SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit I- NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

Topic : IP Authentication Header

What is Authentication Header

The Authentication Header (AH) is a security protocol used within the IPsec suite. Its primary function is to ensure that the message remains unmodified during transmission from the source and it confirms that the data originates from the expected source.
Authentication Header achieves this by adding a header to IP packets, containing a checksum and a digital signature.

Its main functions are:
•**Message Integrity –** It means, the message is not modified while coming from the source.
•**Source Authentication –** It means, the source is exactly the source from whom we were expecting data.

What is Authentication Header CONT.,

When a packet is sent from source A to Destination B, it consists of data that we need to send and a header that consists of packet information. The Authentication Header verifies the origin of data and also the payload to confirm if there has been modification done in between, during transmission between source and destination. However, in transit, values of some IP header fields might change (like- Hop count, options, extension headers). So, the values of such fields cannot be protected from Authentication header. Authentication header cannot protect every field of IP header. It provides protection to fields which are essential to be protected.

Authentication Header Format

- **Next Header –** Next Header is 8-bit field that identifies type of header present after Authentication Header. In case of TCP, UDP or destination header or some other extension header it will store correspondence IP protocol number . Like, number 4 in this field will indicate IPv4, number 41 will indicate IPv6 and number 6 will indicate TCP.

- **Payload Length –** Payload length is length of Authentication header and here we use scaling factor of 4. Whatever be size of header, divide it by 4 and then subtract by 2. We are subtracting by 2 because we're not counting first 8 bytes of Authentication header, which is first two row of picture given above. It means we are not including Next Header, Payload length, Reserved and Security Parameter index in calculating payload length. Like, say if payload length is given to be X. Then (X+2)*4 will be original Authentication header length.

Authentication Header Format

- **Next Header –** Next Header is 8-bit field that identifies type of header present after Authentication Header. In case of TCP, UDP or destination header or some other extension header it will store correspondence IP protocol number . Like, number 4 in this field will indicate IPv4, number 41 will indicate IPv6 and number 6 will indicate TCP.

- **Payload Length –** Payload length is length of Authentication header and here we use scaling factor of 4. Whatever be size of header, divide it by 4 and then subtract by 2. We are subtracting by 2 because we're not counting first 8 bytes of Authentication header, which is first two row of picture given above. It means we are not including Next Header, Payload length, Reserved and Security Parameter index in calculating payload length. Like, say if payload length is given to be X. Then (X+2)*4 will be original Authentication header length.

What is IPSec

What is IPSec

What is IPSec

What is IPSec

What is IPSec

What is IPSec

What is IPSec

What is IPSec

Any Query????

Thank you……