TECHNOLOGICAL UNIVERSITY DUBLIN

KEVIN STREET CAMPUS

BSc. (Honours) Degree in Computer Science (Infrastructure)

Year 3

SEMESTER 2 SUPPLEMENTAL OPEN BOOK EXAMINATIONS 2019/20

Security / Systems Security

Bojan Božić

Duration 9hrs

Exam script available 9am on date of the exam.
All exams submissions should be uploaded before 6pm on the date of the exam

Answer **ALL** questions.

Question 1 carries 40 marks. Questions 2 and 3 carry 30 marks each.

1. (a) Which of the following activities might be considered a possible source of threat to a company's network, and why? (Give a **detailed reason.**)

(i) The daily courier service personnel who drop off and pick up packages.

(ii) Former employees who left the company because of downsizing.

(iii) An employee traveling on company business to another city.

(iv) The building management company where an organization has its offices has decided to install a fire sprinkler system.

(8 marks)

(b) Consider the following login protocol.

user knows password P

user knows Hash function H(.) and has a mobile calculator

user gives login name N to machine

machine generates random number R

machine gives R to user

user computes X := Hash(P) XOR Hash(R)

user gives X to machine

machine uses N to obtain P from password table

machine computes Y := Hash(P) XOR Hash(R)

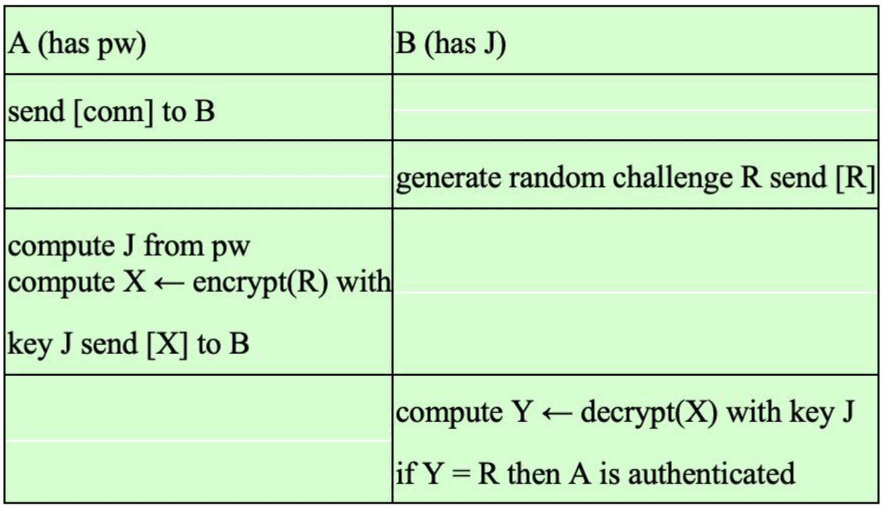
if X=Y then machine allows login

b1. Explain what is wrong with it and how it can be broken.

b2. Show a simple way to strengthen this protocol against your attack.

(12 marks)

(c) In the authentication protocol below, pw is A's password and J is a key derived from pw. Can an attacker that can eavesdrop messages (but not intercept or spoof messages) obtain pw by off-line password guessing? If you answer no, **explain** in detail. If you answer yes, **describe** the attack.



A (has pw)	B (has J)
send [conn] to B	
	generate random challenge R send [R]
compute J from pw compute X ← encrypt(R) with key J send [X] to B	
	compute Y ← decrypt(X) with key J if Y = R then A is authenticated

(20 marks)

2 (a) Consider an Intrusion Detection System with a False Positive Rate of 0.001 and a False Negative Rate of 0.09.

i. If there are 100,000,000 legitimate transactions (connections) a day, how many false alarms will occur?

ii. If there are 1000 hacking attempts (connections) per day, how many true alarms will be given?

iii. How many hacking attempts will go unnoticed?

(8 marks)

(b) **Describe in detail** how viruses can be categorised based on how they attack. **Explain** each type in detail. **Give** at least 5 **examples**.

(11 marks)

(c) **Discuss** the 5 steps to conduct successful penetration testing and ethical hacking projects. Use a **diagram** to help **illustrate** your answer. Give one concrete example to explain your diagram.

(11 marks)

3. (a) Assuming you can do 2^{20} encryptions per second and the key size is 40 bits, how long would a brute force attack take? **Give a scenario** where this would be practical and **another** where it wouldn't. What happens if you double the key size?

(10 marks)

(b) Assume that we have scenario A where a company requests users to authenticate before using a secure channel, and scenario B where a classified document needs to be sent via email. State whether each of the scenarios are using **Symmetric** or **Asymmetric** Key Encryption Methods. What are the advantages and disadvantages in either scenario and why are they used for the specific scenario? Give at least two more examples for each type of encryption.

(10 marks)

(c) You have been tasked with introducing a new security policy in your company. The new policy allows employees to use laptops and other mobile devices at home, when travelling and on the company network. **Discuss in detail** how this policy can be safely rolled out without endangering the company network.

(10 marks)