UNIVERSITY EXAMINATIONS: 2013/2014

EXAMINATION FOR THE MASTER OF SCIENCE IN DATA COMMUNICATIONS

MDC 6302 SECURING INFORMATION SYSTEMS

DATE: AUGUST, 2014 **TIME: 2 HOURS**

INSTRUCTIONS: Answer Question One and Any Other Two Questions

QUESTION ONE: [20 Marks]

a) Briefly describe any TWO characteristics that make networks vulnerable to attacks. (4 Marks)

b) Briefly explain the two classifications of computer software program faults. (4 Marks)

c) Briefly describe the two circumstances under which a user can experience authentication failure. (4 Marks)

d) Explain why AES encryption and decryption should be performed on hardware instead of software? (4 Marks)

e) Some governments require that every citizen provide their biometric data and DNA samples. Explain the threat that such requirements pose to the citizens? (2 Marks)

f) State any way by which "Time of Check to Time of Use" errors in software programs can be prevented? (2Marks)

QUESTION TWO [15 MARKS]

Kirinyaga Auto Parts Company produces multiple automobile parts for various destinations in East Africa. These include parts for the car industry, boat industry and bike industry. Recently they have decided to improve their production efficiency by installing a system that enables tracking of the production from the raw material to the final product. Tracking takes place as follows:

(i) When a new item is put into production, a bag with the raw material needed to produce it is composed and a new TAG is created and attached to it.

(ii) At each step of the production an employee takes the product to process it. He logs into the system and registers when it starts and finishes working on the item (inserting the TAG in the system).

(iii) At the final step when the item is complete, the item is registered in the system as finalized.

The system relies on a wireless infrastructure. TAGs are read by wireless devices and multiple terminals (connected to the central system by wireless) are placed around the production site.

Refer to the above scenario to answer the following questions:

a) The company has to decide between Bar Code and RFID technology based TAGs for the bags produced. As a system security expert, advise the company management on what type of TAG to use. (2 Marks)

b) Advise the company on the method they should use to identify each employee. (2 Marks)

c) Discuss the protocols that would be suitable for the design of the network within the production chain and which security level it should have. (4 Marks)

d) The CEO of Kirinyaga Auto Parts wants to be able to remotely check the status of the production. In particular he wants to be able to monitor where, in the production chain, a particular item is, and to track employees in order to find out who is working on what. Specify how the system should be set up to allow him remote access, focusing on making the connection secure, based on the knowledge you have gained throughout the course. (7 Marks)

QUESTION THREE [15 MARKS]

a) Describe the relationship between a Substitution Cipher and a Product Cipher. (5 Marks)

b) Explain how WEP violates the “fundamental rule” of cryptography. (5 Marks)

c) Describe a man-in-the-middle attack and explain how one can be launched against a wireless network (5 Marks)

QUESTION FOUR [15 MARKS]

a) Describe two ways in which a denial of service (DoS) attack can be launched against a WLAN. (4 Marks)

b) What is a wireless security policy and why is it important? (5 Marks)

c) You have been contacted by Charlie, CEO of the small financial company Cash-Cache AG, for help on a digital forensics case. Charlie recently noticed strange behavior from their main competitor, and is now convinced that this competitor had access to some of their confidential data and is using it against them. Charles owns the company and would be at direct personal loss if the company was to fail; you safely exclude the possibility that he mounted a tortuous scheme himself to frame a coworker. Charles identified five suspects among his employees:

- Penny, Charles' associate and company co-founder, has recently become unhappy with the way things are managed. Charles suspects her of wanting to leave and rejoin their main rival. She has access to all customer files.
- Miranda, Penny's administrative assistant. The two women are very close and Miranda would probably follow Penny if the former left for a position at their main competitor. Younger and careless, Miranda may be willing to take bigger risks to enhance her prospective career paths.
- Terence, the network administrator, manages the network equipments (switches and routers). Terence is a passionate poker player, and regular denizen of the local casino. From what he's willing to admit, he's been particularly unlucky lately.
- Jeff, the web developer, has access to the company web server, develops the web site and some specific intranet applications. After a painful divorce, Jeff recently remarried to a young woman with expensive tastes, and it is certainly not whith his lowly web developer pay that he could afford all the jewelry and designer clothes.
- Leo, former employee of Charles, was dismissed from the company last month, after Charles busted him conducting a batch of barely legal transactions; the two men had a violent argument over business ethics. Leo left extremely unhappy and was not secretive about it; he definitely has a good motive to seek revenge against his former employer.

Charles is very paranoid about information security; without his coworkers know, he entered a contract with Occulus, a security solutions provider, who installed network probes at a few key locations. These probes are black boxes remotely managed by Occulus, and completely transparent. Because his coworkers are not aware of any network monitoring, it is unlikely that they went through complex hiding schemes to transfer the blame to other people. Given the logs, identify the nature of the breach by answering the following Questions.

(i) What kind of confidential data was stolen? (2 Marks)

□ Business address book (prospective customers identities)

□ Financial records

□ Confidential product specifications

□ Passwords database

□ HR data (salaries, bonuses...)

(ii) Describe 2 methods/characteristics that apply to the attack. (2 Marks)

□ Cross-site request forgery (CSRF)

□ DNS Hijacking

□ Distributed Denial of Service

□ Malicious insider (direct only, not indirectly)

□ Man-in-the-Middle

□ SQL Injection

□ Social engineering

□ Trojan Horse

(iii) Who is the most likely culprit? Give a reason for your choice. (2 Marks)

□ Penny, the co-founder

□ Miranda, the assistant

□ Terence, the network admin

□ Jeff, the web developer

□ Leo, the disgruntled trader