Voice over Internet Protocol- Security Issues

6th November 05

Introduction

VoIP can provide more flexible service at a lower cost, but there are significant tradeoffs to consider. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied into the data network, resulting in additional security weaknesses and avenues of attack. Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with PSTN systems.

Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. While the PSTN is extremely reliable, Internet service is generally much less so. In addition, VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed and maintained, will be at greater risk if based on VoIP.

Encryption

Unless the VoIP network is encrypted, anyone with physical access to the office's local area network (LAN) could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect to a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Adequate physical control should be in

place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Proper physical countermeasures need to be in place to mitigate some of the biggest risks, such as the insertion of sniffers or other network monitoring devices. Otherwise, the installation of a sniffer could result in not just data being intercepted, but all voice communications as well (Ransome, 2004).

TLS:

To avoid exposure of a person's identity as well as who one calls and receives calls; TLS is used to secure the SIP messages hop-by-hop between the SIP entities (Ransome, 2004).

IPSec

IPSec is the standard encryption suite for the Internet Protocol and will be fully supported in IPv6. l In ESP Tunnel Mode, IPSec protects both the data and the identities of the endpoints (Ransome, 2004).

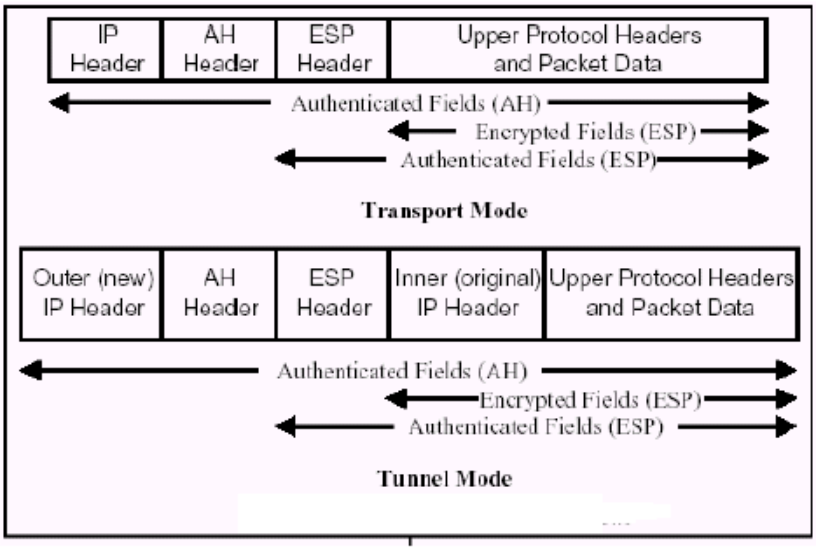

Figure . IPsec Tunnel and Transport Modes

Real-time Transport Protocol (RTP)

RTP is used to transfer real-time media, such as audio and video, over packet switched networks. It is used by both SIP and H.323 protocols. The protocol provides timing information to the receiver so that it can correctly compensate for delay jitter. It also allows the receiver to detect packet loss and take appropriate measures. The RTP header contains information that assists the receiver to reconstruct the media and also the information about how the CODEC bitstreams are fragmented into packets. RTP provides enough information to the receiver so that it can recover, in the event of packet loss or jitter. RTP is specified by IETF in RFC1889 and provides functions such as sequencing, payload and source identification, frame indication and intra-media synchronization. Intra-media synchronization is normally implemented as a play-out buffer to compensate for delay jitter (Ransome, 2004).

Bibliography

Ransome, James F. Voice over Internet Protocol (VoIP) Security. Digital Press, 2004.