

# NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

FINAL YEAR (SOFTWARE ENGINEERING)

FALL SEMESTER EXAMINATION 2020

BATCH 2017

Time: 3 Hours

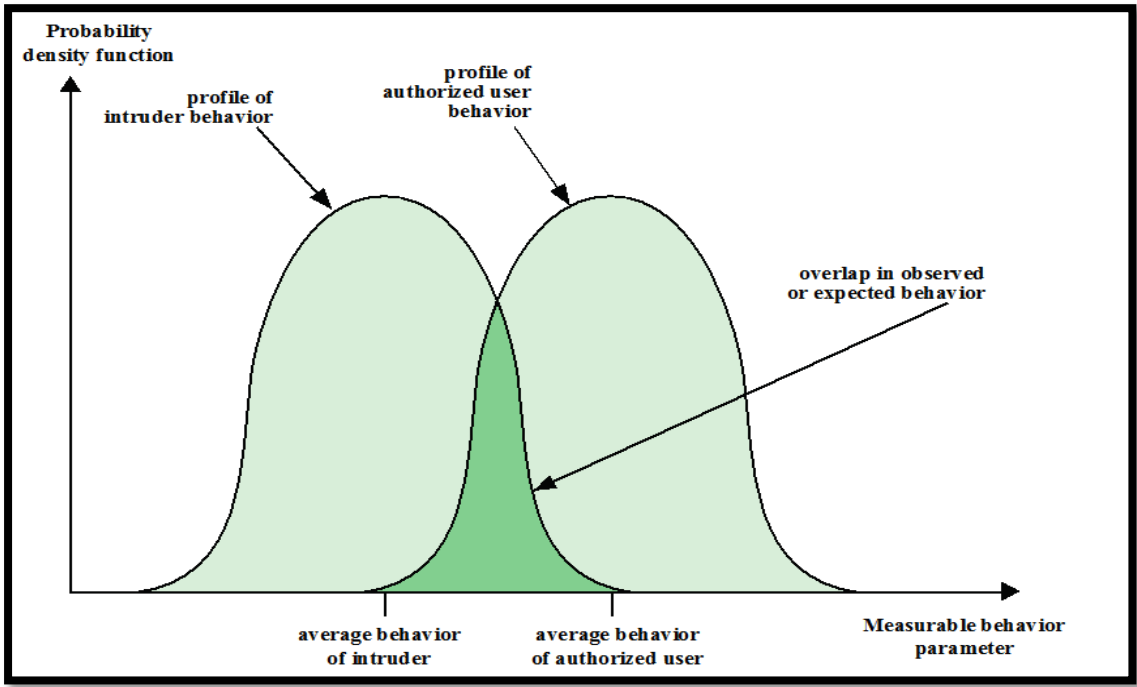
Dated: 13-02-2021

Max Marks: 60

## Network & Information Security (CT-460)

### Instructions:

- Attempt ALL questions.
- Make neat and clean diagrams where necessary.
- Questions can be attempted in any order but all parts of a question must be attempted together.

<b>Q1</b> (a)	Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. <b>EXPLAIN</b> the examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement. [CLO-1]	[6]
(b)	Consider the following diagram and <b>DISCUSS</b> the profiles of the behavior of Intruders and Authorized users [CLO-1] <div style="text-align: center; margin-top: 20px;">  </div>	[6]
<b>Q2</b> (a)	Download the digital certificate from the website <a href="https://www.facebook.com">https://www.facebook.com</a> . <b>EXPLAIN</b> the important components of this digital certificate with respect to the domain of facebook.com [CLO-1]	[6]
(b)	<b>DESCRIBE</b> Malware classification mechanism with the help of examples. [CLO-1]	[6]
<b>Q3</b> (a)	A university is conducting online classes and examinations. The university has 5000 students appearing in the final exam in 100 different virtual classrooms concurrently. <b>DETERMINE</b> how you will design a security policy for such an organization to prevent and mitigate DDoS attacks. [CLO-2]	[6]
(b)	You are given the following “Informal Firewall Policy” details to be implemented	[6]

# NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

FINAL YEAR (SOFTWARE ENGINEERING)

FALL SEMESTER EXAMINATION 2020

BATCH 2017

	<ol style="list-style-type: none"> <li>1. Users inside may retrieve their e-mail from the DMZ mail gateway, using either POP3 or POP3S, and authenticate themselves.</li> <li>2. DNS lookup requests by internal users are allowed via the DMZ DNS server, which queries to the Internet</li> <li>3. Web requests (both insecure and secure) are allowed from any internal user out through the firewall but must be relayed via the DMZ Web proxy.</li> <li>4. Web requests (both insecure and secure) are allowed from anywhere on the Internet to the DMZ Web server.</li> <li>5. External DNS requests are provided by the DMZ DNS server.</li> <li>6. E-mail may be sent using SMTP in both directions through the firewall, but it must be relayed via the DMZ mail gateway. External e-mail must be destined for the DMZ mail server.</li> </ol> <p><b>APPLY</b> suitable packet filter rule sets to be implemented on the “External Firewall” and the “Internal Firewall” to satisfy the afore-mentioned policy requirements. [CLO-2].</p>	
<b>Q4</b>	Alice wants to send the message “4” to Bob using RSA Algorithm. Given, $p=13$ , $q=17$ .	[6]
(a)	<b>CALCULATE</b> the Public, Private Key, Cipher Text, and Decrypt the Cipher Text to recover the original message i.e., “4”. [CLO-2]	
(b)	<p>Suppose you receive a letter from a finance company stating that your loan payments are in arrears, and that action is required to correct this. However, as far as you know, you have never applied for, or received, a loan from this company! <b>DETERMINE</b> the following [CLO-2]</p> <ul style="list-style-type: none"> <li>• What may have occurred that led to this loan being created?</li> <li>• What type of malware, and on which computer systems, might have provided the necessary information to an attacker that enabled them to successfully obtain this loan?</li> <li>• How such malware can be prevented?</li> </ul>	[6]
<b>Q5</b>	An organization decides to secure its network using Firewall. As a security consultant, you have been assigned the task to develop and implement an Access Policy for the organization. The organization has different network devices (Routers, Switches, etc.), Servers like Web, Email, DNS, etc., and end-users. Organization requires that its Web and Email Services will be available to the outside world. Internal users of the organization can access the internet except Twitter and Facebook. Assume that the internal organization network consists of 210.120.0.0/16 subnet. <b>EXAMINE</b> this situation and write Access Policy as a pseudo code. Also, draw the diagram of your proposed solution indicating <b>DMZ</b> and <b>Distributed Firewall</b> location. [CLO-2]	[6]
(b)	Assume that one of the largest enterprises has been hit by a <b>Metamorphic worm</b> which is a class of Malware. You have assigned the task to mitigate the attack in order to minimize the current damage. The other task assigned is to propose a plan in order to protect the organization from such attacks in the future. <b>APPLY</b> Metamorphic worm countermeasures approach based upon the malware protection recommendations. [CLO-2].	[6]