JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DOCTORATE OF PHILOSOPHY IN IT SECURITY AND AUDIT

1STYEAR 1STSEMESTER 2018/2019 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: IIT6113

COURSE TITLE: EMERGING ISSUES IN CYBER SECURITY
EXAM VENUE: STREAM:

DATE: EXAM SESSION:

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other three questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE 20 MARKS

The university, like many others in the USA, requires students to own their own computers. The infrastructure on-campus consists of a high-speed network, with access points in most classrooms and residence halls. Thus, unlike businesses which have a large degree of control over the computers attached to their networks, and the software installed on these, the University faces unique security challenges. Moreover, these machines are being used in learning environments, where students are free (and encouraged) to use their resources as they see fit in their studies, and in their personal lives. Thus the balancing act between freedom and security is not easy.

Your brief

Identify the issues the University faces in securely integrating student-owned computers. Make recommendations as to the policy it should adopt.

The following are given as a starting point for this – draw upon your own experiences of university life, reading, etc.

i. Communicating University policy and federal/state laws
ii. Training students in security awareness
iii. Privacy
iv. Restricting access to resources
v. Monitoring resources, imposing sanctions for misdemeanours
vi. Internet and email security
vii. Network design (esp. domain questions)
viii. Incident response

This question is based on a paper by Kerry Vosswinkel (no longer available) from the SANS Institute, Information Security Reading Room, September 2001

(20 marks)

QUESTION TWO 20 MARKS

Strathallen is an independent insurance brokers, a member of the British Insurance Brokers Association (BIBA) and the Institute of Insurance Brokers (IIB). They will find a policy to cover just about anything; car, home, travel and marine policies make up much of their business, but they also find cover for pets, horses, events depending on good weather, etc.They promise to find the insurance policy that best suits their clients' requirements, at the best price. To do this, they sell no policies of their own, but search the marketplace to find the right product. This mostly involves on-line access to specialist (non-public) web-based systems which provide policy information from many policy-writers, but they also have their own in-house decision support systems, developed for them by a third party software house.

They operate from modern offices on an industrial estate on the outskirts of Dudley in the West Midlands. The 60 full-time and 80 part-time staff work 2 shifts (7.00am to 3.00pm, and 3.00pm to 10.00pm Monday to Friday, and one shift (10.00am to 6.00pm) on Saturday. The company interacts with customers by telephone or through its web-site (operated by a third party ISP). This includes taking payment by credit/debit card over the internet or on the phone.The company has a network of PCs and servers in the office, with a state-of-the-art telephone facility supporting both tele-workers and internet applications. They also maintain customer records on their system, to allow them to track annual renewals, commissions, etc. They also send and receive in excess of 120,000 emails per month.They do not employ any IT staff, and rely on their hardware and software suppliers for technical support.

Required

Conduct a threat assessment of the information provision at Strathallen. Make any reasonable assumptions you feel are necessary, and make a note of things about which you would like to know more. Based on your assessment, make tentative recommendations as to how they might respond to these threats.

(20 marks)

QUESTION THREE 20 MARKS

a) Explain how asymmetric encryption (or public key encryption) can be used to secure communications over the internet, what benefits there may be, but also noting any technical or organizational weaknesses.

(10 marks)

b) Discuss how asymmetric encryption may be enhanced, in order to engender greater confidence in business communications.

(10 marks)

QUESTION FOUR 20 MARKS

a) A software house specializing in financial systems, with over 1,000 customers in the U.K. and Europe, intends to send system components to these customers via the Internet, to save time, money and administrative efforts. You have been asked to advise them on the security implications of this, identifying the issues you feel are important, and how you would address these.

(12 marks)

b) Discuss the relative strengths and weaknesses of symmetric and asymmetric encryption, commenting on their commercial value to e-commerce

(8 marks)

QUESTION FIVE 20 MARKS

Northern Ordinance, a major defence contractor in the UK, has a large research and manufacturing facility on the outskirts of Sheffield, with several office blocks, a factory and other storage buildings standing on 20 acres. They have a 3 metre fence surrounding the site, permanent security staff watching CCTV cameras placed around the perimeter, and a manned security position at the main gate, which logs staff, visitors and vehicles entering and leaving the site.

(a) Identify ways in which the physical security of the company's site could be improved, given the highly sensitive nature of its business, and the need to convince the Government that information vital to the national interest is safe.

(8 marks)

(b) Discuss what the company should do to protect its electronic information from unauthorized access by visitors to the facility.

(8 marks)

(c) What measures might the company take to minimize the risks of disaffected staff compromising information security?

(4 marks)