Isfahan University of Technology
Network Security
Dr. Manshaei
Homework 6: Module 6 & 7 (IPsec/Wireless security)
Deadline: Monday 22^{nd} Dey, at 23 : 59

We only accept the homework **delivered via Yekta (yekta.iut.ac.ir), before the deadline**. If you have any questions or concerns about this homework, feel free to contact Mr. Sepehr Shirani via Telegram: *@sepovsky* (Preferred) or email: sepishiran@gmail.com.

Q1: Specify the True/False of the following questions related to Figure 1 by stating the reason.

- When a host in 172.16.1/24 sends a datagram to an Amazon.com server, the router R1 will encrypt the datagram using IPsec.
- When a host in 172.16.1/24 sends a datagram to a host in 172.16.2/24, the router R1 will change the source and destination address of the IP datagram.
- Suppose a host in 172.16.1/24 initiates a TCP connection to a Web server in 172.16.2/24. As part of this connection, all datagrams sent by R1 will have protocol number 50 in the left-most IPv4 header field.
- Consider sending a TCP segment from a host in 172.16.1/24 to a host in 172.16.2/24. Suppose the acknowledgment for this segment gets lost, so that TCP resends the segment. Because IPsec uses sequence numbers, R1 will not resend the TCP segment.

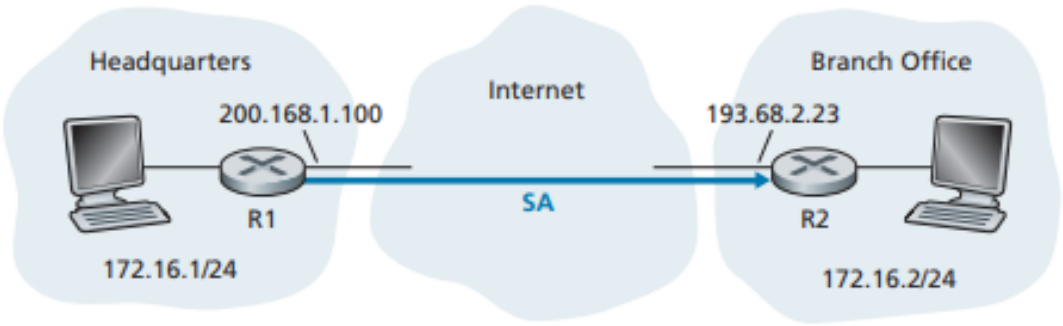

Figure 1: Security association (SA) from R1 to R2

Q2: The sequence number in the ESP header in IPsec is used to prevent replay attacks. The receiver will only accept one packet with each sequence number and reject a packet with a sequence number that has already been used. What then prevents an attacker from sending a packet with a higher sequence number to cause the original packet with this sequence number from being accepted?

Q3: What are the basic approaches to bundling SAs?

Q4: What security services does the GSM security architecture offer, and what critical security services is it lacking?

Q5: What are three main vulnerabilities associated with the WEP protocol?