VoIP Security

M.Tech. Seminar

Rahul Singhai

05329036

Outline

- Motivation
- VoIP
- VoIP Security Threat Scenarios
- H.323 Security Concerns
- SIP Security Concerns
- Firewalls, NAT, and Call Establishment
- Conclusion

Motivation

- VoIP uses the same routes used by data traffic, so prone to same cyber threats
- Phones can be destinations for spam
- DoS attacks
- Spoofing the phone’s IP address and billing back to owner
- Calls can be intercepted and listened

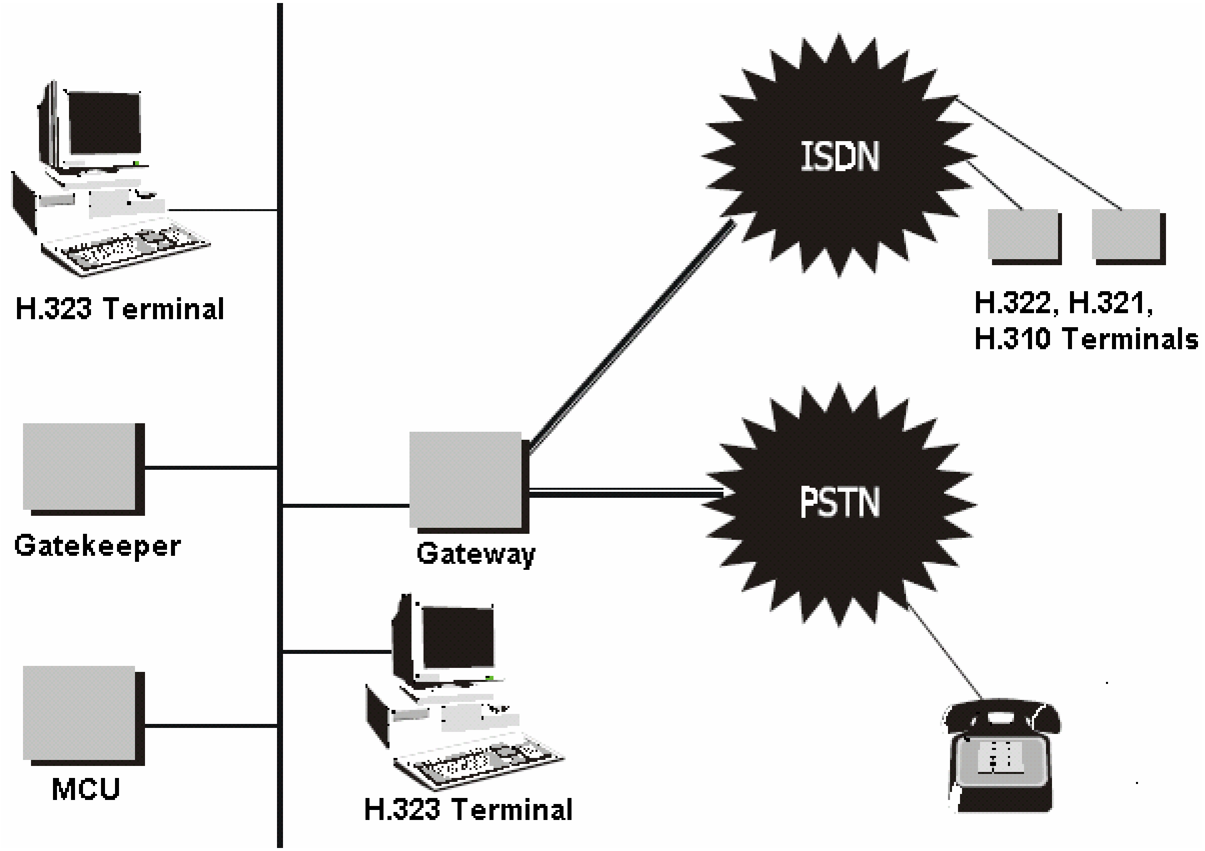
Voice over IP (VoIP)

- VoIP is routing of voice conversations over an IP based network
- Voice data flows over a packet-switched network, instead of traditional dedicated circuit-switched voice transmission lines
- VoIP components include end-user equipment, network components, call processors, gateways, and protocols

Voice over IP (VoIP)

- Protocols used to carry voice are referred as VoIP protocols
- **H.323 family of protocols** : Intelligence both in endpoints and network components
- **Session Initiation Protocol (SIP)** : Intelligence in endpoints of the system
- **Media Gateway Controller Protocol (MGCP)** : Intelligence in network components

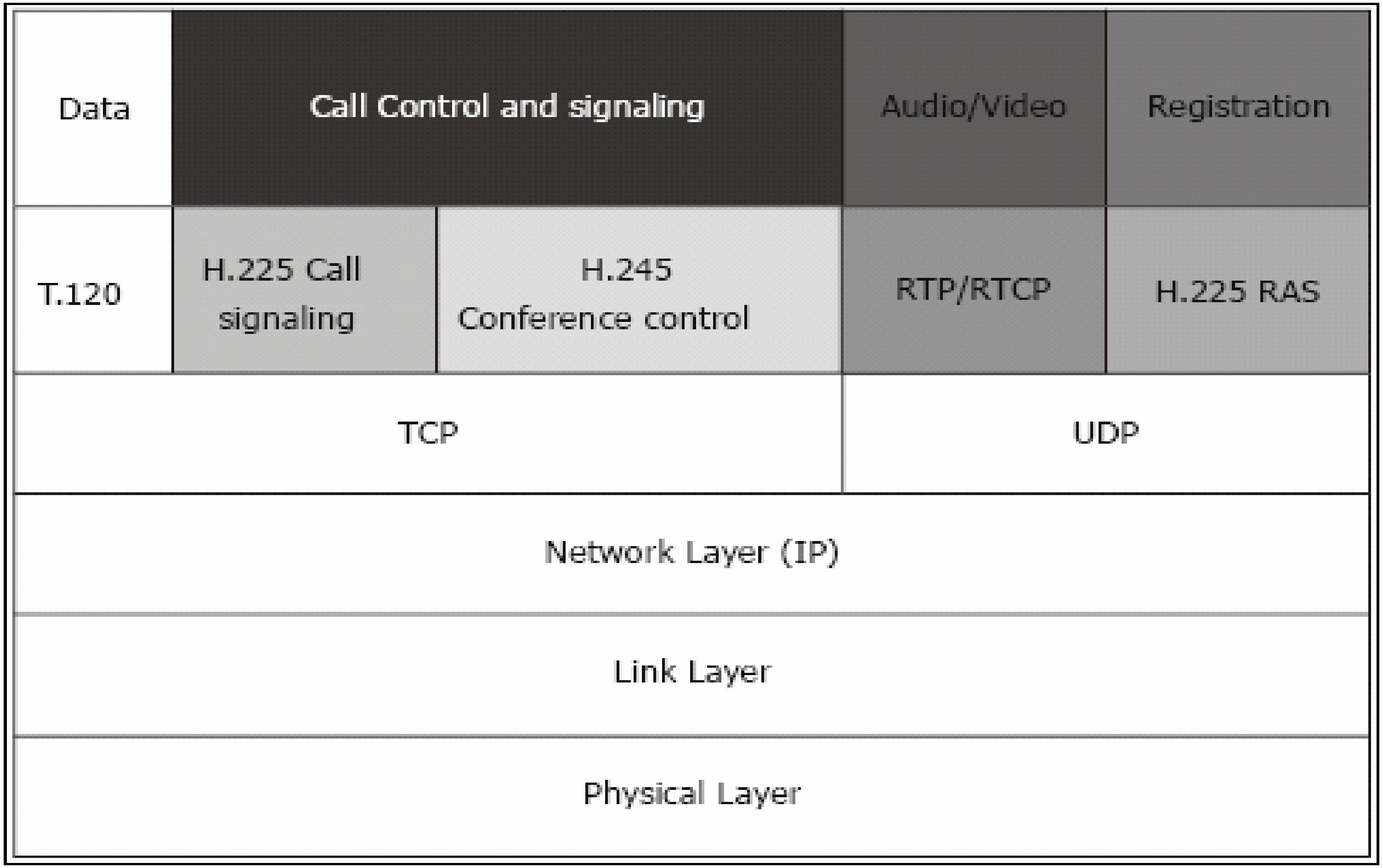
H.323 Architecture



H.323 Architecture

- **Terminals** : Endpoints bound to a specific address and gateway, provides real-time, two-way communication.
- **Gateway** : Provides communications between H.323 terminals on the IP network with other terminals on other H.323 gateway, PSTN or SIP network. Handles different transmission formats.
- **Gatekeeper** : Central point for all the calls within its zone. Provides services to registered endpoints such as address translation, admissions control, call signaling, call authorization and authentication, call management, call routing, accounting and bandwidth management.
- **Multi-point Control Units (MCUs)** : Provides multi-point conference capability. Consists of Multi-point Controller (MC) and Multi-point Processor (MP).
  - **MC** : Determines common capabilities of conferencing terminals
  - **MP** : Multiplexes audio, video and data streams.

H.323 Protocol Stack



Data

Call Control and signaling

Audio/Video

Registration

T.120

H.225 Call signaling

H.245 Conference control

RTP/RTCP

H.225 RAS

TCP

UDP

Network Layer (IP)

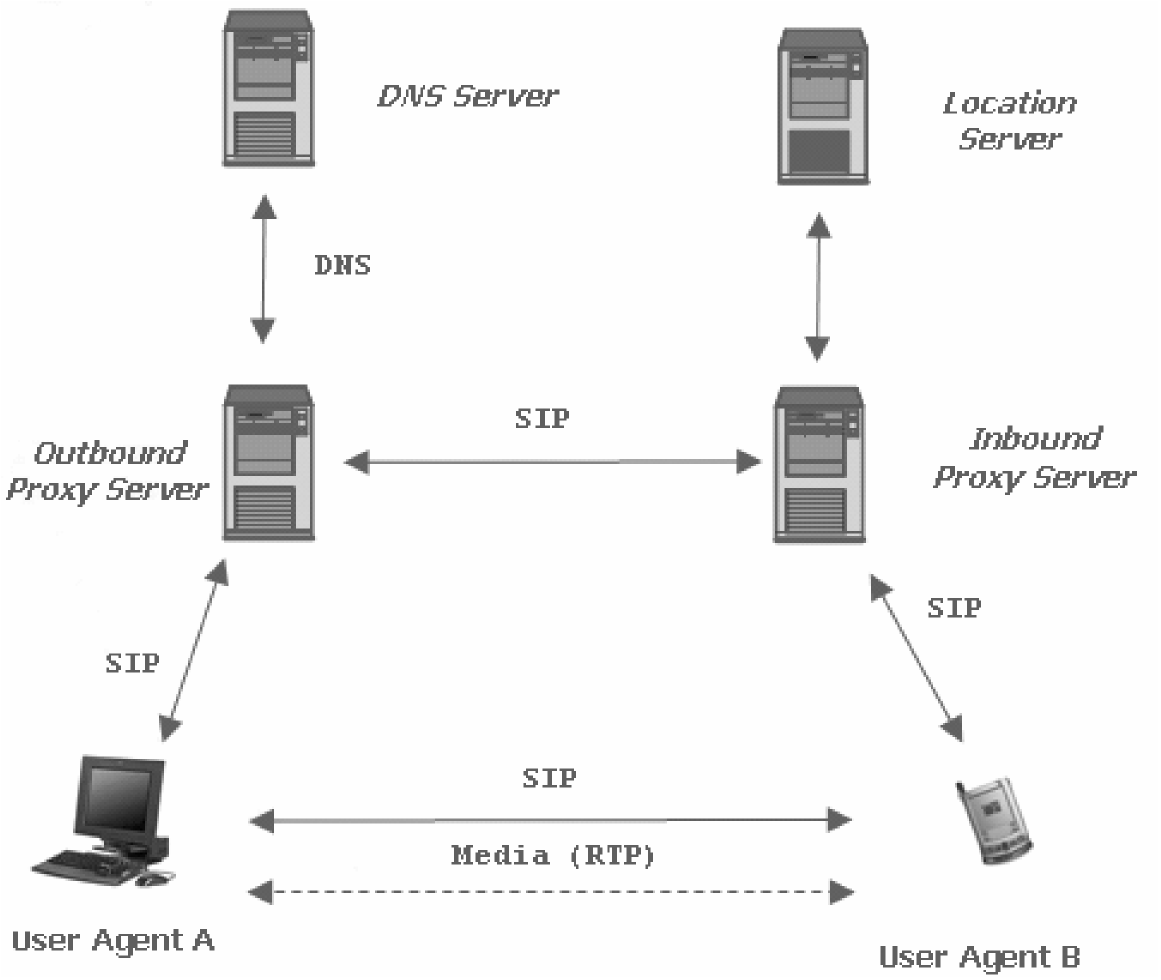
Link Layer

Physical Layer

H.323 Protocols

- **UDP** : To transfer audio, video and registration packets.
- **TCP** : To transfer data and control packets in call signaling.
- **T.120** : To transfer data.
- **H.225/Q.931** : For call signaling control.
- **H.225/RAS (Registration Admission Status)** : To establish a call.
- **H.245** : To negotiate media streams (after the call is established).
- **RTP/RTCP** : To transfer audio and video using audio (G.711, G.723.1, G.728) and video (H.261, H.263) codecs.

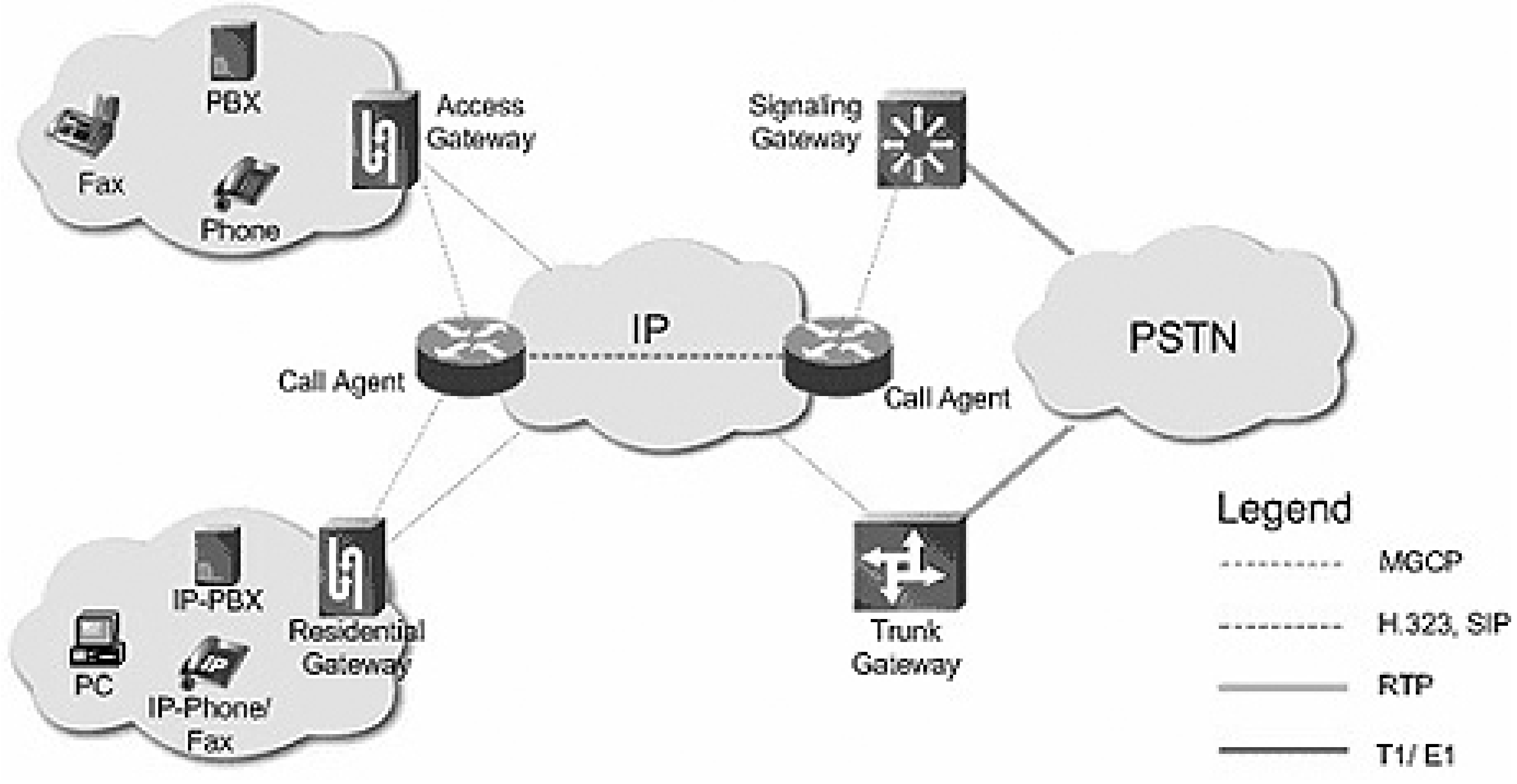
SIP Architecture



SIP Architecture

- **User Agent** : End system acting on behalf of the user.
  - **User Agent Client (UAC)** : To initiate a SIP request to UAS
  - **User Agent Server (UAS**) : Listens and responds to SIP requests.
- **SIP Server** : Provides SIP call setup and services.
  - **Registration / Location Server** : Receives and authenticates registration requests from SIP users and updates their current location with itself.
  - **Proxy Server** : Receives SIP requests and forwards them to the next-hop server.
  - **Redirect Server** : Resolves information for the UAC. On receipt of the SIP request, determines the next-hop server and returns the address of next-hop server to the client.
  - **DNS Server** : Locates in-bound proxy servers.

MGCP Architecture



MGCP Architecture

- **Media gateway controller (MGC) or Soft-Switch or Call Agent**: Controls multiple media gateways.
- **Media Gateway** : Executes commands sent by the centralized MGC and converts data between PSTN to IP, PSTN to ATM, ATM to IP, and also IP to IP.
- **MGCP** : Defines the communication between call-agents and gateways. Monitors events on end-points and gateways and instructs them to send media to specified addresses. The issued commands are executed in a master/slave manner.

VoIP Security Threat Scenarios

- **Application Level Attacks :**
  - **Call Hijacking** : Attacker spoofs a SIP response, indicating to the caller that the called party has moved to a rogue SIP address, and hijack the call.
  - **Resource Exhaustion** : Exhausts the IP addresses of a DHCP server.
  - **Eavesdropping** : Attacker may sniff the network traffic on VoIP LAN and decipher the voice conversations, e.g. VOMIT.
  - **Message Integrity** : Attacker conducts a man-in-the-middle attack and alters the original communication between two parties.
  - **Toll Fraud** : Attacker impersonates a valid user/IP phone and uses the VoIP network for making free long distance calls.

VoIP Security Threat Scenarios

- Application Level Attacks (cont.)
  - **Denial of Service (DoS)** : DoS is caused by anything that prevents the service from being delivered.
    - **Unavailable bandwidth** : Network getting congested to a level that it cannot provide the bandwidth needed to support the application.
    - **Servers incapable of handling traffic** : Extraneous services, such as viruses and Trojan horses, may be reducing the available resources to the server
    - **DoS in SIP-based networks** :
      - Spoofing end-point identity, attacker sends “CANCEL” or “BYE” message to either of the communicating parties and ends the call.
      - Sending a spoofed ICMP “port unreachable” message to the calling party.

VoIP Security Threat Scenarios

- **Availability** : Attacks reduce the quality of speech or target simple equipment malfunctions. The main risk is the lack of electricity to power endpoints and other elements making up an VoIP network or infrastructure.
- **Physical Access** : Attacker place calls at the expense of subscriber while continuing to let the subscriber place calls at the same time.
- **Non-Trusted Identities** : Call participant's identity can be easily spoofed, anywhere along the path of signaling information.
- **Attacks against the Operating System** : VoIP devices inherit same vulnerabilities of the OS or firmware they run on top of. Numerous “point-and-shoot” exploits available for their vulnerabilities.

VoIP Security Threat Scenarios

- **Placement of Intelligence** : Some or all of the intelligence is located at the endpoints, allowing them to interact with different VoIP and networking components. A malicious party using such an endpoint, or a modified client, will have the same ability to interact with these components.
- **Configuration Weaknesses in VoIP devices** : May have exposed TCP and UDP ports. Default services running on open ports vulnerable to DoS, buffer overflows or weak passwords.

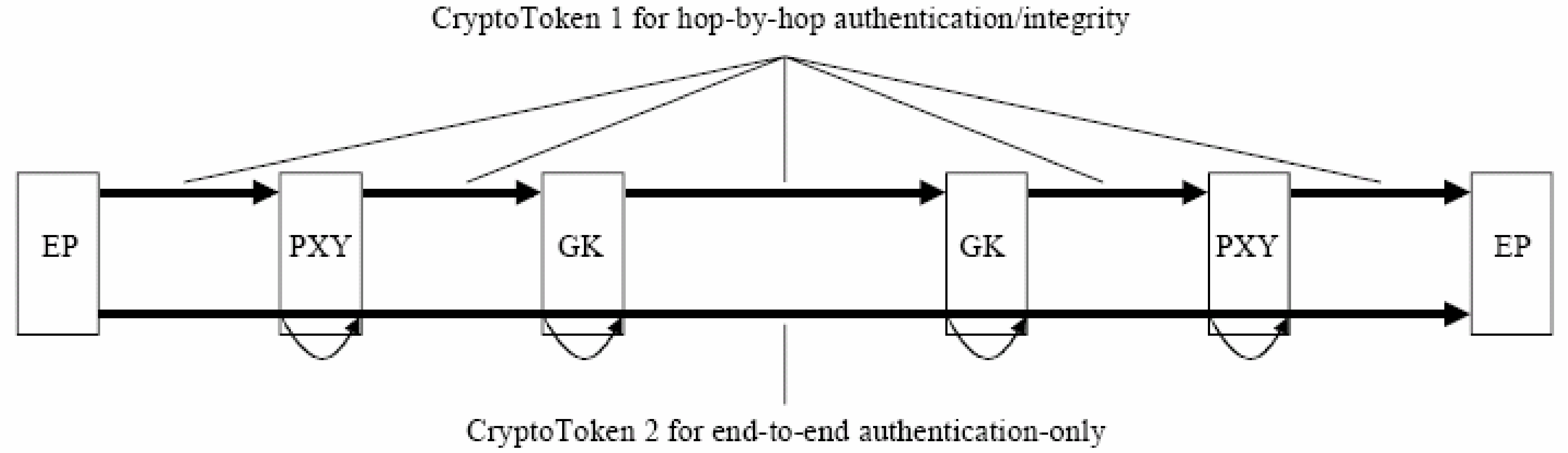
VoIP Security Threat Scenarios

- **Improper IP Telephony network designs** : No authentication of IP Phone to network. No checking of IP Phone's actual location against the credentials it uses.
- **Functional protocol testing or Fuzzing** : Fuzzing has led to a wide variety of DoS and buffer overflow vulnerability discoveries in VoIP products. Many of these vulnerabilities have found by the University of Finland's PROTOS group. The PROTOS group typically makes their tools available to the public, which means anyone can download and run the tools necessary to crash vulnerable implementations.

H.323 Security Concerns

- **Call Establishment (H.225) Security** : Secured mode of communication should be used (e.g. IPSec or TLS) before exchange of call connection message
- **Call Control (H.245) Security** : H.245 channel is secured using privacy mechanisms negotiated during H.225 signaling
- **Media Stream Privacy** : Media stream encoded using algorithm and keys presented during H.245 signaling
- H.235 protocols specify security aspects of H.323 and are expressed as Annexes D, E, F, G, H, and I.

H.235 Annex D - Baseline Security Profile


CryptoToken 1 for hop-by-hop authentication/integrity
EP
PXY
GK
GK
PXY
EP
CryptoToken 2 for end-to-end authentication-only

- End-point and gatekeeper share a secret key. Gatekeeper uses this key to verify messages sent by the end-point and to compute token for messages that it sends to the end-point.
- Tokens are values computed by HMAC-SHA1-96 algorithm applied to the message which includes a monotonically increasing sequence number and timestamp.

H.235 Annex D - Baseline Security Profile

- Calculated tokens are appended to the messages (in the CryptoH323Token field).
- Security works on hop-by-hop basis.
- An "authentication only" option is available for smooth NAT/firewall traversal, so the integrity check is computed only over a special part of the message.
- **Disadvantage of this profile** : The administration of all the shared secret keys. They have to be stored in a central place (back-end service), which makes this one a critical part of the whole system.

H.235 Annex D - Voice Encryption Profile

- Handles media traffic security.
- Describes a Diffie-Hellman Key exchange during H.225 call signaling.
- This key is used to protect media keys that are used to encrypt media (RTP/RTCP) packets.
- Encryption algorithms are 56bit DES, 56-RC2, 168 bit triple DES, AES.

H.235 Annex E - Signature Security Profile

- Provides authentication, message integrity and non-repudiation using asymmetric methods like Digital Signatures on every message.
- Application of the GK-routed model is mandatory.
- Digital Signature model introduces improved security.
- Certificates are used to authenticate the user as well as the end-point. Diminishes risk of man-in-the-middle attacks.

H.235 Annex E - Signature Security Profile

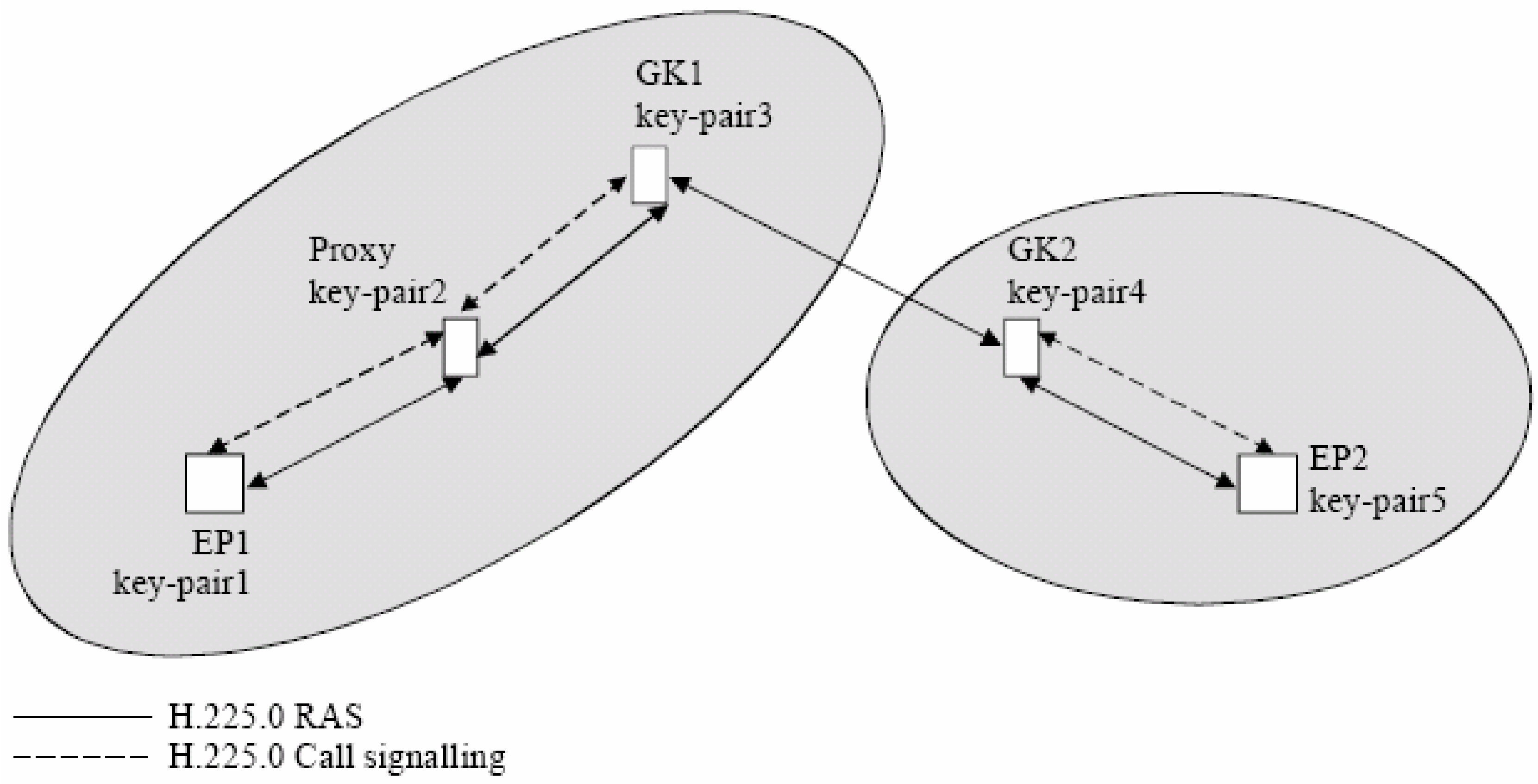


Illustration of public key usage in a gatekeeper routed model

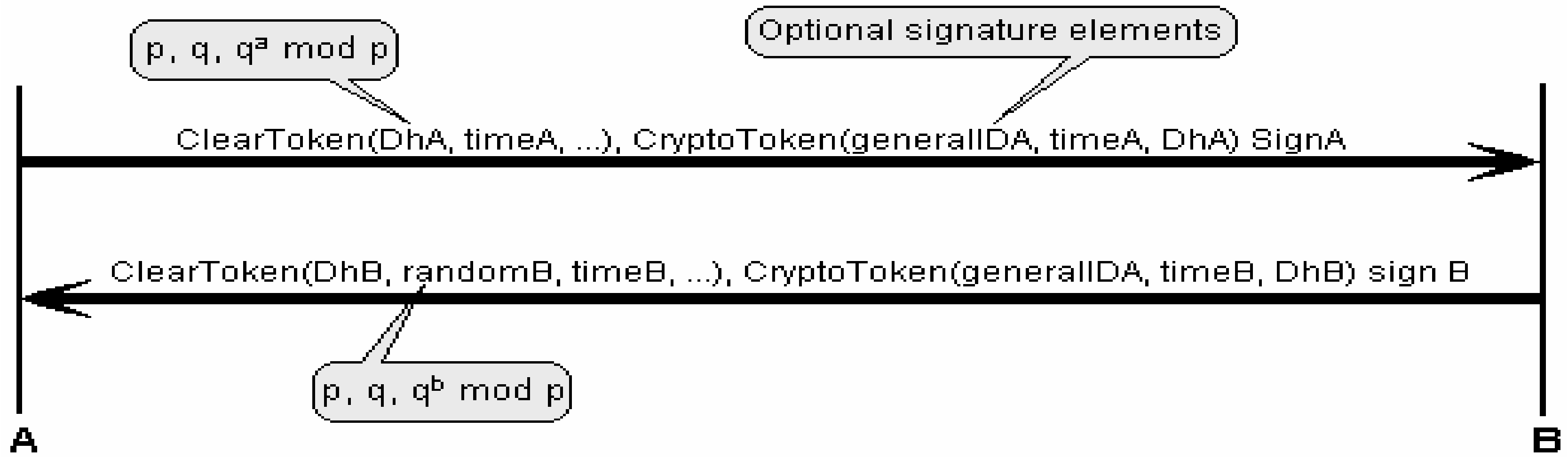
H.235 Annex F - Hybrid Security Profile

- Hybrid of Annex D and Annex E.
- Relies both on asymmetric and symmetric techniques.
- Certificates and Digital Signatures are used to provide authentication, non-repudiation and message integrity for the first handshake between two entities.
- During this handshake, a shared secret is established, used further the same way described for the Baseline Security Profile.
- Gatekeeper routed model is mandatory.

H.235 Annex G - SRTP and MIKEY usage

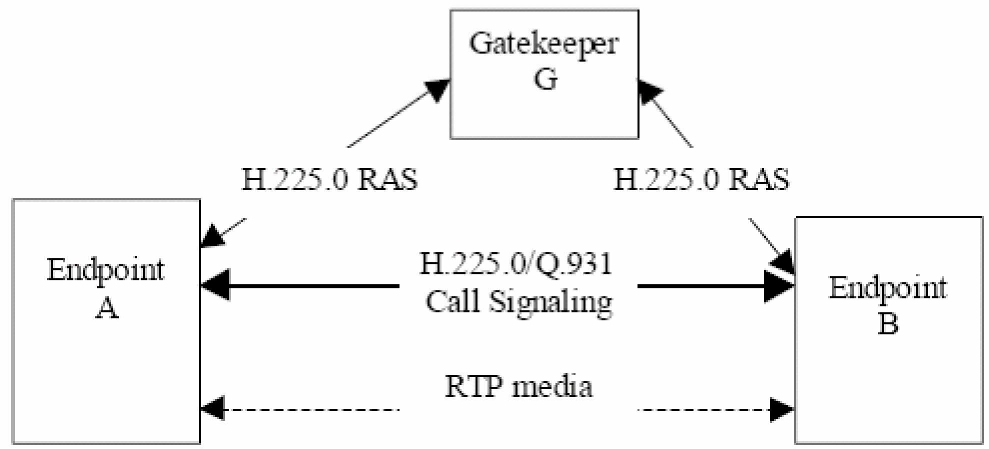
- **Secure Real-time Transport Protocol (SRTP)** : provides confidentiality, message authentication and replay protection to the RTP/RTCP traffic. It ensures a secure media exchange.
- **Multimedia Internet Keying (MIKEY)** : SRTP does not define key management by itself. Preferred key management solution is MIKEY.
  - Addresses real-time multimedia scenarios like SIP calls and SRTP sessions, streaming, unicast, groups, multicast.
  - Defines three options for the user authentication and negotiation of the master keys, all as two-way handshakes. They are symmetric key distribution, asymmetric key distribution and Diffie-Hellman key agreement protected by Digital Signatures.

Annex H - RAS Key Management


p, q, q^a mod p
Optional signature elements
ClearToken(DhA, timeA, ...), CryptoToken(generalIDA, timeA, DhA) SignA
ClearToken(DhB, randomB, timeB, ...), CryptoToken(generalIDA, timeB, DhB) sign B
p, q, q^b mod p
A
B

- Discusses key management negotiation during the RAS gatekeeper discovery phase.
- Diffie-Hellman negotiation takes place during the GRQ, GCF (gatekeeper request, gatekeeper confirm) phase using a ClearToken to convey the parameters needed by Diffie-Hellman.
- This negotiation establishes a shared secret between the endpoint and the gatekeeper.

H.235 Annex I - H.235 Annex D for Direct Routed Scenarios

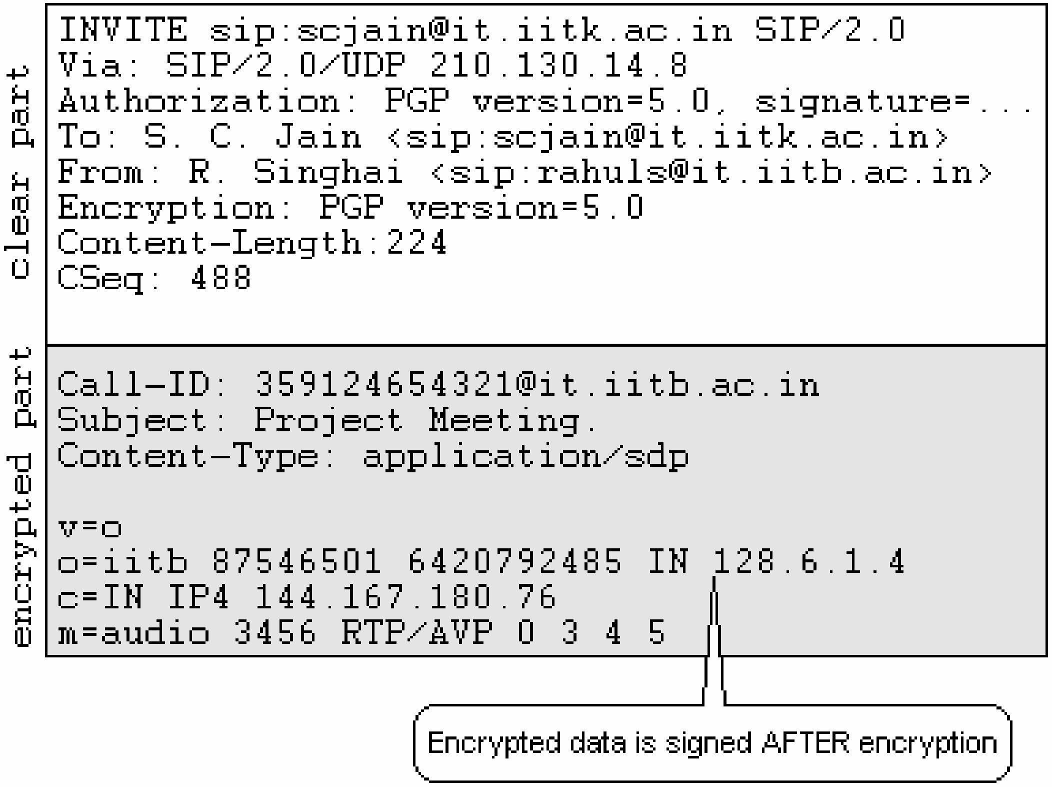


- Applicable to environment where direct routed calls are performed using the gatekeeper for address resolution.
- Gatekeeper serves as key distribution center (KDC), issuing two tokens, one containing the key material secured with the caller's encryption key and the other one secured with the called party encryption key.
- The tokens contain a session key, used for the communication between the two endpoints involved in the call.

SIP Security Concerns

- Message Exchange Security
  - **Requests** : Encryption header field indicates the encryption method in use
  - **Replies** : Sender of the request indicates what key must be used to encrypt the reply.
  - **Authentication** : SIP requests and replies are authenticated using Digital Signature. Authorization header field is used for this purpose. It contains the signature of:
    - the first line (request line or status line)
    - all headers following the Authorization header
    - the message body.

SIP Security Concerns



```
INVITE sip:scjain@it.iitk.ac.in SIP/2.0
Via: SIP/2.0/UDP 210.130.14.8
Authorization: PGP version=5.0, signature=...
To: S. C. Jain <sip:scjain@it.iitk.ac.in>
From: R. Singhai <sip:rahuls@it.iitb.ac.in>
Encryption: PGP version=5.0
Content-Length:224
CSeq: 488

Call-ID: 359124654321@it.iitb.ac.in
Subject: Project Meeting.
Content-Type: application/sdp

v=o
o=iitb 87546501 6420792485 IN 128.6.1.4
c=IN IP4 144.167.180.76
m=audio 3456 RTP/AVP 0 3 4 5
```

Encrypted data is signed AFTER encryption

Message Exchange Security

SIP Security - Transport and Network Layer Security

- Transport or network layer security encrypts signaling traffic guaranteeing message confidentiality and integrity.
- **IPSec** : Provides confidentiality and integrity. User-agents that have a pre-shared keying relationship with their first-hop proxy server are good candidates to use IPSec.
- **TLS** : Provides transport-layer security over connection-oriented protocols. Used when hop-by-hop security is required between hosts with no pre-existing trust association.

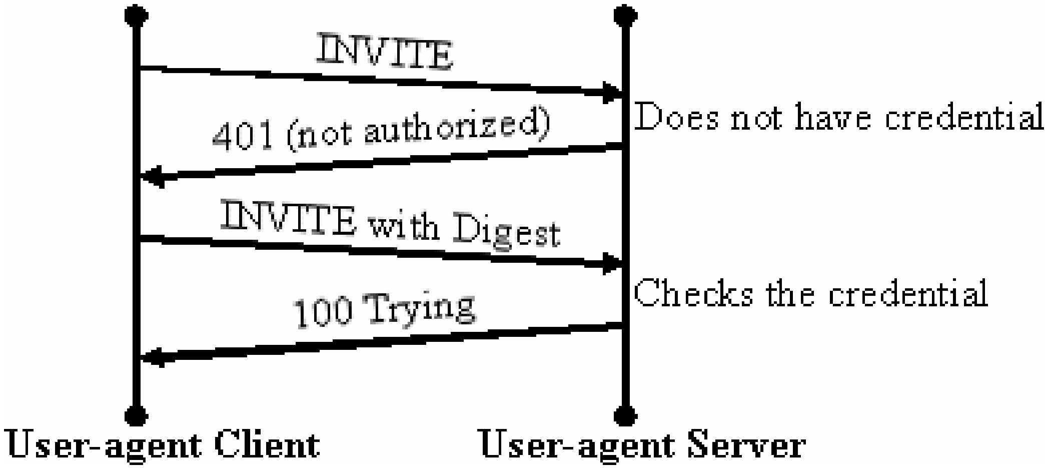
SIP Security – SIPS URI Scheme

- SIPS URI scheme has same syntax as of SIP URI, although the scheme string is “sips” rather than “sip”.
- When used as the Request-URI of a request, it signifies that each hop over which the request is forwarded, until the request reaches the SIP entity responsible for the domain portion of the Request-URI, must be secured with TLS.
- Once it reaches the domain in question it is handled in accordance with local security and routing policy.

SIP Security – HTTP Authentication

- Challenge-response paradigm
- SIP uses HTTP Digest authentication, but *Basic method* of http (user name and password in clear text) is not allowed in SIP
- Any time a proxy or UA receives a message, it may challenge the initiator of the request to provide assurance of its identity
- UAS uses 401 (not authorized) and proxy uses 407 (proxy authentication required) to challenge the initiator

SIP Security – HTTP Authentication



- UAS should not challenge two requests :
  - ACK : Does not have a response.
  - CANCEL : Can not be resubmitted. Generally accepted by a server if it comes from the same hop that sent the request.

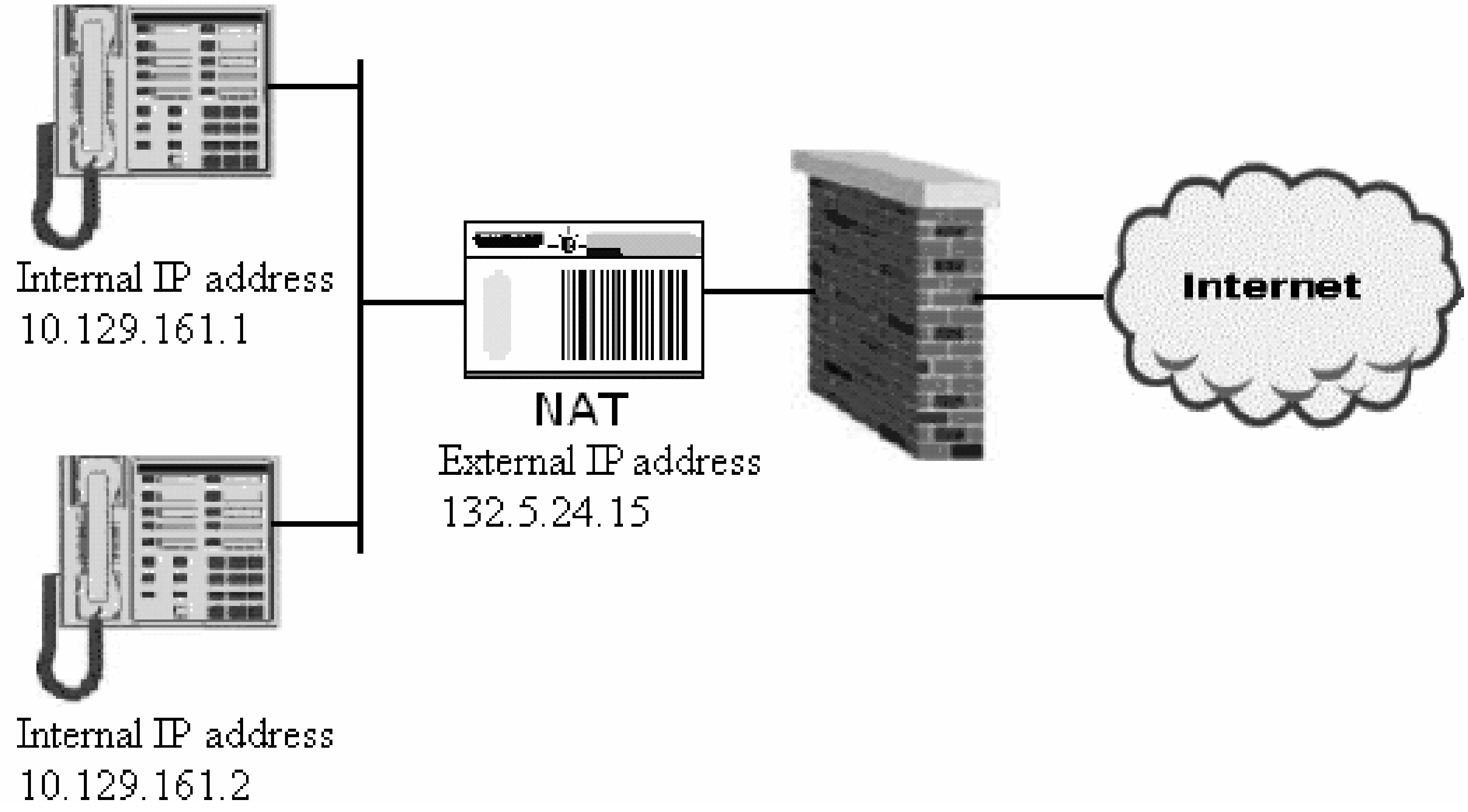
SIP Security – S/MIME

- SIP uses S/MIME to enhance security of the MIME bodies carried by the SIP.
- MIME contains components to provide integrity and encryption for MIME data.
- S/MIME is used for authentication, message integrity, non-repudiation of origin, privacy and end-to-end data security.
- S/MIME certificate is used to identify an end-user and to assert that the holder is identified by an end-user address.
- The certificate also contains the key that is used to sign or encrypt bodies of SIP messages.
- Bodies are signed with the private key of the sender, but bodies are encrypted with the public key of the intended recipient.

Firewall / NAT Issues

- Firewall :
  - Provides a central location for deploying security policies.
  - Relieves end points of maintaining security policies.
- NAT :
  - Used to hide internal network addresses.
  - Enables several endpoints in the network to share the same external address.
  - Makes internal IP addresses less accessible.
  - Attack against the network need be focused only at NAT.

Firewall / NAT Issues



IP Telephones behind NAT and Firewall

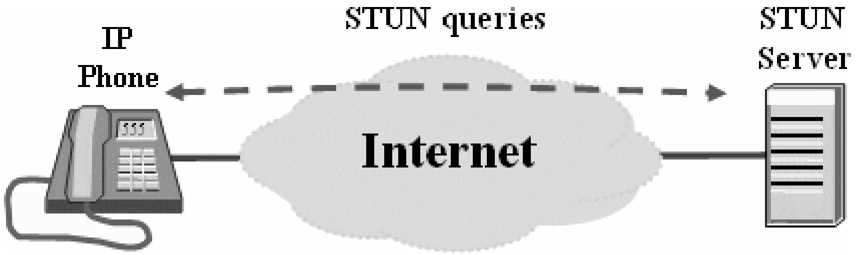
Firewall / NAT Issues

- Firewall issues :
  - RTP ports used by VOIP are dynamically decided during signaling.
  - Hence firewalls cannot statically open the ports.
  - Opening all the RTP ports is not good.
- NAT issues :
  - The IP address and port information is carried in the payload.
  - Since NAT translates the IP address only in the IP header, once H323 / SIP messages traverse a NAT, the IP address would not be valid.

Firewall / NAT Solutions

- Stateful Firewalls :
  - Firewalls made aware dynamically of which ports, media is flowing across and between which terminals.
  - Stateful firewalls open dynamic RTP ports (pinhole) by peeking into the H.323 / SIP signaling messages.
- Proxy placed at the border between two domains
  - Proxy would terminate sessions with both the hosts and relay signaling as well as RTP media streams

Firewall / NAT Issues

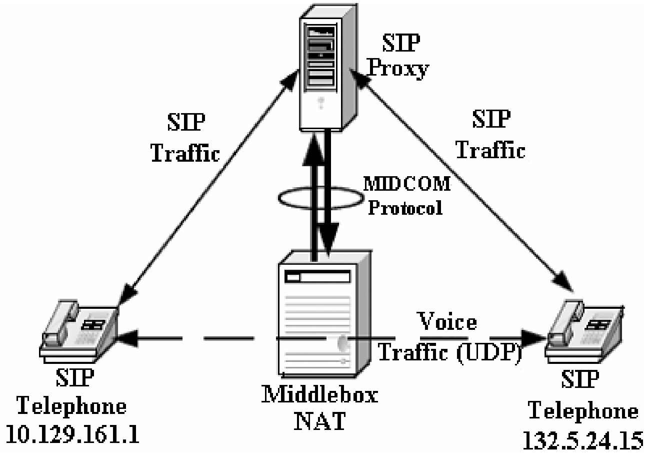


- **Simple Traversal of UDP through NATs (STUN)** :
  - Allows applications to discover
    - Presence and types of NATs and firewalls between them and the public Internet
    - Public Internet Protocol (IP) addresses allocated to them by the NAT.
  - A client-server protocol.
  - A VoIP phone or software package may include a STUN client, which will send a request to a STUN server.
  - The server then reports back to the STUN client what the public IP address of the NAT router is, and what port was opened by the NAT to allow incoming traffic back in to the network.

Firewall / NAT Solutions

- **Traversal Using Relay NAT (TURN)** :
  - Allows for an element behind a NAT or firewall to receive incoming data over TCP or UDP connections.
  - Supports the connection of a user behind a NAT to only a single peer. The connection has to be requested by the TURN client.
  - The TURN server would act as a data relay, receiving data on the address it provides to clients, and forwarding them to the clients.
- **Universal Plug and Play (UPnP)** :
  - In UPnP the NAT is upgraded to support the UPnP protocol
  - Client can query the NAT directly for its external IP Address and Port number.

Call Setup Considerations



- **Application Level Gateway (ALG)** : A firewall with ALG dynamically opens and closes the necessary ports.

- **Middlebox Solutions** : Middlebox-style solutions place an extra device outside the firewall that parses VoIP traffic and instructs the firewall to open or close ports based on the needs of the VoIP signaling.

Conclusion

- VoIP technology is still at the early stage of adoption.
- Attacks against deployments have been largely unheard of or undetected.
- We can expect to see more VoIP application-level attacks occur as attackers become savvier to the technology and gain easier access to test the VoIP infrastructure as it becomes more prevalent across residential areas.
- It will be important to keep track of calls, devices, users, and sessions to enforce security policy and prevent abuse of the VoIP network.
- As we have seen that every security solution comes with a price, both in overhead and monetary terms. Therefore striking a balance between security and the business needs of the organization is key to the success of the VoIP deployment.
- It will be important to prevent these as-yet-undiscovered vulnerabilities from being exploited by enforcing selective conformance of VoIP protocols to their specifications.