Internet Infrastructure Security (COMP444)

A7

Due at 11:55pm on 23 April 2015

Submission site: `https://submit.comp.polyu.edu.hk/`

Rocky K. C. Chang

April 14, 2015

1. `[6 marks]` (ESP) Owing to the fact that block encryption and cryptographic hash functions generate discrete output sizes, an IPSec packet can take on only some legitimate sizes. In this question, the block size for encryption is 256 bits (e.g., using AES-256), and the hash's output size for message authentication is 512 bits (e.g., SHA-3). Determine whether the following two packet sizes are legitimate. Note that an IP packet is always on the 4-byte boundary, and the IP header is 20 bytes long.

   (a) `[3 marks]` The IPSec packet size (including the IP header) is 146 bytes.

   (b) `[3 marks]` The IPSec packet size (including the IP header) is 440 bytes.

2. `[6 marks]` (AH) Consider an IPSec SA using AH. What is the impact on an IPSec packet of this SA if each of the following fields has been modified in transit to the destination.

   (a) (2 marks) The SPI

   (b) (2 marks) The source IP address

   (c) (2 marks) The ICV data