VOIP security

Presented by
Mokkarala Ravi Kiran .
Shenoy Aashish .
Ved Ritu .

Introduction to VOIP

- VoIP was originally developed to provide voice communication between computer users in different locations.

- VoIP is a set of software, hardware and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network , or across the Internet .

Advantages & Disadvantages of VOIP

ADVANTAGES :

- Cost Effective .
- Integration with other services .
  Ex :
- Allowing web access with telephone features through a single PC or terminal
- PC to PC phone calls .
- Makes use of packet switching .
- Easy to upgrade.
- Bandwidth efficient.
- Benefit of providing telephone service to areas of low telephone coverage.
- Easy installation as compared to normal telephone systems.

DISADVANTAGES:

- Startup cost .
- Security lapses.
- VoIP only works if the PC is switched on and the VoIP software is running.
- Poor sound quality and reliability generated by VoIP.
- If your internet connection goes off, you can't have you VOIP working.
- Needs Electric Power.
- Limited Emergency Calls .

Application of VoIP

- Skype.
- Gizmo.
- Yahoo messenger.
- AIM
- Voice Buster.
- jajah.
- ooVoo.
- wengoPhone.
- SightSpeed.
- PhoneGnome.
- Zfone.

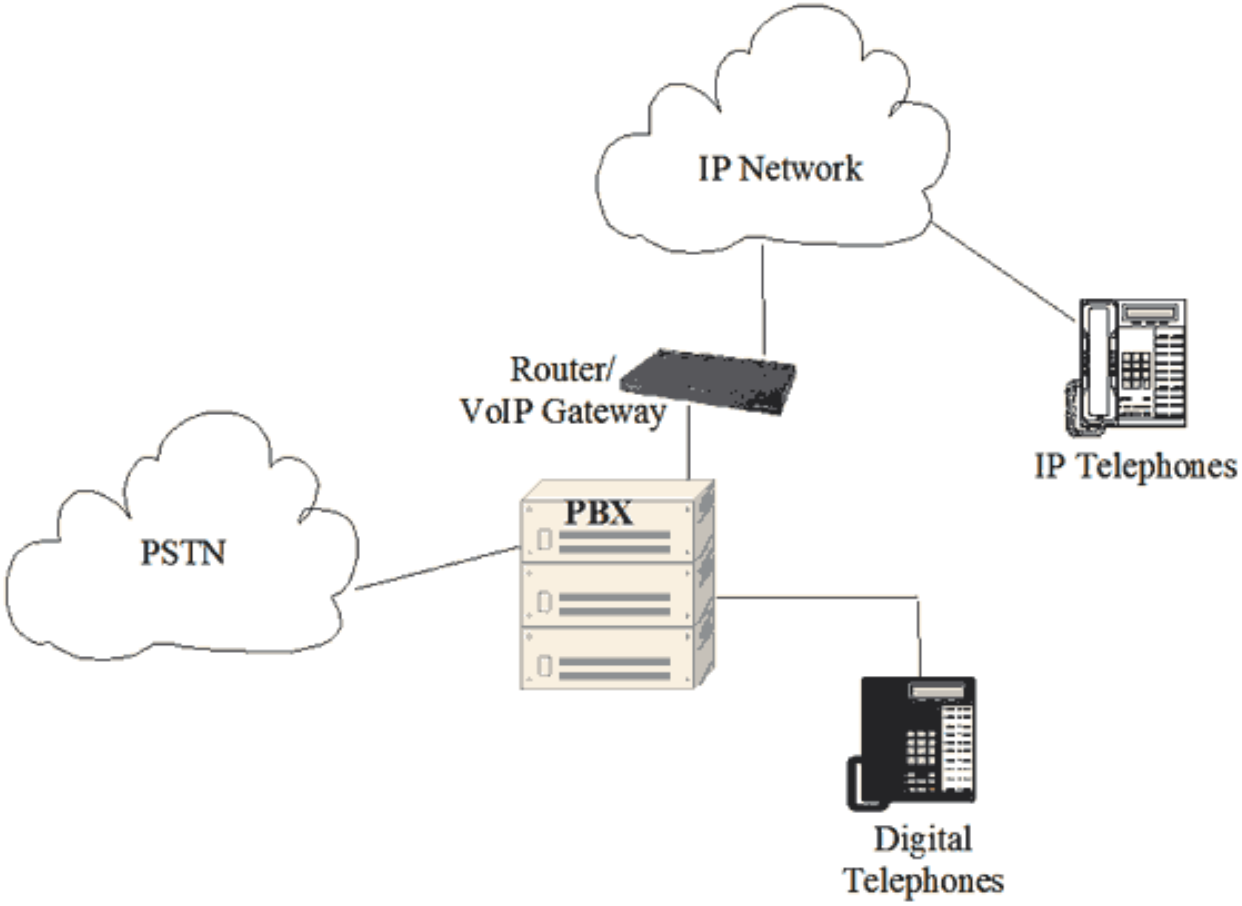
VOIP Risks, Threats & Vulnerability.

Confidentiality & Privacy :	Integrity Uses :
▪Switch Default Password Vulnerability ▪Classical Wiretrap Vulnerability. ▪Web server Interfaces. ▪IP Phone Netmask Vulnerability. ▪Extension to IP address mapping vulnerability.	▪Intrusion. ▪Insecure state. ▪DHCP server insertion attack. ▪TFTP server insertion attack.

Availability and Denial of Service :

- **CPU Resource Consumption Attack without any account information.**
- **Exploitable Software Flaws.**
- **Default Password Vulnerability.**
- **Account Lockout Vulnerability.**

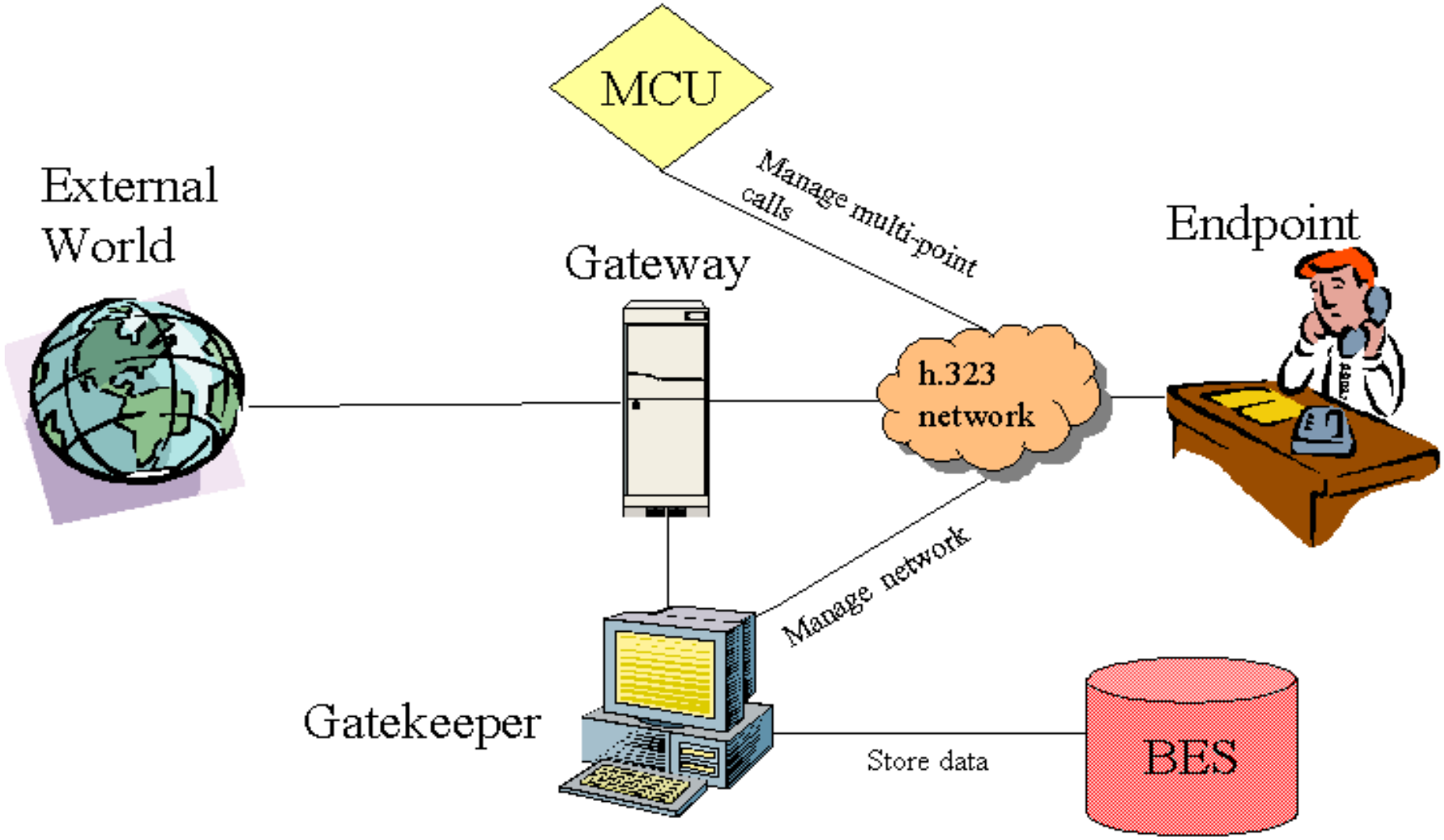
VOIP Data Handling



QOS issues related to VOIP

- Latency .
- Jitter.
- Packet Loss
- Bandwidth and Effective Bandwidth.
- Need for Speed.
- Power failure and Backup Systems.
- Quality of service Implications for Security

H.323 Architecture



H.323 Security,Encryption & Performance Issues.

Security Issues:

- Firewalls.
- NAT.

Encryption and Performance Issue:

- Delay in VoIP system by addition of codec.
- Increase in processing time due to encryption.
- Significant delay introduced by computing HMAC hash values for authentication .

Firewalls, NAT and Call Establishment

Firewalls, NAT and Call Establishment

1. Firewalls and NAT - Formidable challenge to VOIP implementers.
2. Much of the standards work for SIP in the IETF
3. SIP, H.323 ans H.248 / MEGACO al have similar problems with Firewalls and NATs
4. IPV6 will not alleviate the need for Firewalls or NATs.

Firewalls, NAT and Call Establishment

1. Firewalls
2. Network Address translations
3. Voip Issues with respect to Firewalls and NATs.
4. Call Setup Considerations with NATs and Firewalls.
5. Mechanism to solve the NAT Problem

Firewalls, NAT and Call Establishment

Firewalls

1. Firewall is usually the first line of defense against attackers.

- Traffic not meeting the requirements is dropped.
- Processing of traffic is determined by a set of rules specified by the Network Administrator.
- Provides a central location for deploying Security Policies
- no traffic can enter or exit the LAN without passing through it.

Firewalls, NAT and Call Establishment

Firewalls

Advantage for VOIP:

- Takes and enormous burden off the VOIP infrastructure.
- Security management is consolidated at the Firewalls instead of end points.

Price to Pay :

- Complicates Aspects of VOIP like:
  - Dynamic port trafficking,
  - Call set up Procedures.

Firewalls, NAT and Call Establishment

Firewalls

Packet Filtering:

<S IP | S Port | D IP | D Port | Protocol>

Types of Firewalls:

Stateless : No memory of traffic that occurred.

Stateful:

- Remembers previous traffic and investigates the application data in a packet.
- Can handle traffic that may not be destined to a static port

Firewalls, NAT and Call Establishment

Firewalls

Voip Specific Firewall Needs:

- Added responsibility of brokering the data flow between the voice and data segments of the network.
- All voice traffic to and from these devices would have to be explicitly allowed if no firewalls were present because RTP makes use of dynamic UDP ports making the device vulnerable for a UDP DOS attack.
- Hence place these devices behind a stateful firewall to broker VOIP media traffic.
- Physical segmentation is not practical because of the capability of VOIP to have Voice and Data on the same Physical Network.

Firewalls, NAT and Call Establishment

Network Address Translation

- Maps internal network addresses to external IP addresses.
- Contributes indirectly towards the security for a LAN, Making internal IP addresses less accessible for public Internet.
- NAT Routers are generally more secure than a PC directly connected to the Internet.
  - reduced chance of Open ports, Malicious programs, etc.

Firewalls, NAT and Call Establishment

Types of Network Address Translation

Full Cone NAT:

same inertnal IP & PORT <==> same External IP & PORT

any external host can communicate to the internal host by sending a packet to the mapped external ip.

Restricted Cone NAT:

same inertnal IP & PORT <==> same External IP & PORT

unlike full cone, External host with IP address X can send packet to an internal host only if the internal host had previously sent a packet to IP address x.

Firewalls, NAT and Call Establishment

Types of Network Address Translation

Port Restricted Cone:

same inertnal IP & PORT <==> same External IP & PORT

Similar to Restricted Cone NAT but, External host with IP address ***X*** and Port number ***P*** can send a packet to an internal host only if the internal host had previously sent a packet to IP address ***X*** and Port number ***P***.

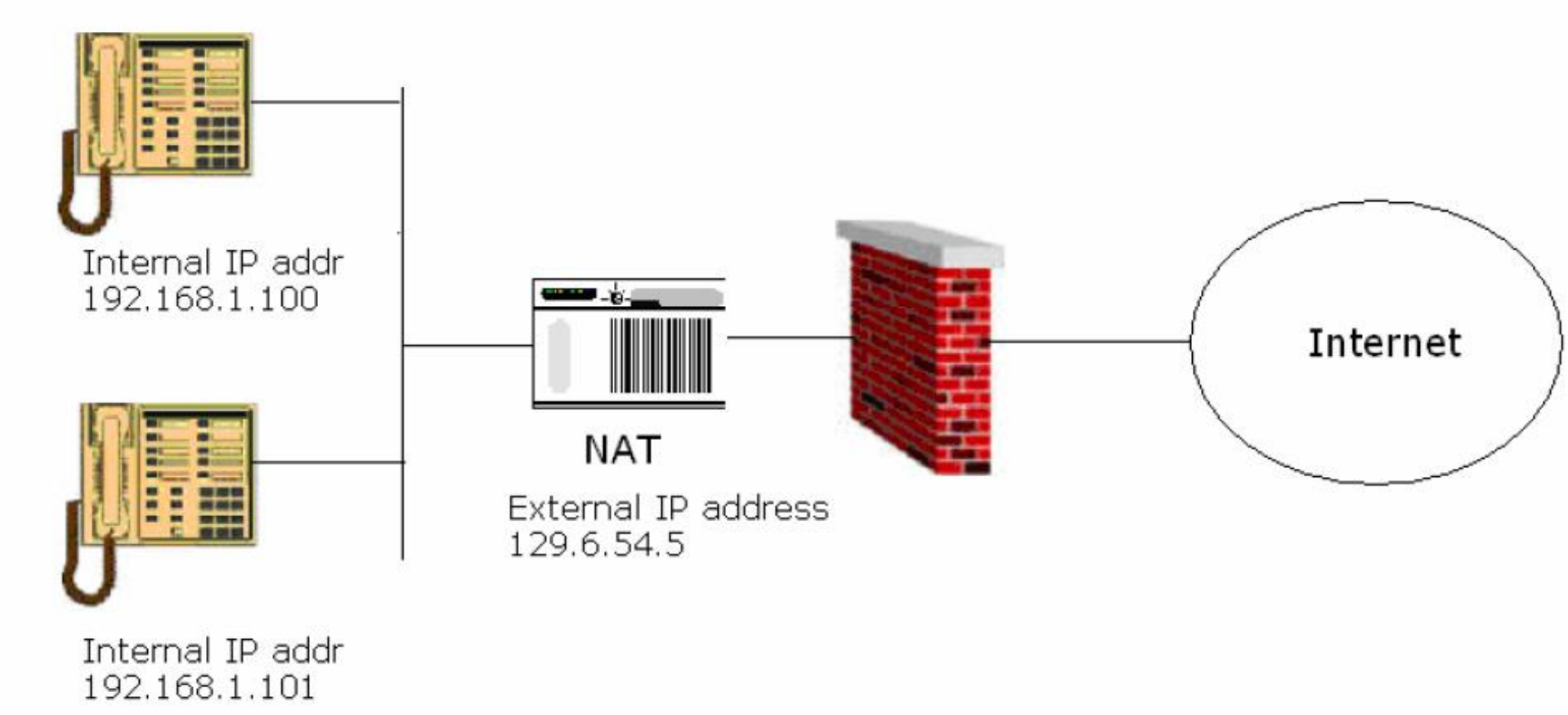
Symmetric NAT:

[(same inertnal IP & PORT) (Specific Destination IP & Port)]<==> same External IP & PORT

Only the external host that receives the packet can communicate to the internal host.

Firewalls, NAT and Call Establishment

IP Telephones Behind NAT and Firewall



Firewalls, NAT and Call Establishment

Firewall, NATs and VOIP Issues

- FIREWALL:
  - RTP Traffic is dynamically assigned an even port number in the range ofUDP ports (1024 - 65,534).
  - Thus Stateful Firewalls are used that can process H.323 and SIP.

- NAT:
  - The standard NAT practice of assigning new port numbers at random breaks the pair relationship between RTP and RTCP Port numbers.
  - Problem is exacerbated if both parties are behind NATs.

Firewalls, NAT and Call Establishment

Firewall, NATs and VOIP Issues

<u>Incoming Calls:</u>

Careful Administration and rule definitions should be used at the firewalls when allowing incoming connections.

Solutions:

- Application Level Gateways
- Firewall Control Proxies

NATs create even more difficulties for incoming calls. as the external host must know the mapped External IP and Port at the NAT of the Internal Host.

Firewalls, NAT and Call Establishment

Firewall, NATs and VOIP Issues
<u>Effect on QOS:</u>

VOIP is very sensitive to latency.

QOS / VOIP Aware Firewalls are designed to avoid performance problems.
Issue:

Not only how fast the firewall can interact with the network traffic, but also how fast itz processor can handle VOIP Packets.

- Firewall has to open the packets for filtering them
- NAT has to fill in new data into these packets and send them across.

Firewalls, NAT and Call Establishment

Call Setup Considerations with NATs and Firewalls

Factors that influence the setup time of a VOIP call:

- At the Network Level:
  - Include the topology of the network
  - Location of both endpoints
  - Presence of NAT and Firewalls

- At the Application Level:
  - The degree or lack of Authentication and other data security measures.
  - Choice of protocol used to set up the call.

Firewalls, NAT and Call Establishment

Call Setup Considerations with NATs and Firewalls

1. Application Level Gateways (ALG)

- ALGs is an embedded software on a Firewall or NAT.
- Allows for dynamic configuration based on application specific information.
  - A firewall with VOIP ALG can parse and understand H.323 or SIP and dynamically open and close the necessary ports.
  - When NAT is employed, the ALG needs to open up the VOIP packets and reconfigure the header information to correspond to the correct IP and Port addresses.
- Currently, ALG is the simplest and safest workaround to allow the coexistence of VOIP, Firewall and NAT.

Firewalls, NAT and Call Establishment

Call Setup Considerations with NATs and Firewalls

1. Application Level Gateways (ALG)

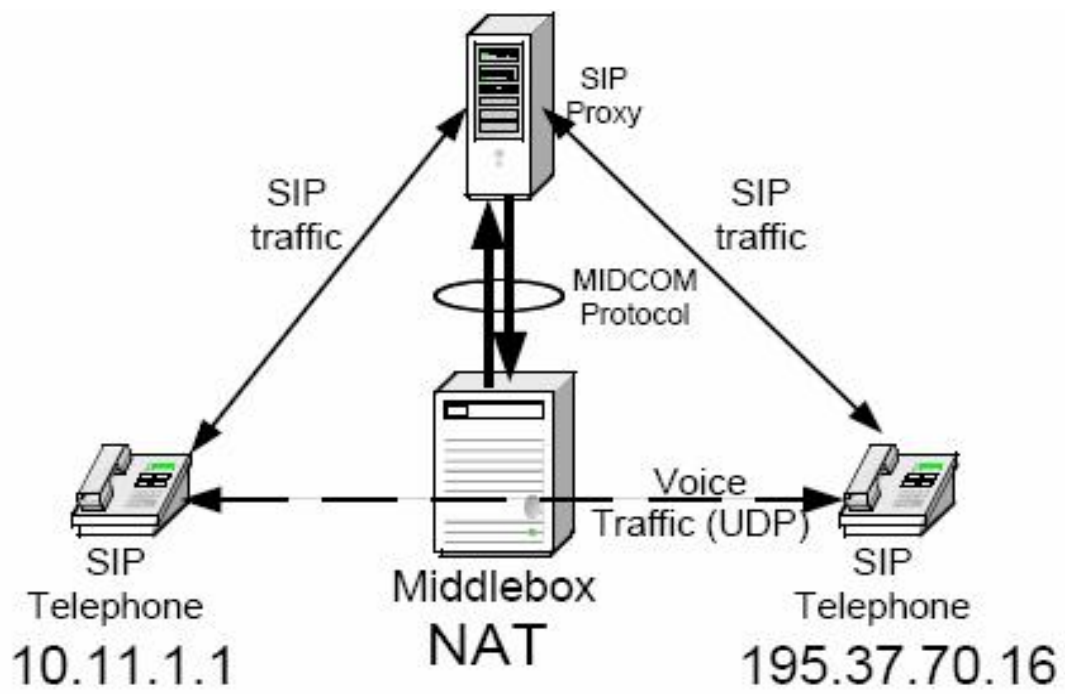
- Significant performance and Fiscal costs associated with the implementation of an ALG.
  - The manipulation of VOIP packets introduces latency into the system.
  - Can slow down the throughput of the firewall
  - Contributes to general network congestion.
  - A firewall with ALG support will need to be upgraded each time the standards for VOIP change.
  - The additional Application Intelligence can introduce instabilities into the firewall itself.

Firewalls, NAT and Call Establishment

Call Setup Considerations with NATs and Firewalls

2. Middlebox Solutions:

- Drawback of ALG - Embedded in the Firewall itself.
- Middlebox-style implies, placing an extra devic outside the firewall that performs many of the functions associated with an ALG.



Firewalls, NAT and Call Establishment

Call Setup Considerations with NATs and Firewalls

2. Middlebox Solutions:

- The Midcom Protocol has not been finalized yet by the IETF.

Advantages:

- Abstracting Stateful inspection and manipulation of signaling packets from the NATs and Firewalls will improve scalability and reduce cost of updating the network.
- Performance improvement.

Disadvantages:

- The Middlebox requires protection from attackers.
- A second firewall must be placed outside to protect the device

Firewalls, NAT and Call Establishment

Call Setup Considerations with NATs and Firewalls

3. Session Border Controllers (SBC):

- SBCs are dedicated appliances that offer one or more of the following services to a VOIP Perimeter:
  - Firewall / NAT translation,
  - Call Admission Control,
  - Service Level Agreement Monitoring,
  - Support for Lawful intercept
  - Protocol interworking.

- Demand for these devices is likely to grow in the future.

Firewalls, NAT and Call Establishment

Mechanism to solve the NAT Problem

1. **Simple Traversal of UDP through NATs (STUN)**
2. **Traversal Using Relay NAT (TURN)**
3. **Interactive Connectivity Establishment (ICE)**
4. **Universal Plug and Play (UPnP)**

Encryption & IPsec

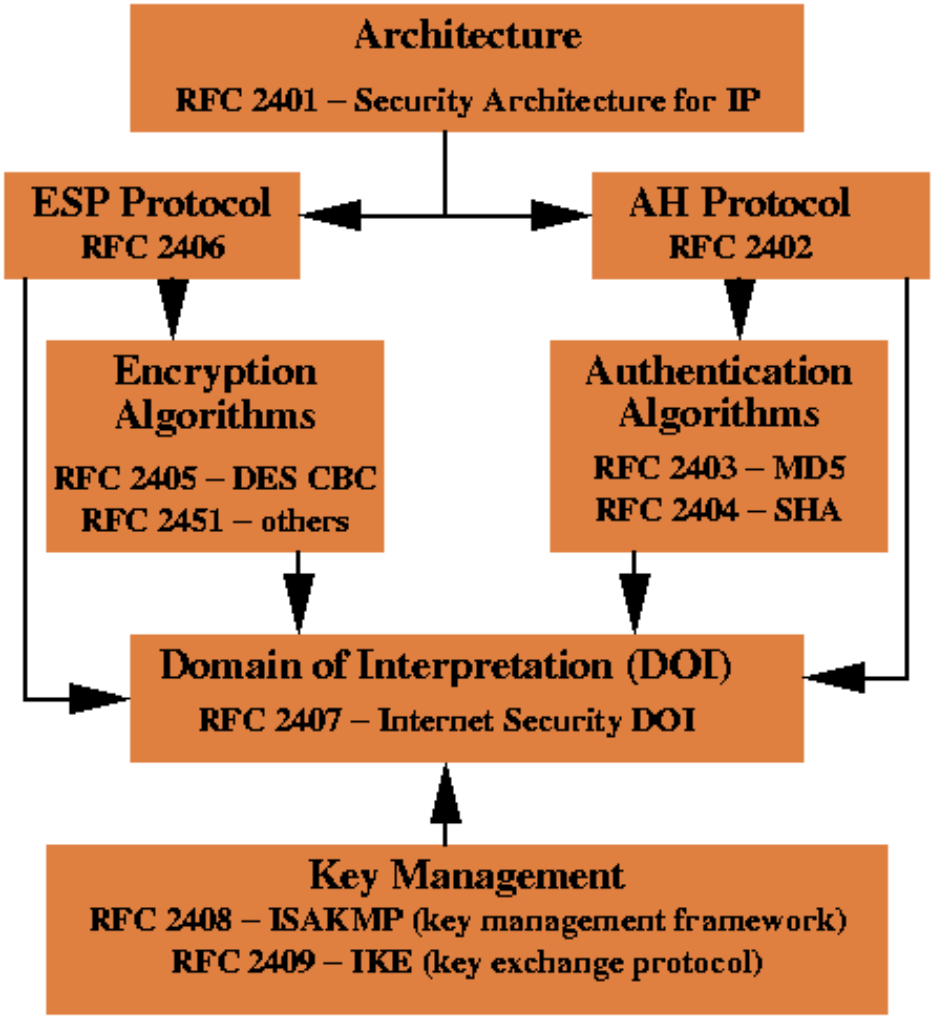
Necessity

- Protection from Internal hackers
- Protection from Packet Sniffers

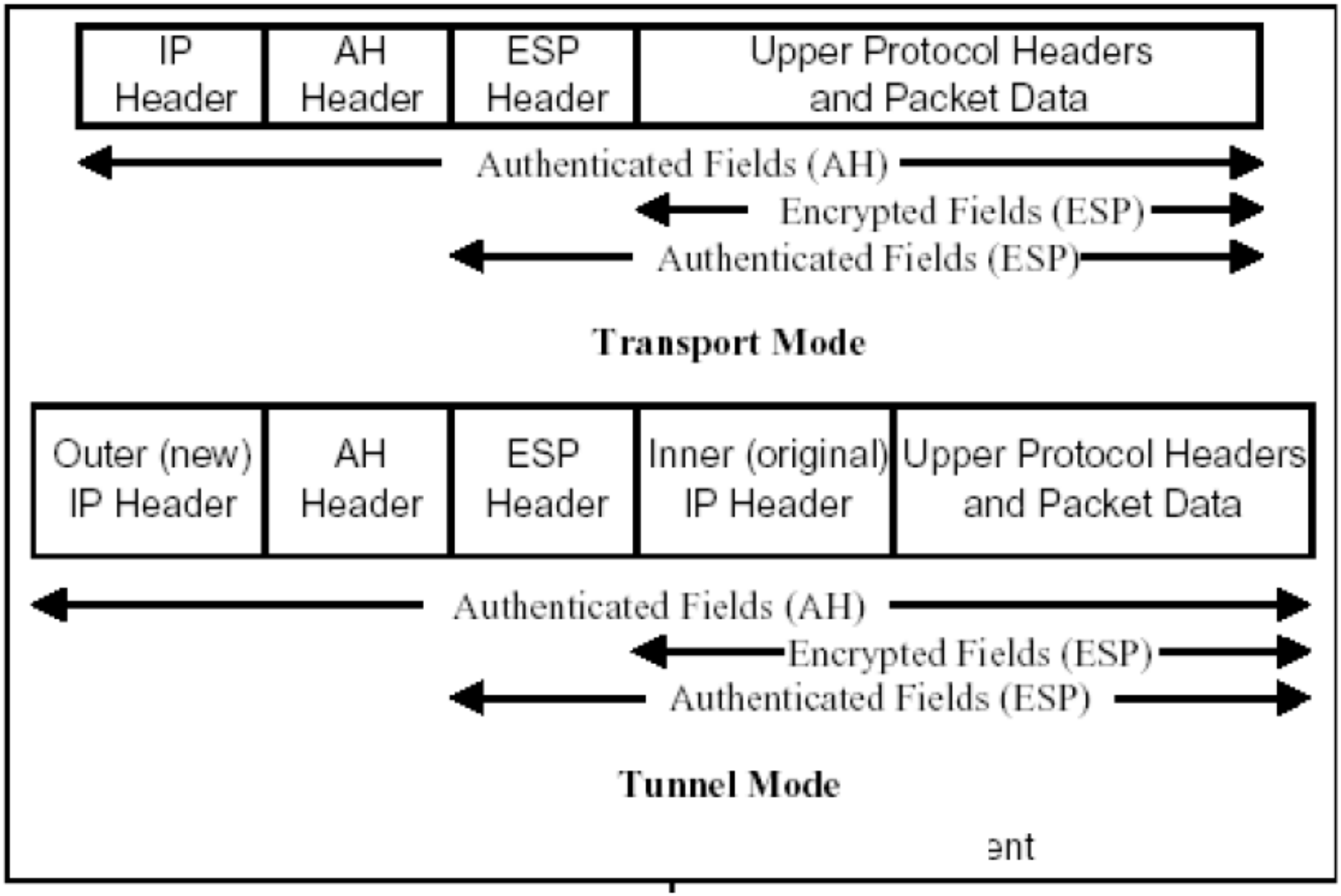
Challenges and Tradeoffs

- QOS and Latency vs Security

IPSec Architecture



Transport and Tunnel



VOIPSec Issues

Delay

o Processing—PCM to G.729 to packet

o Encryption — ESP encapsulation + 3DES

o Serialization —

- IPsec overhead: about 40 bytes (depending on configuration)
- IP header: 20 bytes
- UDP + RTP headers: 20 bytes
- RTP header compression: 3 bytes for IP+UDP+RTP

Effects on 8 kbps CODEC (voice data: 20 bytes)

o clear text voice overhead: 3 bytes =>
required bandwidth ~ 9 kbps

o IPsec encrypted voice overhead: 80 bytes =>
required bandwidth 40 kbps

Encryption Decryption Latency

- Study by Barberi et al.
- DES vs 3DES vs SHA-1 vs 3DES + SHA-1

Scheduling in Crypto Engines

- (Routers, Firewalls) vs Crypto Engines(FIFO)
- Homogenous Traffic Differentiation

Expanded Packet Size

- Increased Header overhead
- Bandwidth utilization reduced by 63%

IPSec NAT Incompatibility

- Sender Authentication
- AH and ESP incompatibility
- IKE Negotiations required

Solutions for VOIPSec

Encryption at Endpoints

- LANs do not require Encryption
- Important for Internet traffic
- Endpoint issue – Processing Capabilities
- New Devices with high processing
- SRTP and MIKEY

SRTP

- AES – counter, f8(UMTS) modes.
- HMAC-SHA1, Akey= 80 bits, 128 bit MasterKey

- Confidentiality for RTP as well as for RTCP by encryption of the respective payloads;
- Confidentiality - encryption of payloads.
- Integrity and replay protection.
- Session keys Refresh – cryptanalysis guard.
- Framework allows upgrading with new cryptographic algorithms.
- Secure session key derivation with pseudo-random function at both ends;
- Salting keys - against pre-computation attacks.
- Security for unicast and multicast RTP applications.

SRTP Advantages

- Low computational cost.
- Low bandwidth cost and a high throughput.
- Small footprint.

- RTP profile - easy integration into RTP stack.
- Independent from transport, network, and physical layers.
- Low key management overhead.

MIKEY

- Implemented as an Independent software library
- Establishment of key material within a 2-way handshake
- Four options for Key Distribution:
  - Preshared-key
  - Public-key encryption
  - Diffie-Hellman key exchange protected by public-key encryption
  - Diffie-Hellman key exchange protected with preshared-key and keyed hash functions (using a MIKEY extension (DHHMAC))

Better Scheduling Schemes

- QOS Prioritization

Packet Compression

- cIPSec – Barberi, et al.

NAT/IPSec Compatibility

- Realm-Specific IP (RSIP)
- IPv6 Tunnel Broker
- IP Next Layer (IPNL)
- UDP encapsulation.

Trunking

Protocol suite	Channels	Overhead	Codec bitrate	Trunked bitrate	unicast bitrate
Frame Relay or MP	8	3.6 kbps	G.729 (8 kbps)	67.6 kbps	92.8 kbps
MPLS	8	18.8 kbps	G.729 (8 kbps)	82.8 kbps	214.4 kbps
IPSec	8	34.8 kbps	G.729 (8 kbps)	98.8 kbps	342.4 kbps

Codec	Payload bandwidth	MOS	Description
G.729	8 kbps	3.92	This is the second most supported codec and offers nearly the same quality as G.711. The key advantage is that it is compressed eight times smaller than G.711 while sounding almost as good.

VOIP Deployment

- SIP vs H.323 - Multi-protocol devices
- End-to-End vs Firewall based VPNs vs Hybrids

Legal Directives

• The Privacy Act of 1974.

• Office of Management and Budget "Guidance on the Privacy Act Implications of Call Detail Programs to Manage Employees' Use of the Government's Telecommunication System" (See FEDERAL REGISTER, 52 FR 12990, April 20, 1987).

• NARA General Records Schedule 12, which requires a 36-month retention of telephone CDR records http://www.archives.gov/records_management/ardor/grs12.html

THANK YOU

VOIP FAQ (Appendix)

- 1. What is VOIP?

  Voice Over Internet Protocol is a set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

- 2. What are some of the advantages of VOIP?

  - a. Cost – a VOIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.

  - b. Integration with other services – Innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VOIP system may be integrated with video across the Internet, providing a teleconferencing facility.

- 3. What are some of the disadvantages of VOIP?

  - a. Startup cost – although VOIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VOIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VOIP field develops.

  - b. Security – the flexibility of VOIP comes at a price: added complexity in securing voice and data. Because VOIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VOIP system than a conventional voice telephone system or PBX.

VOIP FAQ (Appendix)

- 1. What is VOIP?

  Voice Over Internet Protocol is a set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

- 2. What are some of the advantages of VOIP?

  - a. Cost – a VOIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.

  - b. Integration with other services – Innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VOIP system may be integrated with video across the Internet, providing a teleconferencing facility.

- 3. What are some of the disadvantages of VOIP?

  - a. Startup cost – although VOIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VOIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VOIP field develops.

  - b. Security – the flexibility of VOIP comes at a price: added complexity in securing voice and data. Because VOIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VOIP system than a conventional voice telephone system or PBX.

Glossary

- **Application Level Gateway (ALG)** – Application Level Gateways (ALGs) are application specific translation agents that allow an application (like VOIP) on a host in one address realm to connect to its counterpart running on a host in different realm transparently. An ALG may interact with NAT to set up state, use NAT state information, modify application specific payload and perform whatever else is necessary to get the application running across disparate address realms.

- **Abstract syntax notation one (ASN.1)**: A standard, flexible method that (a) describes data structures for representing, encoding, transmitting, and decoding data, (b) provides a set of formal rules for describing the structure of objects independent of machine-specific encoding techniques, (c) is a formal network-management Transmission Control Protocol/ Internet Protocol (TCP/IP) language that uses human-readable notation and a compact, encoded representation of the same information used in communications protocols, and (d) is a precise, formal notation that removes ambiguities.

- **Call Processor –** component that sets up and monitors the state of calls, and provides phone number translation, user authorization, and coordination with media gateways.

- **Firewall Control Proxy -** component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination.

Glossary

- **Application Level Gateway (ALG)** – Application Level Gateways (ALGs) are application specific translation agents that allow an application (like VOIP) on a host in one address realm to connect to its counterpart running on a host in different realm transparently. An ALG may interact with NAT to set up state, use NAT state information, modify application specific payload and perform whatever else is necessary to get the application running across disparate address realms.

- **Abstract syntax notation one (ASN.1)**: A standard, flexible method that (a) describes data structures for representing, encoding, transmitting, and decoding data, (b) provides a set of formal rules for describing the structure of objects independent of machine-specific encoding techniques, (c) is a formal network-management Transmission Control Protocol/ Internet Protocol (TCP/IP) language that uses human-readable notation and a compact, encoded representation of the same information used in communications protocols, and (d) is a precise, formal notation that removes ambiguities.

- **Call Processor –** component that sets up and monitors the state of calls, and provides phone number translation, user authorization, and coordination with media gateways.

- **Firewall Control Proxy -** component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination.

References

- http://www.lincoln.edu/math/rmyrick/ComputerNetworks/InetReference/141.htm
- http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
- http://www.all-voip-info.com/security_risks.htm