5. IP Security

Thursday, March 4, 2021 9:53 AM

IP security can be integrated in source or destination
It maintains integrity and confidentiality

- AH: Authentication Header (used only for integrity)
- ESP: Enhanced Security Payload (used for integrity and confidentiality)

ESP+tunnel mode = VPN (virtual private network)

Router is a network device that has a physical, data link and network layer.
Using a network layer, a router can also provide IP security.
Instead of end devices, routers add IP security headers.

Using IP security:

- Access control: rather than using name/password or certificates, we can assign the responsibility to the IP layers of source and destination
- Web service/SOAP requests can use IP security rather than application level security (SSL)
- Origin authentication
- Rejection of playback attack
- Maintain confidentiality

Security Association

Security association required from

- A to B (SA1)
- B to A (SA2)

Unidirectional

What does it convey?

- By having 2 SA, we can provide bidirectional integrity and confidentiality.
- Uniquely identified by:

1. SPI: security parameter index: unique 32-bit number
2. Destination IP address:
3. AH/ESP: SA1 can have AH, SA2 can have ESP (one SA can have AH or ESP, not both)

Without IP security

IP header	DL header	Message(IP data gram)

With IP security:

IP header	AH/ESP header (IPSec header)	DL header(TCP/UDP)	Message

AH header contains fields that help us incorporate integrity of information

- **Type of next header (IP, TCP)**
- Length of the header
- Unused
- **SPI**: all packets have same SPI [for a segment from A to B]
- **Sequence number**: to avoid playback attack [sequence number cannot be repeated]
- **Authentication data**: digital signature of the header+data without IP security

Encrypt the digest (of IP header+date) with private key (authentication data)

Security Parameter Index:

- Contains digest algorithm (MD5, SHA)
- Encryption algorithm of digest for digital signature (RSA, DES)
- Source agrees to add a 32-bit number, destination uses the mentioned algorithms in the SPI to decrypt and decode the information
- B will maintain a database with digest and cryptography algorithms