CANDIDATE: please attach Student Support Unit sticker, if relevant

**THE UNIVERSITY OF SUSSEX**

**FOUNDATION YEAR EXAMINATION**
**BSc and MComp FIRST/SECOND/THIRD/FINAL EXAMINATION**
**MComp FINAL YEAR EXAMINATION**
**MSc EXAMINATION**

**Introduction to Computer Security G6077**

You can start this exam at a time of your choosing within a 24 hour window. Once started you will have a set exam duration in which to complete it (note: the assessment will close at end of the 24 hour window; start with sufficient time to complete).

If you have extra time due to Reasonable Adjustments this is additional to the exam duration below and has been added to your assessment on Canvas.

Date 2022
24 Hour Window starts at: 09:30
Exam Duration: 3 hours (including time for scanning, collating, uploading)

**Candidates should answer TWO questions out of THREE.**
**If all three questions are attempted only the first two answers will be marked.**
**Each question is worth 50 marks.**

**Write or type your answers on A4 paper, scan and save as a single PDF file and upload to Canvas.**

**Please make sure that your submission includes the following:**

**Your candidate number (Do not put your name on your paper)**
**The title of the module and the module code.**

Read Academic Integrity Statement
You MAY access online materials, notes etc. during this examination. You must complete this assessment on your own and in your own words. DO NOT discuss this assessment with others before the end of its 24 hour window. By submitting this assessment you confirm that your assessment includes no instances of academic misconduct, for example plagiarism or collusion. Any instance of academic misconduct will be thoroughly investigated in accordance with our academic misconduct regulations.

1. (a) For each of the following terms, provide a brief description of the term relates to the security of a web application for a company's customers:
   i. Confidentiality [4 marks]
   ii. Integrity [4 marks]
   iii. Availability [4 marks]
   iv. Authenticity [4 marks]
   v. Accountability [4 marks]

   (b) You have been hired by AcmeWidget Ltd to secure the web interface to a legacy system, backed by a database management system using SQL. This system is complex, its source code has been lost, and you have been unable to find a precise definition of allowable input values. You have been asked to write input validation procedures, that will identify values which are suspected to be malicious, and flag them for later manual inspection. For each of these input fields, explain one validation procedure you could perform, and justify why it is appropriate:
   i. the name of a file in a particular directory on the server; [7 marks]
   ii. a parameter that you believe will be used in an SQL statement [7 marks]
   iii. a string that will be loaded into memory and parsed as English text [7 marks]

   (c) For one of the validation procedures you gave above, discuss how a sophisticated attacker could circumvent detection. [9 marks]

2. (a) What is Public Key Cryptography? [15 marks]

   (b) Transport Layer Security (TLS) provides session security for connections over the Internet.

      i. Describe how the TLS handshake protocol can be used to deliver a secure session key for symmetric encryption using TLS' record protocol. [15 marks]

      ii. Why isn't public key encryption used to encrypt the entire session? [5 marks]

      iii. If an organised criminal group (ocg) stole the private key for the web server at `www.sussex.ac.uk`, describe one possible attack that the ocg could execute, and how the Sussex system administrators should respond to the attack. [15 marks]

3. (a) From the lectures, recall that the *Wannacry* malware was a *worm* that encrypted the hard drive of computers, and then executed a *Ransomware* attack on the computer owner.

   i. Describe the operation of a *worm* [5 marks]

   ii. What is a *Ransomware* attack? [5 marks]

   iii. Using your understanding of the legal framework for computer security in the UK, what laws could be used to prosecute the people behind the Wannacry worm? [15 marks]

   (b) AcmeDesign Ltd is a small web company with nine employees. Each employee works from their company owned laptop from their home, and all the company's working files are stored using the cloud services provided by Microsoft. You have been tasked with undertaking the design of a security policy and implementation for the company.

   i. Outline how you would approach the design of a security policy and its implementation. [10 marks]

   ii. Identify five assets that are likely held by the company, and provide a security risk analysis for two risks against each of the five assets. [15 marks]



*End of Paper*