CHAPTER 16

IP Security

IP Security Overview

- The Internet Community has developed application specific security mechanisms in a number of application areas, including electronic mail (S/MIME, PGP), client/server (Kerberos), web access (Secure Socket Layer) and others.

- However users have some security concerns that cut across protocol layers. For example, an enterprise can run a secure, private TCP/IP network by disallowing links to untrusted sites, encrypting packets that leave the premises, and authenticating packets that enters the premises.

- By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but for the many security-ignorant applications.

IP Security Overview Continue…

- The IP-level security encompasses three functional areas:
  1. Authentication
  2. Confidentiality
  3. Key Management

The authentication mechanism assures that a received packet was in fact transmitted by the party identified as the source in the packet header.

The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.

The key management facility is concerned with the secure exchange of keys.

IP Security Overview Continue…

- According to CERT (Computer Emergency Response Team) report, the most serious types of attacks included IP spoofing.
  - in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP.
  - and various forms of eavesdropping and packet sniffing, in which attackers read transmitted information, including logon information and database contents.

Application of IPSec

IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include the following.

1. Secure branch office connectivity over the Internet:
   A company can build a secure virtual private network over the internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving cost and network management overhead.

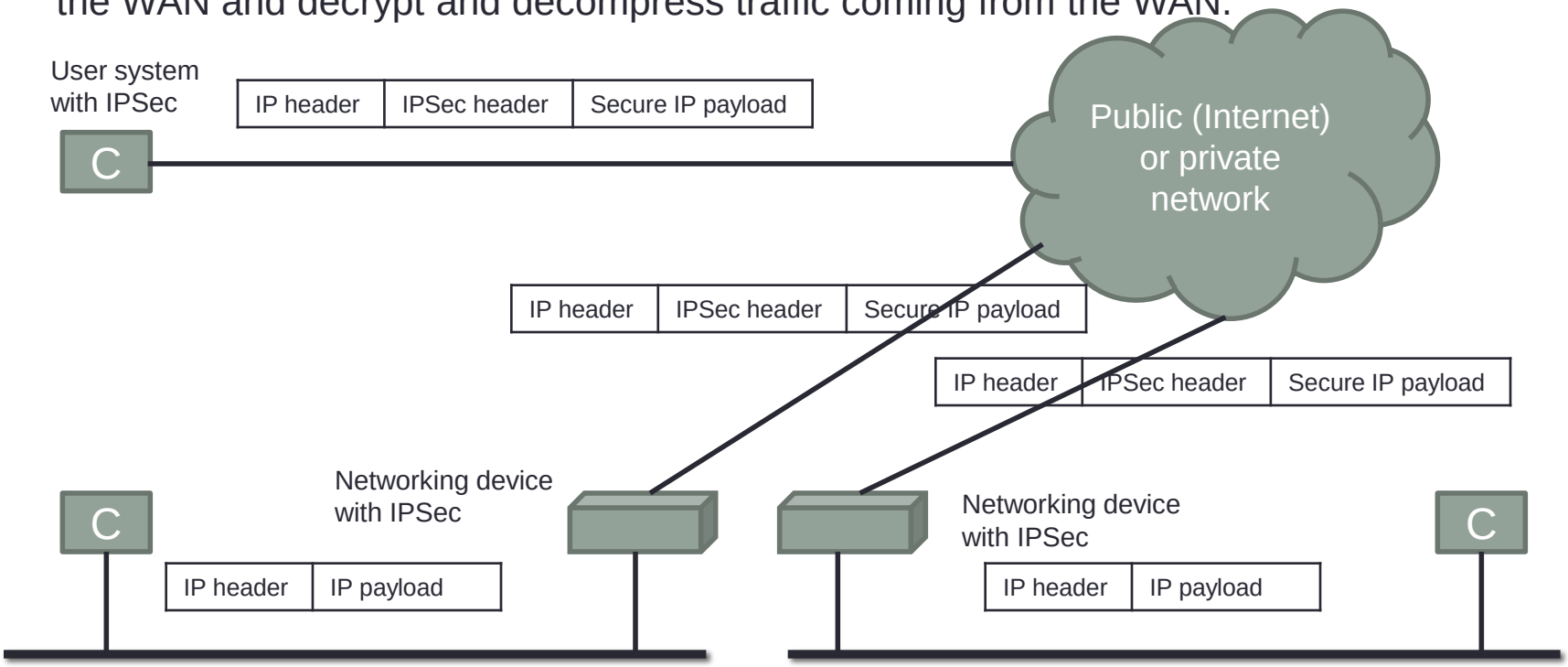
2. Secure remote access over the Internet:
   An end user whose system is equipped with IP security protocols can make a local call to an ISP and gain a secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

3. Establishing extranet and intranet connectivity with partners:
   IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

4. Enhancing electronic commerce security:
   Electronic commerce applications have built-in security protocols, however the use of IPSec enhances that security.

Scenario of IPSec usage

- Figure below is a typical scenario of IPSec usage.
- IPSec protocols operate in networking devices, such as a router or a firewall, that connect each LAN to the outside world.
- The IPSec networking device will typically encrypt and compress all traffic going into the WAN and decrypt and decompress traffic coming from the WAN.



Benefits of IPSec

- When IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the Internet into the organization.
- IPSec is below the transport layer (TCP, UDP) and so is transparent to applications.
- IPSec can be transparent to end users.
- IPSec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

Routing Applications

IPSec play a vital role in the routing architecture. IPSec can assures that

1. A router advertisement (a new router advertises its presence) comes from an authorized router.
2. A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) comes from an authorized router.
3. A redirect message comes from the router to which the initial packet was sent.
4. A routing update is not forged.

Without such security measures, an opponent can disrupt communications or divert some traffic.