มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

การสอบไล่ปลายภาคการศึกษาที่ 1 **ประจำปีการศึกษา 2547**

วันที่ 4 ตุลาคม 2547 **เวลา 9.00-12.00 น**

วิชา 240-425 Information Systems Security **ห้องสอบ R201**

ไม่อนุญาตให้นำเอกสารเข้าในห้องสอบ

Answer all questions, each of the 6 questions carries equal marks.

1.From the literature given in class "Linking security needs to e-business evolution"

1.1For the following State of e-business adoption , describe each state and its Security and privacy requirements:

-Publish
-Transact
-Internal integration; Refining core business processes
-External integration; Crossing enterprise boundaries
-The digital economy; Intelligent, collaborative coexistence

1.2 Explain how comprehensive planning, security and threat assessment strategies

The following strategies for planning IT security and privacy can aid in establishing an effective set of policies and procedures.

-Create a security and privacy blueprint
-Actively check security and privacy controls
-Use available security products rather than those developed in house
-Provide security training
-Track information, assets and users

- Inventory management
- Configuration control
- Problem reporting.
- Supply and asset management.
- User control.
- System documentation.

2. From the literature given in class "Ethical hacking"

2.1 explain the following questions:

What is ethical hacking?

Who are ethical hackers?

What do ethical hackers do?

What are three basic questions that ethical hacker's evaluation of a system's security seeks to answer?

2.2.Explain the following methods and combinations that may be used for ethical hacking:

-Remote network
-Remote dial-up network
-Local network
-Stolen laptop computer
-Social engineering
-Physical entry

3. From the literature given in class "Business Security Patterns"
3.1Explain the following types of Risk Management Options
in which businesses can manage these risks:
3.1.1Risks to the Institution;

-Asset Risk
-Identity Risk
-Infrastructure Risk
-Custodial Risk
-Compliance Risk

3.1.2 Risk Management Options

-Transfer
-Indemnify
-Mitigate
-Avoid
-Accept

3.2 Security Patterns
The five major business security patterns are:
3.2.1Web Presence;

-Isolated from core business
-Integrated with core business

3.2.2Business to Consumer

-Store Front
-Subscription-Based Services
-Purpose Optimized Devices
-Employee-to-Business

3.2.3Business to Business;

-Simple Supplier
-Trusted Supplier
-Partnership

3.2.4Operational Security;

-Users
-Decentralized, or "branch office", infrastructure
-Data Centers
-Communications
-Manufacturing

3.2.5 High Assurance;

-Enclave Environment
-Bounded Environment
-Unbounded Environment

3.3 Explain the eight major attributes of a particular business security pattern highlight the countermeasures that a business could take to reduce risk to an acceptable level:

-Who
-Access Point
-Access Method
-Access Portal
-Collateral Access
-Data Value
-Privacy
-Business Value

4. From the literature given in class "A method for designing secure solutions"

4.1 Explain Common Criteria Functional Class for the following Functional Categories

-Audit Audit
-Access control
-Flow control
-Identity/credentials
-Solution integrity

4.2.Explain the seven security design objectives:

- A need to control access to computer systems and their processes
-A need to control access to information
-A need to control the flow of information
-A need to manage the reliability and integrity of components
-A need for protections from malicious attack
-A need for trusted identity to address the requirement of accountability of access to systems
-A need to prevent fraud within business processes and transactions

4.3 Explain integrating security requirements into component architectures;

-Mandate
-Best practice for security
-Component capability
-Location in the configuration
-Impact
-Necessity

5. From the given literature given in class "Enhancing security and privacy in biometrics-based authentication systems"

5.1Eight places in the generic biometric system where attacks may occur.

- Presenting fake biometrics at the sensor
- Resubmitting previously stored digitized biometrics signals

- Overriding the feature extraction process
- Tampering with the biometric feature representation
- Corrupting the matcher
- Tampering with stored templates
- Attacking the channel between the stored templates and the matcher
- Overriding the final decision

5.2 What are the following two methods used for?

-WSQ-based data hiding

-Image-based challenge/response method

6. From the given literature given in class "Securing e-business applications using smart cards"

6.1.Explain examples of new secure Web applications projects;

-The db-markets eTrade Project.

-The e-Safe Project.

6.2Explain functions of Smart-card-based security in details:

-Authentication.

-Authentication using smart cards without public key cryptography.

-Authentication using public key smart cards.

-Digital signature using smart cards.

6.3Explain Common smart card types.

-Simple file-system smart card.

-File-system card with public key cryptography.

-Java Card.

-Windows for Smart Card.

-MULTOS smart card.

6.4Explain "The OpenCard Framework(OCF)