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 System Security

DATE:16 October, 2017 Time: 1 Hour

Instructions: This examination consists of FIVE questions; Answer all questions.

QUESTION ONE

Define what is an IP flow a give an example of the flow. Describe main building blocks of NetFlow system with a short explanation of the functionality. Explain following techniques for advanced data processing: filtering, sampling, and aggregation. Demonstrate on the example how these technique can be implemented in NetFlow system. (**12 points**)

QUESTION TWO

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**)

QUESTION THREE

Define four essential parts of typical network management system. Explain basic functions of each part. Demonstrate how such system can be implemented using SNMP monitoring. (**12 points**)

QUESTION FOUR

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? (**6 points**)

QUESTION FIVE

Describe at least four MIB-2 object groups, two RMON-1 or RMON-2 groups. For each group give at least two objects that can be used for network monitoring. (**12 points**)