TECHNOLOGICAL UNIVERSITY DUBLIN

KEVIN STREET CAMPUS

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

Year 3

SEMESTER 2 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.

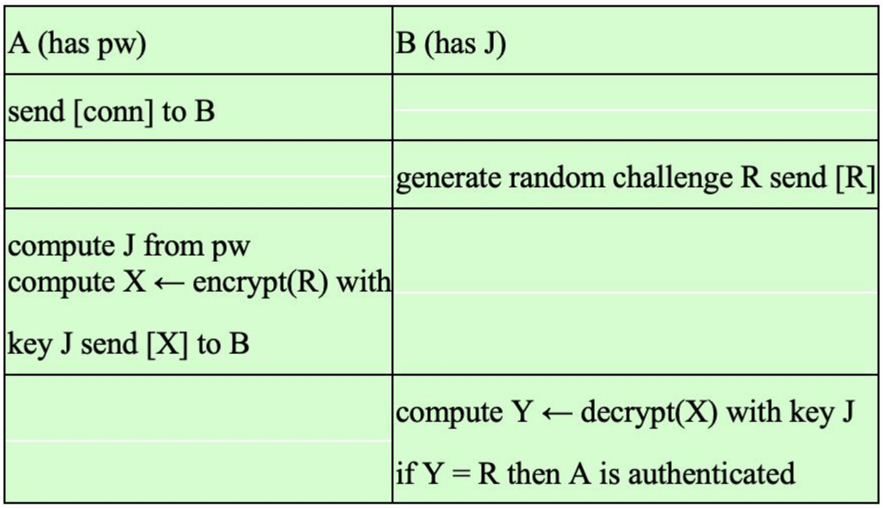
(iv) The building management company where an organization has its offices has decided to install a fire sprinkler system.

(8 marks)

(b) Consider an application that requires an encryption and MAC algorithm be implemented on a processor with a small amount of non-volatile memory. The only cryptographic algorithm that the processor can compute is Triple-DES. But you have space for one 168-bit key. Describe how it is possible to both encrypt and MAC using only a single key. **Justify** your answer and **state any assumptions** you use.

(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) You’ve been asked to protect a site with a firewall. There are no inbound services. The only outbound service is Web browsing, which of course requires some form of DNS name resolution. There is a lot of concern about people going to improper sites; there is also a desire to filter all web content to remove active content. **Describe in detail** the best firewall configuration for this site. **Justify** the purpose of each element.

(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)