Intro to Network Security

Application Encryption & VPN

Text:
Network Security: The Complete Reference, Bragg, Rhodes-Ousley, Strassberg et al.

Intranets, Extranets, and VPNs

Private Network: A network that is not freely available to the public.

Intranet: Private network that uses Internet technology. Often includes:
Web browsers & servers
May include private IP addresses, including:

10.0.0.0:		Class A Address
172.16.0.0-	172.31.255.255:	16 Contiguous Class B Addresses
192.168.0.0-	192.168.255.255:	256 Contiguous Class C Addresses

Extranet: Enables two or more companies to share common information & resources by extending the intranet
Accommodates business-to-business communication (B2B): post orders, share projects, share pricing, communicate collaboratively.
Extranets can introduce weaknesses in security.

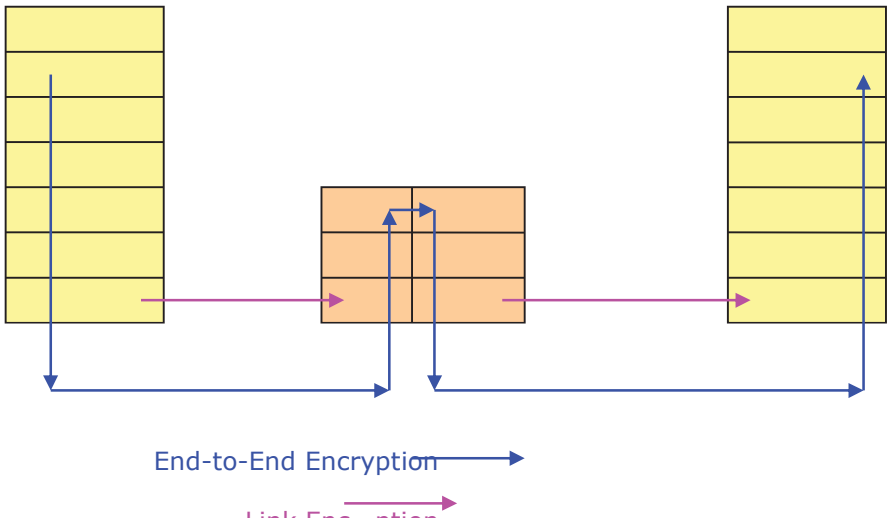
Virtual Private Network (VPN): A means of carrying private traffic over a public network
Uses link encryption to give users sense that they are operating on a private network when they are actually transmitting over a public network
Communications pass through an **encrypted tunnel**

Intranet VPN: Connects two or more private networks within the same company

Extranet VPN: Connects two or more private networks between different companies (for B2B or business-to-business communications).

Remote Access VPN: A roaming user has access to a private network via wireless, hotel room, etc.

Encryption Techniques: End-to-End vs. Link Encryption



Comparison:

	Link	End-to-End
Purpose	Link itself is vulnerable: Packet sniffers & eavesdroppers	Intermediate nodes may be compromised
Encryption coverage	Link-Specific: All packets transmitted on the single link are encrypted	Connection-Specific: A connection is encrypted across all its links
Protocol header security	Encrypted for all protocol layers (at or above layers 1 or 2)	Encrypted for upper layer protocols only
Network device exposure	Intermediate nodes decrypt	Intermediate nodes cannot decrypt
Authentication	Provides node authentication	Provides user authentication
Ease of use	Transparent to user, One key per link	Not user-transparent, One key per connection
User Selectivity of algorithm	One algorithm for all users	User selects encryption algorithm
Implementation	Encryption done in hardware	Encryption done in hardware or software
Applications	Virtual Private Network (VPN)	Secure Shell (SSH) SSL Pretty Good Privacy (PGP)