Sharad Dixit

CMSC 487 Introduction to Network Security

**Assignment 3**

* **OBJECTIVE**

The objective of this assignment is to analyze protocols for flaws and then verify their correctness properties using Cryptographic Protocol Shapes Analyzer(CPSA). We analyze two protocols Blanchet and Kerberos with CPSA and then verify their correctness.

* **METHODOLOGY**

The CPSA tool analyze the protocol and verify their correctness by providing output shapes to analyze. Shapes provided are either unrealized and realized in which the realized shapes are the final output of a skeleton of a defined protocol, therefore in order to check and verify a protocol the realized shapes are analyzed.

Further, In the realized shape nodes may be blue, red or black where a black node represents transmission and blue, red represents receptions. Also, a blue node represents an explainable reception and whereas a red node represents an unexplainable reception.

Arrows in the shapes represents ordering of events in the skeleton, where a solid arrow represents the same message getting received which was send from the transmission point. The dashed arrow represents that the message received and transmitted do not agree.

Note: Throughout the document I have represented the screenshots of the analyzes of both protocols respectively that is first Blanchet and second Kerberos. The screenshots are aligned in such a way that the first screenshot represents the original protocol and the below it represents the screenshot for the corrected in protocol.

* **ANALYSIS**

The analysis of both the protocols is done using CPSA tool and the flaws are found in the protocol and are rectified. On each page the first screenshot belong to the original protocol and the second screenshot below it represents the corrected protocol that is after fix. The detailed explanation for each screenshot is give adjacent to it.