STRATHMORE UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY
MASTER OF SCIENCE IN INFORMATION SYSTEMS SECURITY
END OF SEMESTER EXAMINATION
MST 8505 - SPECIAL TOPICS IN NETWORK SECURITY AND SYSTEMS SECURITY

DATE: 16 April, 2018 **Time: 2 Hours**

Instructions

- This examination consists of **FIVE** questions.
- Maximal points for the examination is **50**.

1. What is a flow from point of view of network monitoring? What statistics can be collected about the flow? Propose at least four techniques that can be used to analyse Netflow data. For each technique give at least one example of application for security monitoring. (**12 points**)

2. What sources of event logging do you know? Name at least four different log sources. For each of the source, give an example of events and logging data. Explain how the data can be used for network management using FCAPS functions. (**8 points**)

3. Compare SNMP and event logging from point of view monitoring data. Discuss benefits and drawbacks of each of the system used for practical security monitoring. (**12 points**)

4. Describe typical architecture of IoT network (topology). What devices and communication protocols are part of the architecture? Which monitoring protocols are typically used for home IoT networks and for industrial IoT networks? (**8 points**)

5. Describe ANS.1 language and different types of ASN.1 syntaxes. How are described objects using ASN.1? Name common ASN.1 data types that are used for network monitoring in SNMP system. **(10 points)**