptive-chosen-ciphertext

4 Explain the following:

4.1 What is primality testing?
4.2 How is the RSA algorithm used for authentication and digital signatures in practice?
4.3 What is DES?
4.4 What is triple-DES?
4.5 What are DSA and DSS?
4.6Explain the 6 stages of the life cycle of a key?

5. PUBLIC-KEY

5.1 What is a PKI?
5.2 What happens if one's private key is compromised?
5.3 What are certificates? How are they used?
5.4What are Certificate Revocation Lists (CRLs)?
5.5 Describe different fields of ITU's X.509 certificate

6 Explain the following Electronic money related systems:

6.1 electronic money
6.2 Internet Keyed Payments Protocol (iKP)
6.3 SET
6.4 Mondex
6.5 micropayments

7.What are the following Public-Key Cryptography Standards (PKCS) used for:?

-PKCS #1
-PKCS #3
-PKCS #7
-PKCS #8
-PKCS #9
-PKCS #10

-PKCS #11
-PKCS #12

8. Answer the following:
8.1Describe activities of following IETF Security Area working groups :
-PKIX Public-Key Infrastructure (X.509),
-IPSec IP Security Protocol,
-S/MIME
-TLS Transport Layer Security,
8.2 What is Clipper chip ?
8.3 What is Optimal Asymmetric Encryption Padding (OAEP)
8.4 What is digital timestamping?
8.5 How are hardware devices made tamper-resistant?

9 Computer Security Problems

9.1 Explain vulnerabilities ,and threats to information security in computer systems
9.2.Explain Four broad areas of Computer Misuse.
-Theft of computational resources
-Disruption of computational services
-Unauthorized disclosure of information in a computer
-Unauthorized modification of information in a computer

9.3Explain characteristics of 4 types of Trojan horses
-Virus,
-time bombs,
-logic bombs,
- worms.

10 Explain following Classes of information oriented Misuses
-User abuse of authority
-Direct Probing
-Probing with malicious Software
-Direct Penetration
-Subversion of Security Mechanism