NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF APPLIED SCIENCE
COMPUTER SCIENCE DEPARTMENT
DECEMBER EXAMINATIONS 2004

SUBJECT: COMPUTER SECURITY
CODE: SCS 4107

Instructions to candidate:

Answer any four questions.

3 HOURS

QUESTION ONE

a) Describe the following modes of operation of a block cipher: message authentication code and hash function [5]

b) Controls for providing computer security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Explain and describe each of these controls. [10]

c) "Why should I bother with doing risk assessment?!" "I already know what the risks are!" "I' ve got enough to worry about already!" "It hasn' t happened yet ..." Most resistance to risk assessment boils down to one of three conditions: Ignorance, Arrogance, and Fear. Discuss?? [10]

QUESTION TWO

a) By first defining each of the following, differentiate amongst them,

i) Risk analysis

ii) Risk management

iii) Risk assessment [5]

b) Suppose that we are using a Vigen`ere-style encryption scheme with an alphabet of 27 characters, A-Z plus a space. Recall that the key for such a cipher is a repeating word which represents right-rotations in the alphabet.

i.) Consider the plaintext:

TO TRAVEL HOPEFULLY IS BETTER THAN TO ARRIVE

Show the encrypted version of this text using the 3-letter key BUS.

ii.) Consider the 42-letter ciphertext:

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS find the 42-letter key that yields the plaintext:

MR MUSTARD WITH THE CANDLESTICK IN THE HALL

iii.) Considering the same ciphertext again, find the 42-letter key that yields the plaintext:

MISS SCARLET WITH THE KNIFE IN THE LIBRARY

What does this result and the previous one tell you about the security of this cipher? Give a careful explanation.

iv.) How can this cipher be broken when used with a short key length? [12]

c) Type enforcement is a security mechanism that can be used as the basic security building block for a large number of systems in which security is an important factor. Give a detailed explanation of the type enforcement mechanism. [8]

QUESTION THREE

a) The traditional purpose of information security is deliver confidentiality, integrity, accountability and availability. Explain each of these concepts. [5]

b) What vulnerabilities where poised by the Server Message Block Protocol (SMB) on systems running on the Microsoft Platform? What potential damage could a hacker do on systems running this protocol, before a Microsoft released a fix for it? [10]

c) There are two types of DOS attacks: flaw-based and flooding. By first defining what DOS is, explain these two types of DOS attacks and also explain how you would counter each of these attacks? [10]

QUESTION FOUR

a) In terms of computer security define the following

i. Non-repudiation.

ii. Firewall Ruleset.

iii. UDP protocol

iv. Information asset

v. Message Authentication code [5]

b) Give a detailed description of the security features that are in place for unix based operating systems [10]

c) Part of the security features of Microsoft Windows 2000 server is the use of Secure Sockets Layer (SSL) protocol – which provides an encrypted channel for authentication. The SSL protocol uses a combination of public-key and symmetric key encryption. Symmetric key encryption is much faster than public-key encryption, but public-key encryption provides better authentication techniques. Give a detailed description of SSL and how SSL works. [10]

QUESTION FIVE

a)

i. Explain the difference between discretionary and mandatory access control

ii. Define the following: Trapdoor One way function [5]

b) By first giving an overview of the Microsoft Windows 2000 operating system architecture (with the aid of a diagram where necessary), give a detail account of the MS Windows security subsystem. [10]

c) A firewall policy dictates how the firewall should handle applications traffic such as web, email, or telnet. The policy should describe how the firewall is to be managed and updated. Most firewall platforms utilize rulesets as their mechanism for implementing security controls. The contents of these rulesets determine the actual functionality of a firewall. Depending on the firewall platform architecture, firewall rulesets can contain various pieces of information. By first stating the steps required to develop a firewall policy, give a detailed account of how you would implement a firewall ruleset. [10]

END OF QUESTION PAPER

GOOD LUCK!