VoIP: Voice over Internet Protocol

Le nuove frontiere delle telecomunicazioni su Internet

La tecnologia, l'implementazione, la sicurezza

a cura dell'**Ing. Francesco Amendola** – Nextel Italia s.r.l.

Profilo del relatore

Francesco Amendola è laureato in Ingegneria Elettronica con Lode presso l'Università degli Studi di Roma Tre ed è un laureato del Collegio Universitario "Lamaro-Pozzani".

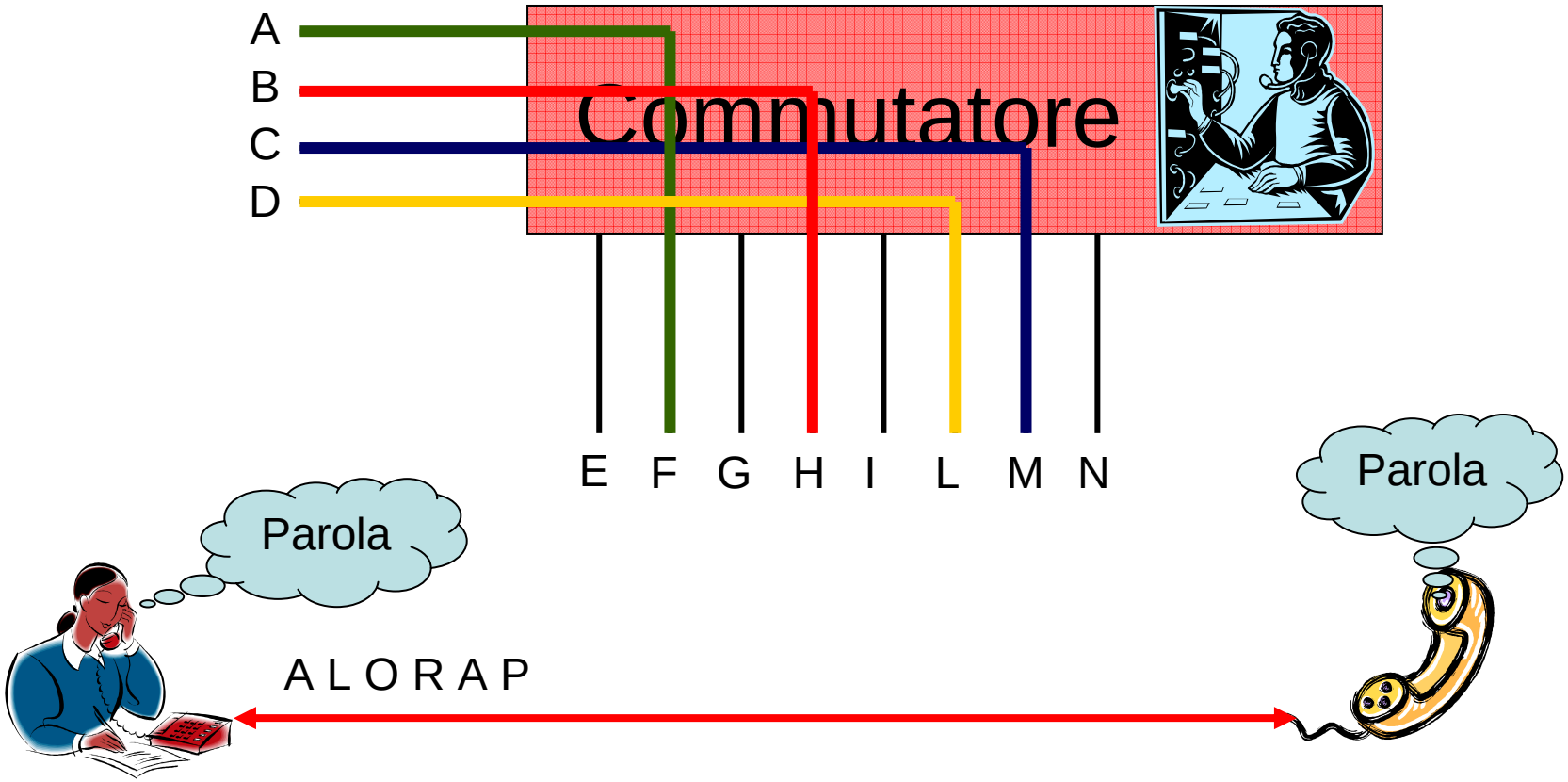
Attualmente ricopre la carica di *IT Security Specialist* all'interno della Nextel Italia s.r.l. – www.nextel.it – società romana di telecomunicazioni, specializzata nella progettazione di sistemi VoIP.

Gestisce anche un sito personale all'indirizzo www.ingamendola.com, dove sono disponibili articoli e presentazioni in materia di sicurezza informatica e protezione dei dati personali.

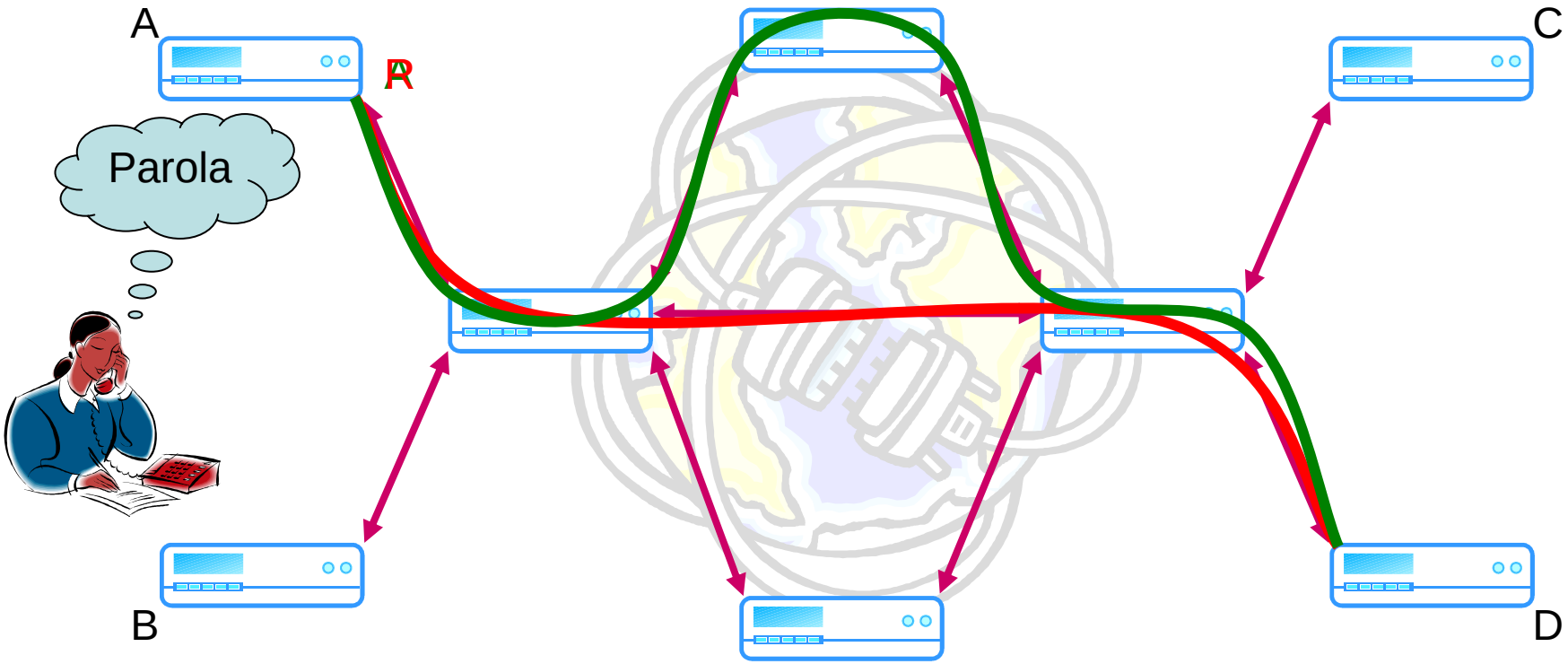
Sommario

1. Introduzione
2. Stato dell'arte della tecnologia
3. Contesto di riferimento in Italia
4. Implementazione di soluzioni VoIP
5. Sicurezza delle comunicazioni
6. Riferimenti bibliografici e sitografici

Telefonia tradizionale a commutazione di circuito



VoIP: comunicazione su reti a commutazione di pacchetto



VoIP: comunicazione su reti a commutazione di pacchetto

Vantaggi

- Il canale trasmissivo non è riservato per tutta la durata della comunicazione
- In assenza di comunicazione le risorse di rete non vengono impegnate
- Il numero di trasmissioni contemporanee non dipende dal numero dei canali fisici

Svantaggi

- Non è semplice gestire l'ordine d'arrivo ed il ritardo dei pacchetti trasmessi
- All'aumentare del numero di trasmissioni contemporanee aumenta il ritardo
- Aumenta la quantità dei dati trasmessi, in quanto occorre aggiungere informazioni per l'instradamento su ogni singolo pacchetto

VoIP: comunicazione su reti a commutazione di pacchetto

Problematiche nella trasmissione della voce su reti IP

- Le reti IP non sono ottimizzate per trasmissioni di informazioni in tempo reale
- IPv4 non supporta in maniera nativa la Quality of Service (QoS)
- Non è sufficiente collegare l'apparecchio VoIP alla rete IP per farlo funzionare correttamente, come avviene per gli apparati telefonici tradizionali
- In caso di mancanza di alimentazione elettrica, occorre alimentare i dispositivi in maniera alternativa
- Le comunicazione sono intercettabili con maggiore semplicità per l'assenza di un canale fisico dedicato e riservato
- Non è di fatto possibile identificare l'origine geografica delle chiamate

VoIP: comunicazione su reti a commutazione di pacchetto

La trasmissione della voce su reti IP, quale è Internet, consente:

- la riduzione dei costi delle conversazioni fino all'annullamento
- la riduzione dei costi di cablaggio e la semplificazione delle procedure di amministrazione, grazie alla convergenza voce-dati
- l'integrazione con altri servizi di comunicazione basati su IP (es. e-mail)
- la convergenza dei servizi e delle applicazioni (es. MoIP – Multimedia over IP)
- il delinearsi di nuovi scenari di comunicazione per la flessibilità di implementazione
- l'implementazione di nuovi servizi a valore aggiunto (VAS), quali Instant Messaging e servizi di presenza
- l'apertura verso tutte le tecnologie di comunicazione, presenti e future (es. Wi-Fi, Wi-MAX)

Sommario

1. Introduzione
2. Stato dell'arte della tecnologia
3. Contesto di riferimento in Italia
4. Implementazione di soluzioni VoIP
5. Sicurezza delle comunicazioni
6. Riferimenti bibliografici e sitografici

Protocolli VoIP a livello applicativo

SIP *(Session Initiation Protocol)*	H.323 *(Packet-based multimedia communications systems)*
IETF – RFC3261	ITU-T
Standard aperto all'interoperabilità, non definito integralmente per tutti i servizi	Ombrello che definisce un sistema completo di protocolli per tutti i servizi
Codifica ASCII, analogo ad HTTP, più semplice il debug	Codifica binaria, richiede minore banda ma non è direttamente intelligibile
Modulare: flessibile e scalabile, anche su larga scala	Monolitico: maggiore integrazione tra i servizi, preferibilmente in ambito LAN
Implementazione più semplice	Maggiore complessità implementativa
Espandibile con funzionalità non previste	Espansione richiede soluzioni proprietarie
Va diffondendosi sempre di più (3gpp)	Molto diffuso alle origini del VoIP

SIP: Session Initiation Protocol definizione

- Il SIP (RFC3261) è un protocollo di segnalazione a livello applicativo ideato per la creazione, la modifica e la terminazione di sessioni che prevedono lo scambio di informazioni tra più parti. Le sessioni possono includere conversazioni telefoniche su reti IP, distribuzione di contenuti multimediali, conferenze multimediali etc.
- Vengono utilizzati dei Proxy Server per instradare correttamente le comunicazioni verso i destinatari, per autenticare ed autorizzare gli utenti, per la gestione delle politiche di routing e per offrire servizi agli utenti
- Gli utenti possono registrarsi ai Registrar Server per comunicare le informazioni utili alla loro localizzazione su IP

SIP: Session Initiation Protocol nelle sue 5 fasi fondamentali

1. Raggiungibilità dell'utente: informazioni per poter raggiungere l'utenza SIP collegata ad una rete IP
2. Disponibilità dell'utente: informazioni circa l'intenzione dell'utenza chiamata di accettare la comunicazione
3. Capacità dell'utenza: informazioni sulle risorse disponibili per instaurare la comunicazione tra le parti
4. Avvio della sessione: la sessione viene stabilita tra le due parti
5. Gestione della sessione: possibilità di trasferire o modificare una sessione attiva o di modificarne i parametri costitutivi o di richiamare ulteriori servizi

SIP: Session Initiation Protocol architettura

- **User Agent (UA)**: entità logica composta da una parte client *(UAC)* che genera richieste SIP e da una parte server *(UAS)* che gestisce le richieste SIP ad essa pervenute
- **Registrar Server**: gestisce la registrazione degli UA, anche con binding multipli, ed inoltra al **Location Server** le informazioni per raggiungere lo UA collegato ad una rete IP
- **Redirect Server**: fornisce al chiamante le informazioni sul destinatario della comunicazione, utili per riuscire a contattarlo
- **Proxy Server**: ha il compito primario di instradare le chiamate, ma anche di autenticare e autorizzare il chiamante

SIP: Session Initiation Protocol architettura

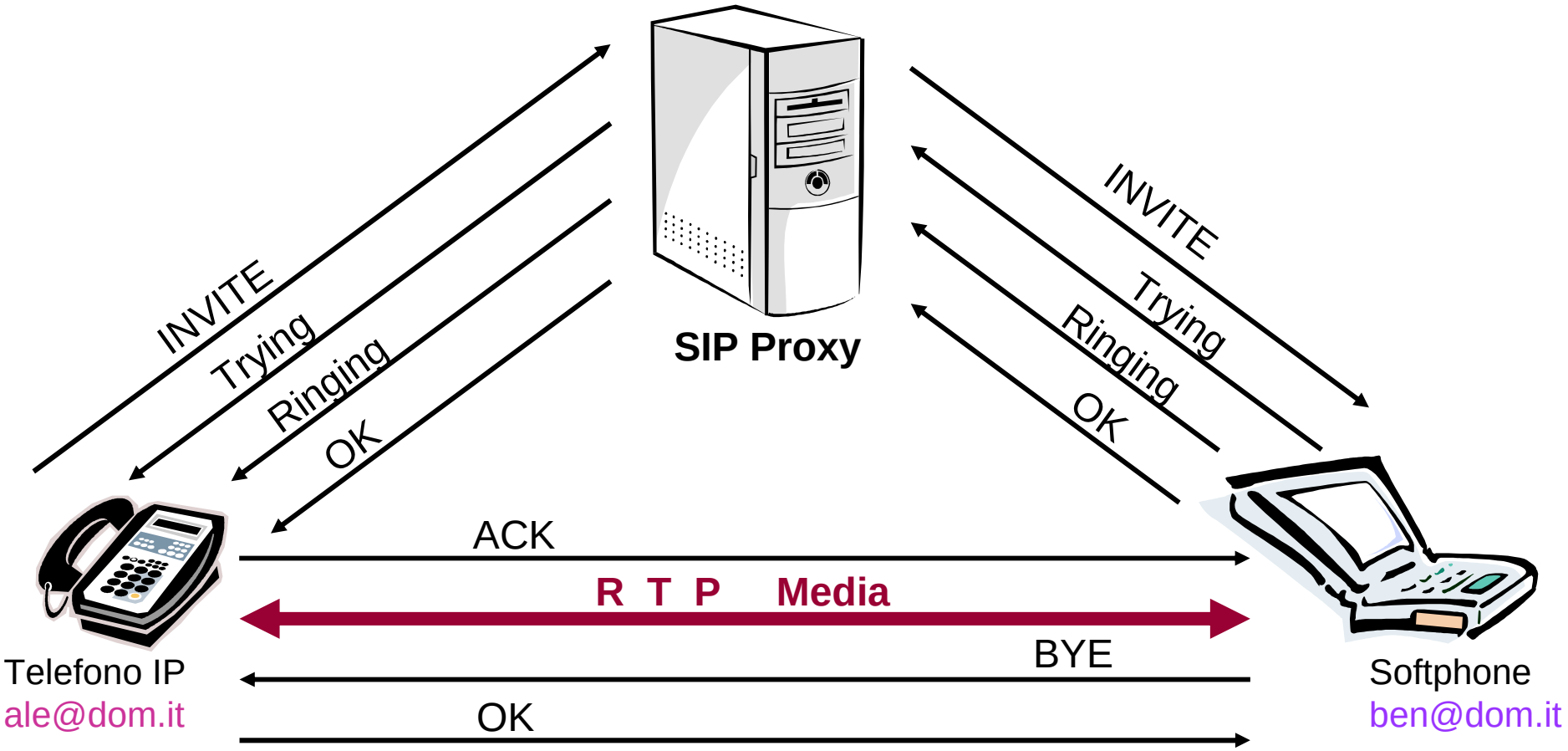
- **B2B-UA (Back-to-Back User Agent)**: entità logica che agisce contemporaneamente da UAC e UAS, nel senso che riceve richieste da un lato e dall'altro le inoltra al destinatario, opportunamente modificate
- **SIP URI (Uniform Resource Identifier)**: contiene le informazioni per identificare le parti coinvolte nella comunicazione. Ha lo stesso formato delle email: nomeutente@dominio.tld
- **SDP (Session Description Protocol)**: RFC2327, descrive il contenuto multimediale di una sessione
- **RTP (Real-time Transport Protocol)**: RFC3550, permette il trasporto in tempo reale delle informazioni *end-to-end*, con un riscontro sulla QoS

SIP: Session Initiation Protocol richieste (metodi) e risposte

- **INVITE**: invito rivolto al destinatario ad iniziare una sessione
- **ACK** (acknowledge): riscontro del completamento di una richiesta
- **BYE**: chiusura della sessione da parte di un partecipante
- **CANCEL**: per annullare una sessione non ancora instaurata completamente
- **REGISTER**: registrazione ad un Registrar Server
- **OPTION**: verifica le capacità di un elemento SIP (es. metodi supportati, codec)

- **Trying (100)**: la richiesta è stata ricevuta e ne è stato dato seguito
- **Ringing (180)**: il destinatario segnala di aver ricevuto l'INVITE
- **OK (200)**: la richiesta è stata completata con successo

SIP: Session Initiation Protocol architettura



SIP: messaggio INVITE da ale@dom.it a ben@dom.it

```
INVITE sip:ben@dom.it SIP/2.0
    Via: SIP/2.0/UDP sipproxy.dom.it;branch=z9hG4bK776asdhds
    Max-Forwards: 70
    To: Ben <sip:ben@dom.it>
    From: Ale <sip:ale@dom.it>;tag=1928301774
    Call-ID: a84b4c76e66710@sipproxy.dom.it
    CSeq: 314159 INVITE
    Contact: <sip:alice@sipproxy.dom.it>
    Content-Type: application/sdp
    Content-Length: 142
```

SIP: tracciamento catturato con Ethereal

demo_sip.cap - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: sip | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.35.81	217.72.100.4	SIP	Request: REGISTER sip:217.72.100.4
2	0.067453	217.72.100.4	192.168.35.81	SIP	Status: 401 Unauthorized (0 bindings)
3	0.083736	192.168.35.81	217.72.100.4	SIP	Request: REGISTER sip:217.72.100.4
4	0.166129	217.72.100.4	192.168.35.81	SIP	Status: 200 OK (1 bindings)
5	94.457500	192.168.35.81	217.72.100.4	SIP/SD	Request: INVITE sip:0640043101@217.72.100.4, with session descriptio
6	94.548653	217.72.100.4	192.168.35.81	SIP	Status: 100 trying -- your call is important to us
7	94.548883	217.72.100.4	192.168.35.81	SIP	Status: 401 Unauthorized
8	94.561707	192.168.35.81	217.72.100.4	SIP	Request: ACK sip:0640043101@217.72.100.4
9	94.566235	192.168.35.81	217.72.100.4	SIP/SD	Request: INVITE sip:0640043101@217.72.100.4, with session descriptio
10	94.657258	217.72.100.4	192.168.35.81	SIP	Status: 100 trying -- your call is important to us
11	94.962651	217.72.100.4	192.168.35.81	SIP	Status: 180 Ringing
12	99.651406	217.72.100.4	192.168.35.81	SIP/SD	Status: 200 OK, with session description
13	99.657070	192.168.35.81	217.72.100.4	SIP	Request: ACK sip:217.72.100.4;ftag=1184306921239
14	106.454307	192.168.35.81	217.72.100.4	SIP	Request: BYE sip:217.72.100.4;ftag=1184306921239
15	106.533121	217.72.100.4	192.168.35.81	SIP	Status: 200 OK

```
⊞ Frame 1 (471 bytes on wire, 471 bytes captured)
⊞ Ethernet II, Src: AniCommu_c9:44:c2 (00:40:05:c9:44:c2), Dst: SmcNetwo_9b:3c:20 (00:04:e2:9b:3c:20)
⊞ Internet Protocol, Src: 192.168.35.81 (192.168.35.81), Dst: 217.72.100.4 (217.72.100.4)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol
```

Dispositivi di comunicazione basati su IP a standard SIP

Telefono IP

Video-telefono IP

Dispositivi di comunicazione basati su IP a standard SIP

ATA (Analogue Telephone Adaptor)

PC Softphone

Dispositivi di comunicazione basati su IP a standard SIP

Palmari - PDA

Cordless Wi-Fi

Cellulare Dual-Mode Wi-Fi

Codifica dei flussi multimediali su RTP

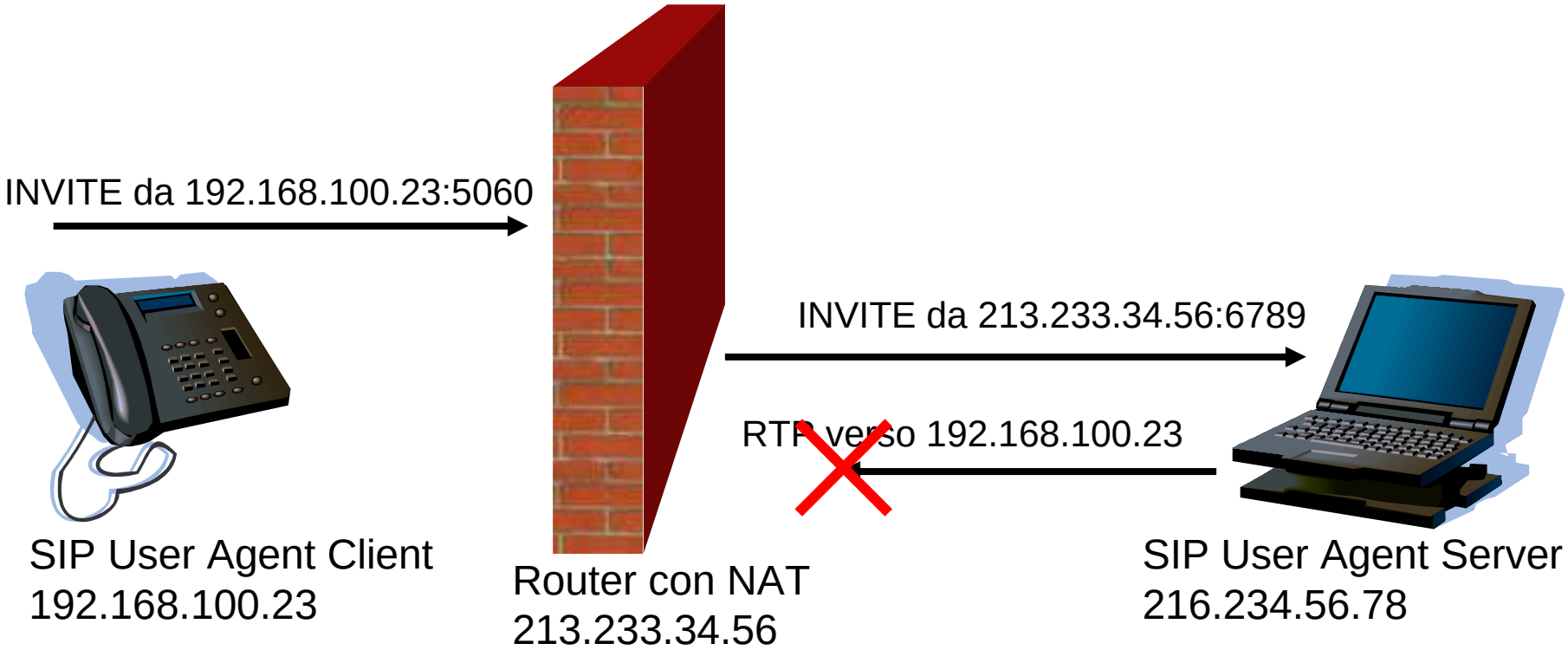
- **Codifica della voce**
  - G.711 (A-law): PCM 64kbps, richiede circa 90 kbps di banda lorda
  - G.729 (Annex A): codifica 8 kbps, richiede circa 30 kbps di banda

  Il G.711 è uno standard ITU-T liberamente implementabile; G.729 invece è sotto brevetto

- **Codifica del video**
  - H.264 (AVC): MPEG-4, richiede almeno 64 kbps di banda lorda

- **Codifica dei FAX**
  - T.38 (FoIP): ottimizzato per l'invio dei FAX su IP, con 90 kbps di banda lorda

NAT Traversal: problema di attraversamento del NAT



Lo UAS può rispondere alla segnalazione correttamente ma le informazioni sulla fonia, presenti all'interno della Session Description dell'INVITE, non vengono tradotte dal router e quindi presentano l'indirizzo privato dello UAC

NAT Traversal: soluzione con STUN Server

- **STUN** (Simple Traversal of UDP through NAT): soluzione che prevede un Server esterno alla rete dello UA
- Lo UA è configurato per connettersi allo Stun Server prima di iniziare una sessione SIP e di generare traffico verso questi
- Lo Stun Server, analizzando i pacchetti IP provenienti dallo UA tradotti dal router, ne deduce informazioni circa l'indirizzo pubblico del router e la porta assegnata allo UA per instaurare connessioni verso l'esterno
- Quindi lo Stun Server comunica quanto appreso allo UA, in modo che possa inserire le giuste informazioni nella SD della sua segnalazione
- Problemi se il NAT è di tipo simmetrico o se si utilizza il TCP

NAT Traversal: soluzione con TURN Server

- **TURN** (Traversal Using Relay NAT): soluzione simile allo STUN, utilizza un Server esterno, e risolve i problemi con il NAT simmetrico
- A differenza dello Stun Server, il Turn Server è il destinatario del flusso multimediale RTP originato dallo UA
- Sarà poi il Turn Server ad inoltrare lo stream RTP allo UA destinatario della conversazione
- In questo modo il destinatario della segnalazione Stun è il medesimo del flusso RTP, e dunque anche in presenza di NAT simmetrici il router non varierà la porta associata allo UA originante il traffico collegato nella rete LAN

NAT Traversal: soluzione con B2B-UA

- **B2B-UA** (Back-to-Back User Agent): gli UA posti dietro il NAT si registrano ad un B2B-UA
- Il B2B-UA ha funzioni di Proxy sia per la segnalazione SIP che per il flusso di dati RTP
- In questo modo ciascuno dei soggetti coinvolti nella comunicazione dialoga direttamente con il B2B-UA, vedendolo come il proprio interlocutore
- Il B2B-UA non richiede alcuna tecnologia implementata sugli UA, in quanto è sufficiente che ogni terminale IP abbia configurato come default outbound proxy proprio il B2B-UA

NAT Traversal: soluzione con UPnP

- **UPnP** (Universal Plug 'n Play): tecnologia che permette ai dispositivi collegati in rete di connettersi tra di loro automaticamente, senza il supporto di un amministratore
- In ambito VoIP l'UPnP permette al SIP User Agent di scoprire in automatico la configurazione del router, in particolare il tipo di NAT e dunque l'indirizzo IP pubblico dell'interfaccia WAN e la porta assegnatagli
- In questo modo lo UA inserirà nella Session Description le informazioni di connettività pubblica del router e non le sue private, consentendo all'altro UA di instaurare correttamente il flusso multimediale

NAT Traversal: soluzione con ALG

- **ALG** (Application Layer Gateway): tecnologia che permette ai router che ne sono dotati di analizzare il traffico e riconoscere la segnalazione SIP che instaura la sessione
- I dispositivi che adottano ALG sono in grado di modificare il contenuto dei pacchetti SIP in modo da inserire le corrette informazioni di connettività
- In questo modo non sarà lo UA a doversi preoccupare di fornire le informazioni per l'instradamento, ma sarà direttamente il router ad inserire il suo indirizzo pubblico e la porta che intende assegnare allo UA per il flusso multimediale all'interno della segnalazione SIP/SDP

QoS – Quality of Service

- Problemi su latenza, jitter, eco, perdita di pacchetti, saturazione della banda
- 802.1p: aggiunge 3 bit a livello data-link per definire 8 differenti livelli di priorità. E' solitamente utilizzato in congiunzione con 802.1q per la definizione di VLAN
- RSVP (Resource reSerVation Protocol): protocollo utilizzato per riservare le risorse di rete desiderate. Le risorse richieste, se disponibili, sono riservate su tutti i nodi che vengono attraversati dal flusso di dati. E' poco scalabile su reti di grandi dimensioni.
- DiffServ (Differentiated Services DiffServ): utilizza il campo ToS (Type of Service) dell'header del datagramma IP per codificare 64 livelli di priorità su ogni singolo pacchetto. Non è richiesto ai router di tenere traccia dell'intero flusso

Il caso Skype

- Milioni di utenti nel mondo, molto diffuso perché non ha costi relativamente ai servizi di base ed è semplicissimo da configurare ed utilizzare
- Sistema chiuso, con protocolli proprietari
- Non è interoperabile con il SIP
- Il codice sorgente non è pubblico
- Le tariffe ed i costi di gestione non sono sempre inferiori rispetto ad altri servizi VoIP basati sul SIP
- I servizi sono limitati solamente a quelli offerti dal produttore
- L'implementazione è controllata dal produttore

Sommario

1. Introduzione
2. Stato dell'arte della tecnologia
3. Contesto di riferimento in Italia
4. Implementazione di soluzioni VoIP
5. Sicurezza delle comunicazioni
6. Riferimenti bibliografici e sitografici

Contesto di riferimento in Italia

Contesto normativo: Delibera AGCOM n.11/06/CIR

- Disposizioni regolamentari per la fornitura di servizi VoIP *(Voice over Internet Protocol)* e integrazione del piano nazionale di numerazione
- L'Autorità per le garanzie nelle comunicazioni ha adottato tra le prime in Europa una disciplina organica per i servizi di telefonia via Internet
- Il provvedimento disciplina i servizi geografici VoIP ed i servizi di comunicazione vocale "nomadici"
- Servizio nomadico: servizio che consente all'utente, identificato da uno stesso numero non geografico del piano nazionale di numerazione e/o altro identificativo, di originare e ricevere comunicazioni vocali nazionali, internazionali, da un qualsiasi punto terminale di rete

Contesto di riferimento in Italia

Contesto normativo: Delibera n.11/06/CIR

- I servizi "nomadici" rappresentano la novità di maggior rilievo nell'ambito delle comunicazioni su IP, rispetto ai servizi telefonici tradizionali
- Consentono di telefonare e di ricevere telefonate, con lo stesso numero o identificativo, a prescindere dal luogo in cui ci si trova, necessitando solo di un accesso ad Internet
- Ad esempio permettono ad un utente che si sposta sulle varie sedi della sua società, in Italia così come nel mondo, di essere raggiungibile sempre tramite il proprio numero personale, senza che il chiamante sappia dove si trovi fisicamente il chiamato

Contesto di riferimento in Italia

Contesto normativo: Delibera n.11/06/CIR

- Si distinguono due tipologie di servizio accessibili al pubblico
  - servizi telefonici forniti da postazione fissa o comunque con numerazione geografica
  - servizi di comunicazione vocale nomadici
- Servizi con numerazione geografica
  - utilizzano il piano di numerazione esistente
  - es. 06 12345678
- Servizi nomadici
  - viene introdotta una nuova numerazione ad hoc
  - 55 XXXXXXXX

Contesto di riferimento in Italia

Contesto normativo: servizi con numerazione geografica

- Gli utenti che hanno sottoscritto il servizio devono avere la possibilità di effettuare e ricevere chiamate dagli utenti di tutte le reti di comunicazione elettronica, nazionali ed estere, ivi incluse le reti di comunicazioni mobili e personali, tramite numeri che figurano in un piano nazionale o internazionale di numerazione
- L'utilizzo nomadico del servizio è consentito esclusivamente nell'ambito distrettuale. L'utente deve essere preventivamente informato in merito al divieto dell'utilizzo nomadico al di fuori del distretto e tale limitazione è sottoposta alla specifica accettazione da parte dell'utente
- È garantita la portabilità del numero tra gli operatori

Contesto di riferimento in Italia

Contesto normativo: servizi di comunicazione nomadici

- Il costo massimo di una chiamata verso le numerazione nomadiche in decade 5 è pari a quello di una chiamata diretta ad una numerazione geografica, per servizi equivalenti, secondo il piano tariffario sottoscritto dal cliente
- Nel caso in cui il piano tariffario sottoscritto preveda la distinzione tra chiamate locali e interurbane, il costo massimo è pari a due volte il prezzo delle chiamate locali verso numerazione geografica
- La numerazione nomadica in decade 5 non può essere utilizzata per la fornitura di servizi a sovrapprezzo
- È garantita la portabilità del numero nell'ambito della stessa decade

Contesto di riferimento in Italia

Contesto normativo: erogazione dei servizi VoIP

- Sia per l'erogazione dei servizi con numerazione geografica che per quelli nomadici, devono essere altresì garantiti l'accesso ai servizi d'emergenza, l'integrità della rete, l'identificazione della linea chiamante, le prestazioni ai fini di giustizia (*Lawful Interception*)
- Relativamente ai soli servizi nomadici, è sempre associata nei sistemi informativi dell'operatore l'informazione riguardo al domicilio del cliente, utilizzato ai fini della sottoscrizione del servizio stesso e della fatturazione
- Gli operatori devono contribuire alla realizzazione di una base dati unica e definire le modalità di inserimento negli elenchi telefonici generali

Contesto normativo: chiamate di emergenza

- I soggetti autorizzati a fornire i servizi VoIP devono fornire anche l'accesso ai servizi di emergenza
- Le informazioni relative all'ubicazione del chiamante devono essere messe a disposizione delle autorità incaricate dei servizi di soccorso e di protezione civile nella misura in cui sia tecnicamente fattibile
- Le eventuali limitazioni nella fornitura delle informazioni relative all'ubicazione del chiamante devono essere oggetto di accurata informativa all'utente, preventiva alla sottoscrizione dell'offerta commerciale e soggetta a specifica accettazione da parte dell'utente stesso

Contesto normativo: interoperabilità

- Gli operatori titolari dell'autorizzazione generale per la fornitura di servizi VoIP hanno l'obbligo:
  - di negoziare tra loro l'interconnessione nella modalità più efficiente sul piano tecnologico ed economico, consentendo la piena interoperabilità dei servizi offerti e migliorare la libertà di scelta dell'utente
  - di concedere un accesso alle interfacce tecniche, ai protocolli e ad altre tecnologie indispensabili per l'interoperabilità dei servizi VoIP
  - di utilizzare protocolli standard, ove praticabile sulla base di quanto stabilito dal Codice delle comunicazioni elettroniche relativamente alla normalizzazione

Contesto normativo: interoperabilità

- L'Autorità per le garanzie nelle comunicazioni ha avviato un procedimento istruttorio al fine di stabilire le condizioni tecniche od operative che devono essere soddisfatte, dal fornitore di servizi o dai beneficiari dell'accesso, per l'attuazione degli obblighi di interoperabilità
- Il procedimento istruttorio ha per oggetto le problematiche connesse alla definizione di un insieme comune di standard, protocolli di segnalazione e interfacce tecniche, ai fini dell'interconnessione ed interoperabilità per la fornitura dei servizi di comunicazione VoIP integrata, della codifica dei media e della localizzazione nella fornitura dei servizi di emergenza
- La convergenza è essenziale per la diffusione della tecnologia

Contesto normativo: neutralità tecnologica

- Principio europeo che vede la regolamentazione dei servizi di comunicazione elettronica, e nella fattispecie di quelli di telefonia, non dipendente dalla tecnologia utilizzata per la loro erogazione, ma correlati piuttosto alla tipologia ed alle caratteristiche dei servizi medesimi

- La regolamentazione dei servizi VoIP si propone gli obiettivi generali di:
  - promuovere lo sviluppo in regime di concorrenza delle reti e servizi di comunicazione elettronica, ivi compresi quelli a larga banda
  - garantire la convergenza, la interoperabilità tra reti e servizi di comunicazione elettronica

Contesto normativo: neutralità tecnologica

- La regolamentazione dei servizi VoIP si propone gli obiettivi generali di:
  - garantire l'integrità e la sicurezza delle reti di comunicazione elettronica
  - garantire in modo flessibile l'accesso e l'interconnessione per le reti di comunicazione elettronica a larga banda
  - garantire una gestione efficiente delle risorse di numerazione
  - garantire un elevato livello di protezione dei consumatori nei rapporti con i fornitori dei servizi
- L'interconnessione tra i diversi *player* deve estrinsecarsi nella interoperabilità dei servizi ed in vantaggi per i consumatori

Contesto di riferimento in Italia

Contesto normativo: numerazione e instradamento

- Ad oggi una chiamata originata da una rete VoIP di un operatore e diretta ad un altro operatore VoIP è instradata su rete PSTN, con relativa tariffazione
- Questo perché non è possibile sapere a priori se il destinatario della comunicazione è una utenza VoIP o no
- Inoltre eventualmente occorre sapere come instradare la chiamata direttamente su rete IP fino a raggiungere il destinatario VoIP
- La soluzione è ENUM: tElephone NUmber Mapping (RFC3761)
- ENUM è un insieme di protocolli per unificare telefonia tradizionale e su IP, facendo convergere le diverse metodologie di instradamento

Contesto normativo: ENUM

- Il protocollo ENUM è alla base del sistema che consente una convergenza delle reti e dei servizi, ovvero della rete telefonica con quella IP quale è Internet
- Tale sistema permette di utilizzare il numero telefonico nella sua composizione tradizionale (come definito dalla raccomandazione dell'ITU E.164) per usufruire sia dei classici servizi telefonici sia dei recenti sviluppati su Internet
- Il protocollo ENUM definisce un'associazione tra numeri telefonici E.164 e indirizzi Internet, utilizzando la tecnologia dei DNS (Domain Name System) su database distribuiti per conoscere l'*ubicazione* IP dell'utente

Contesto normativo: ENUM

- L'AGCOM ha indetto una consultazione pubblica sull'introduzione del protocollo ENUM nel 2003
- Dal 2004 è stata attivata la sperimentazione dello User ENUM che ha consentito ai VoIP provider di offrire numeri in decade 6, con l'obiettivo dell'interoperabilità
- Nel 2005 il ministero delle Comunicazioni ha avuto la delega per la gestione del prefisso +39 nel registro ENUM internazionale (e164.arpa)
- Nel 2006 è partita la sperimentazione del Carrier ENUM, che prevede l'interazione degli operatori su un data-base comune a loro riservato in modo da instradare l'intero traffico a destinazione (es. Number Portability)

Contesto di mercato: situazione attuale

- Il mercato delle comunicazioni sta attraversando un momento di evoluzione, sradicando i modelli di business consolidati con la telefonia tradizionale ed aprendosi verso scenari nuovi ed innovativi
- Il fattore trainante non è soltanto la riduzione della spesa telefonica, bensì la possibilità di integrazione dei servizi e delle applicazioni di comunicazione e lo sviluppo di nuove soluzioni di connettività
- VoIP già non significa più soltanto “Voce” su IP: si parla di MoIP (Multimedia over IP) e SoIP (Service over IP) e IMS (IP Multimedia Subsystem)
- Nuovi player si affacciano su un mercato aperto non ancora delineato

Contesto di riferimento in Italia

Contesto di mercato: situazione attuale

- Le prime comunicazioni VoIP sono state offerte al pubblico come estensioni di programmi di Instant Messaging peer-to-peer
- Al momento l'applicazione VoIP più conosciuta e diffusa, soprattutto a livello consumer, è sicuramente Skype
- Skype non sostituisce la linea telefonica tradizionale
- Questa soluzione p2p è sicuramente un mezzo per far in modo che gli utenti si avvicinino a questa nuova tecnologia e ne prendano confidenza senza bruschi cambiamenti o discontinuità
- Una volta acquisita consapevolezza e dimestichezza con il VoIP, un sistema chiuso non sarà più idoneo a soddisfare tutte le richieste

Contesto di mercato: situazione attuale

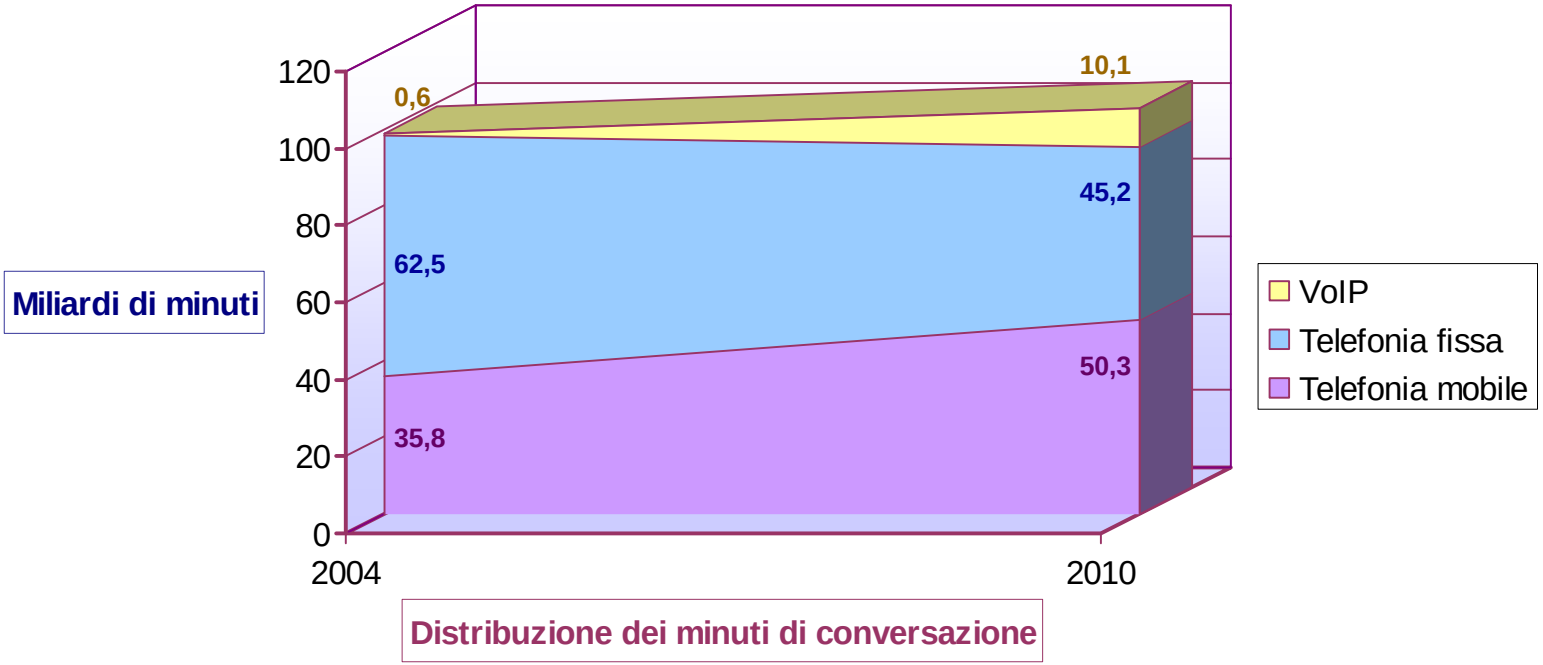
- Le alternative aperte a Skype sono offerte dagli Internet Service Provider, i quali abbinano alle soluzioni di connettività a larga banda offerte (ADSL, HDSL, ADSL2+) la possibilità di effettuare e ricevere chiamate direttamente su IP
- La scarsa diffusione di contratti di fornitura della sola linea dati è sicuramente un freno per il pieno sviluppo delle comunicazioni VoIP pure
- Anche se i tempi non sono ancora maturi per soluzioni full IP, a causa di alcune implementazioni della tecnologia non ancora consolidate (alimentazione, chiamate d'emergenza, etc.), occorre mettere da parte un po' di diffidenza ed iniziare ad utilizzare ordinariamente il VoIP

Contesto di mercato: prospettive future globali

- In futuro non esisterà più una distinzione tra fornitori di telefonia e ISP, in quanto la convergenza dell'infrastruttura e dei servizi porterà al delinearsi di figure *triple player*, cioè in grado di offrire in maniera integrata la trasmissione di voce, video (TV) e dati
- Crescita mondiale: nel 2008 il triplo delle linee VoIP del 2004 (Gartner)
- Le linee VoIP nel mondo erano oltre 25 milioni nel 2005 e se ne prevedono 250 milioni nel 2011 (Idate)
- Si prevede che nel 2007 il 75% del traffico voce transiterà su reti IP (Frost & Sullivan) raggiungendo il 95% nel 2010 (Time Warner Telecom)
- Nel 2010 il giro d'affari generato dal VoIP sarà di 3,3MLD$ (Yankee Grp.)

Contesto di mercato: prospettive future per l'Italia

- Per l'Italia si prevede che nel 2010 il 9% delle telefonate saranno effettuate con tecnologia VoIP (Analysys)



Fonte Analysys

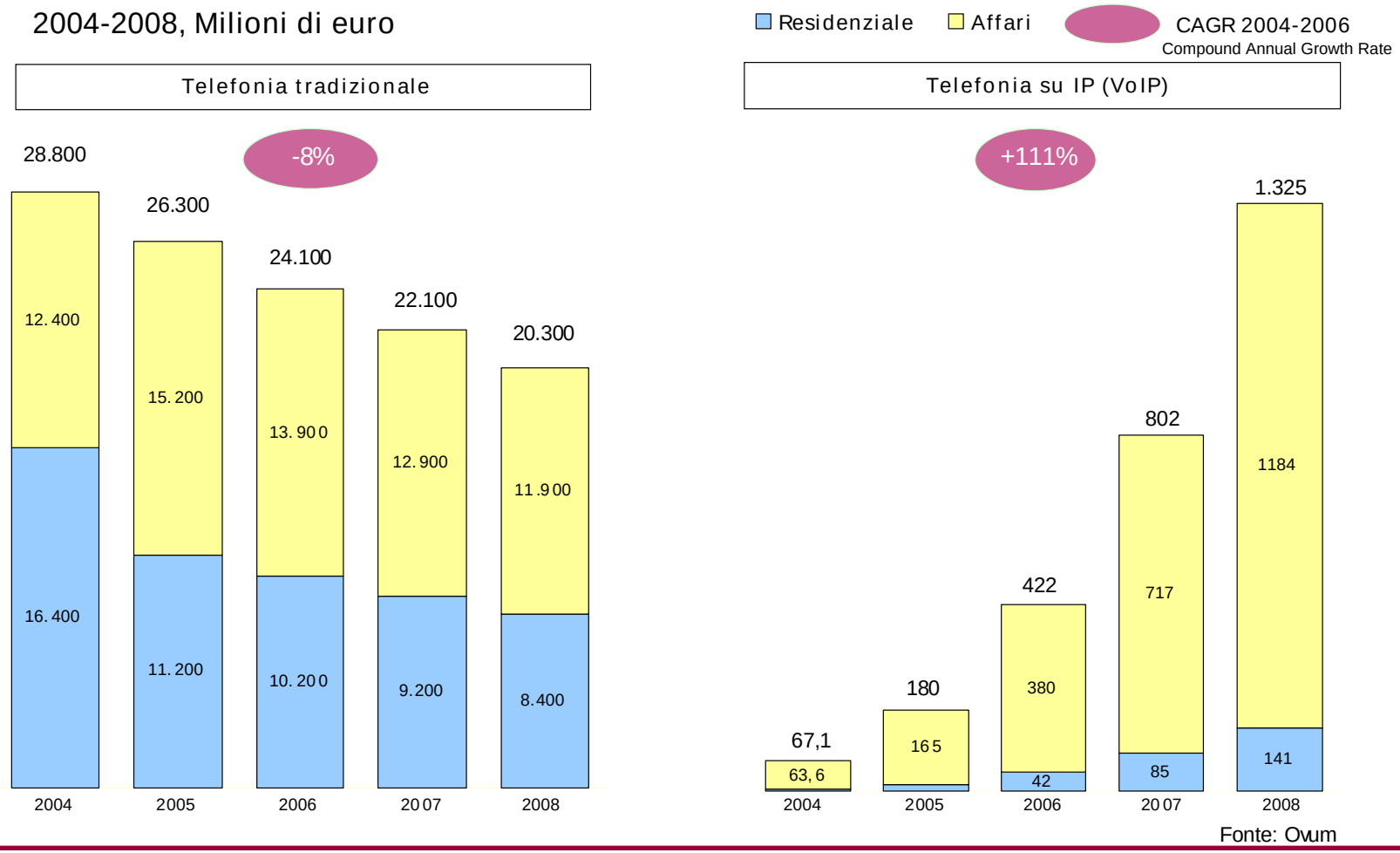
Contesto di mercato: prospettive future per l'Italia

- Nel 2008 si stima che vi sarà una domanda di servizi *double play* (voce e dati integrati) da parte di 2,3 milioni di utenti, contro i 454 mila del 2004
- Inoltre il valore del mercato di servizi *double play* crescerà da 650 a circa 1.600 milioni di euro, con un'incidenza percentuale dal 4 all'8% sul totale del mercato delle telecomunicazioni tradizionali

(Fonte ANFoV-Databank)

- Oggi la fruizione dei servizi VoIP avviene principalmente con sistemi software che richiedono un computer
- Le prospettive di crescita si basano anche su un utilizzo naturale di apparati di comunicazione dedicati basati su IP (es. telefoni IP, IP-PBX)

Contesto di mercato: stima del business in Italia



Sommario

1. Introduzione
2. Stato dell'arte della tecnologia
3. Contesto di riferimento in Italia
4. Implementazione di soluzioni VoIP
5. Sicurezza delle comunicazioni
6. Riferimenti bibliografici e sitografici

Considerazioni preliminari

- A differenza della telefonia tradizionale, nell'implementazione di soluzioni basate sul VoIP vi sono diversi fattori che possono influenzare il corretto funzionamento dell'intero sistema
  - Networking e interconnessione IP
  - Interoperabilità degli apparati
  - Qualità del Servizio
  - Utilizzo da parte dell'utente
  - Gestione e manutenzione
  - Continuità del servizio in caso di mancanza di alimentazione elettrica
  - Affidabilità dei componenti dell'intero sistema

Considerazioni preliminari

- Le soluzioni VoIP per le utenze residenziali sono sostanzialmente diverse da quelle d'interesse per le aziende e le utenze affari
- All'utente residenziale interessa soprattutto risparmiare sulla spesa telefonica ed è anche disposto a tollerare disservizi e malfunzionamenti
- In ambito professionale si è molto meno tolleranti ad eventuali degradi della qualità del servizio, in quanto l'impossibilità di comunicazione nel momento in cui se ne necessita può significare la perdita di business
- Inoltre l'aggiunta di nuovi servizi e funzionalità non è di per sé vantaggiosa se non viene mantenuta la semplicità di utilizzo dell'apparato di comunicazione ai livelli di un attuale apparato telefonico

La qualità della connessione a banda larga

- Fattore chiave per il buon esito di una comunicazione su IP è sicuramente la qualità della connessione ad Internet ADSL(2+) o HDSL
- Al momento non esistono particolari garanzie per l'utente in termini di affidabilità e prestazioni, ovvero di Qualità del Servizio
- L'AGCOM ha appena approvato la "Direttiva in materia di qualità e carte dei servizi di accesso a Internet da postazione fissa" – Delib. 131/06/CSP
- Principali indicatori della QoS: tasso di malfunzionamento e tempi di riparazione, rapporto di concentrazione all'accesso, banda media nazionale ed internazionale, velocità di trasmissione dati, tasso di insuccesso nella trasmissione dati, ritardo di trasmissione dati

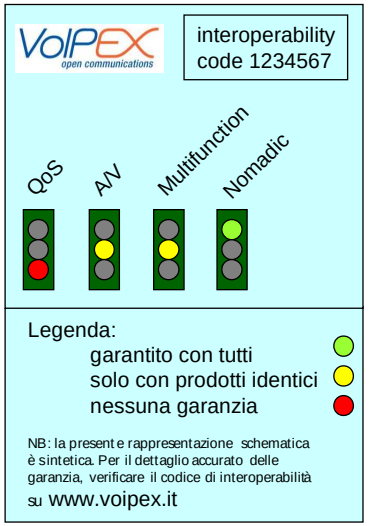
La qualità della connessione a banda larga

- Nel valutare su carta la bontà di una connessione broad band al momento si considera solo la banda minima garantita, unico dato relativo alla QoS presente nei valori di targa di una connessione di qualità
- Non sempre sono disponibili da parte del provider informazioni circa la latenza media della rete, il tipo di connessione (Interleaved o Fast) ed altri parametri tecnici a garanzia della bontà del collegamento
- Infine l'impiego di parametri puramente tecnici non consente certamente all'utente di comprendere a pieno le caratteristiche della connessione e dunque non lo aiuta a scegliere la soluzione più adatta per le sue esigenze di comunicazione

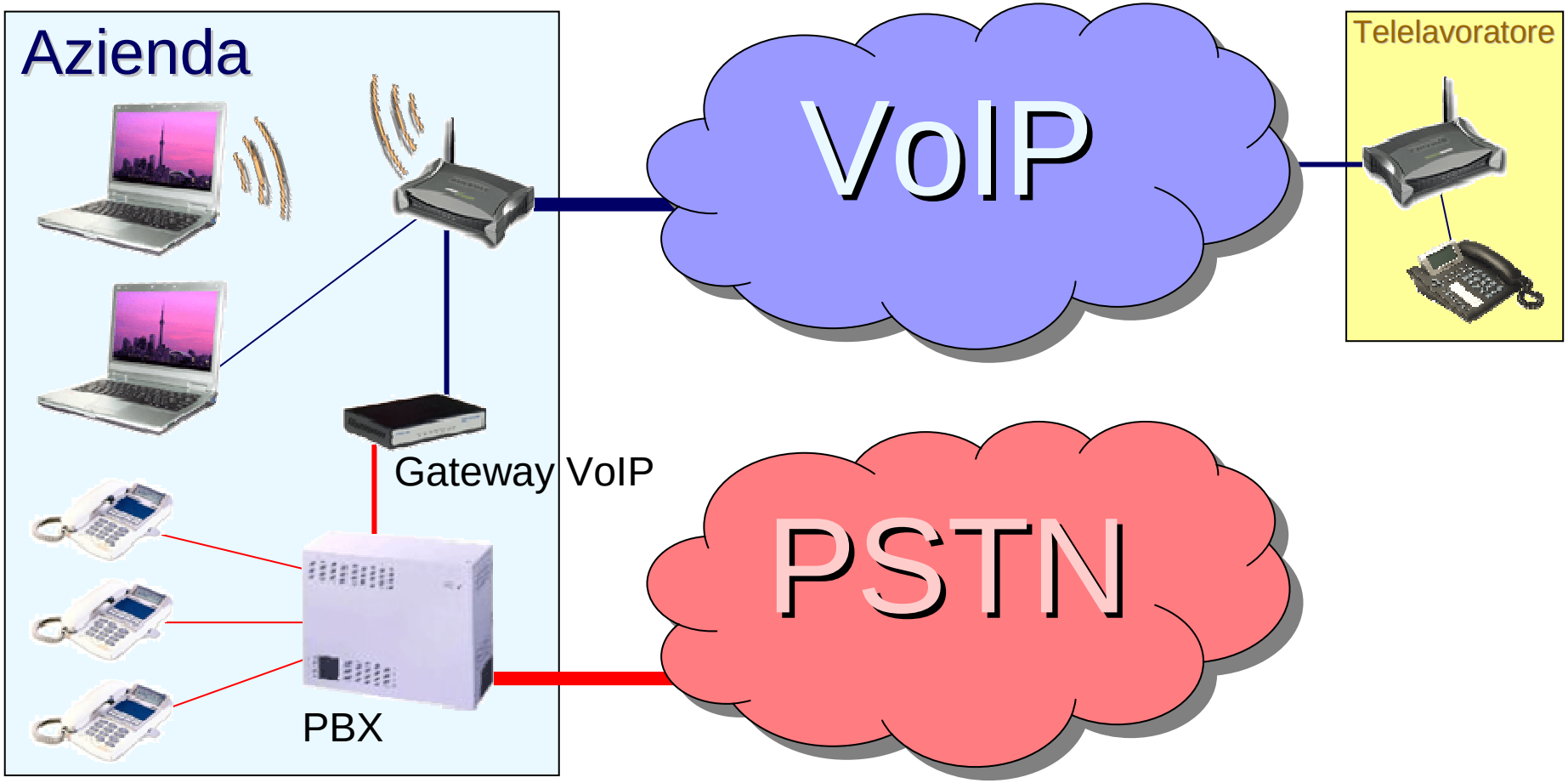
La qualità della connessione a banda larga

- Il consorzio VoIPex intende adottare in Italia, primo esempio al mondo, un bollino di qualità per i servizi basati su IP: l'IPex Certificate

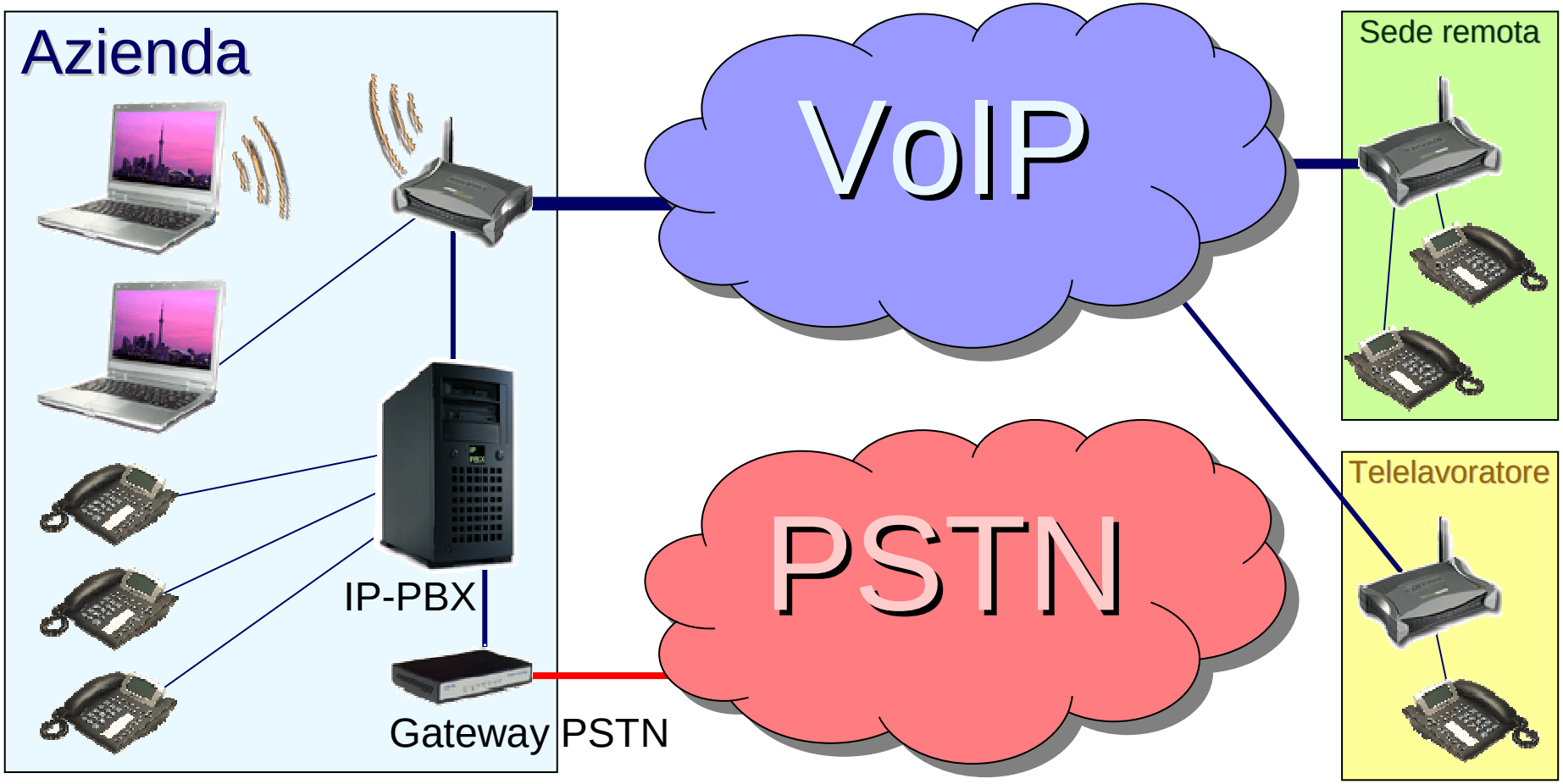
Caratt. / Classe	QoS su IP	Voce e video	Multifunzionalità	Nomadicità
A	Garantisce la QoS sul trasporto IP sul semicircuito di competenza e il trasporto della QoS nell'interconnessione con altre reti se certificate	Garantisce la negoziazione del miglior codec rispetto alle caratteristiche della linea utilizzata dal chiamante e rispetto ai codec disponibili del chiamato	Garantisce la completa interoperabilità dei servizi multifunzione con quella di altri operatori certificati	Consente la piena nomadicità del servizio su altre reti IP
B	Garantisce la QoS sul trasporto IP solo sul semicircuito di competenza, ed il best effort nell'interconnessione con altre reti anche se certificate	Garantisce la negoziazione del miglior codec rispetto alle caratteristiche della linea utilizzata dal chiamante ma non rispetto ai codec disponibili del chiamato	Non garantisce la completa interoperabilità dei servizi multifunzione con quella di altri operatori certificati	Garantisce la QoS sul trasporto Consente la nomadicità del servizio esclusivamente sulle proprie reti
C	Completamente Best Effort	Non consente la negoziazione dei Codec	Non offre servizi multifunzione	Non consente la nomadicità del servizio



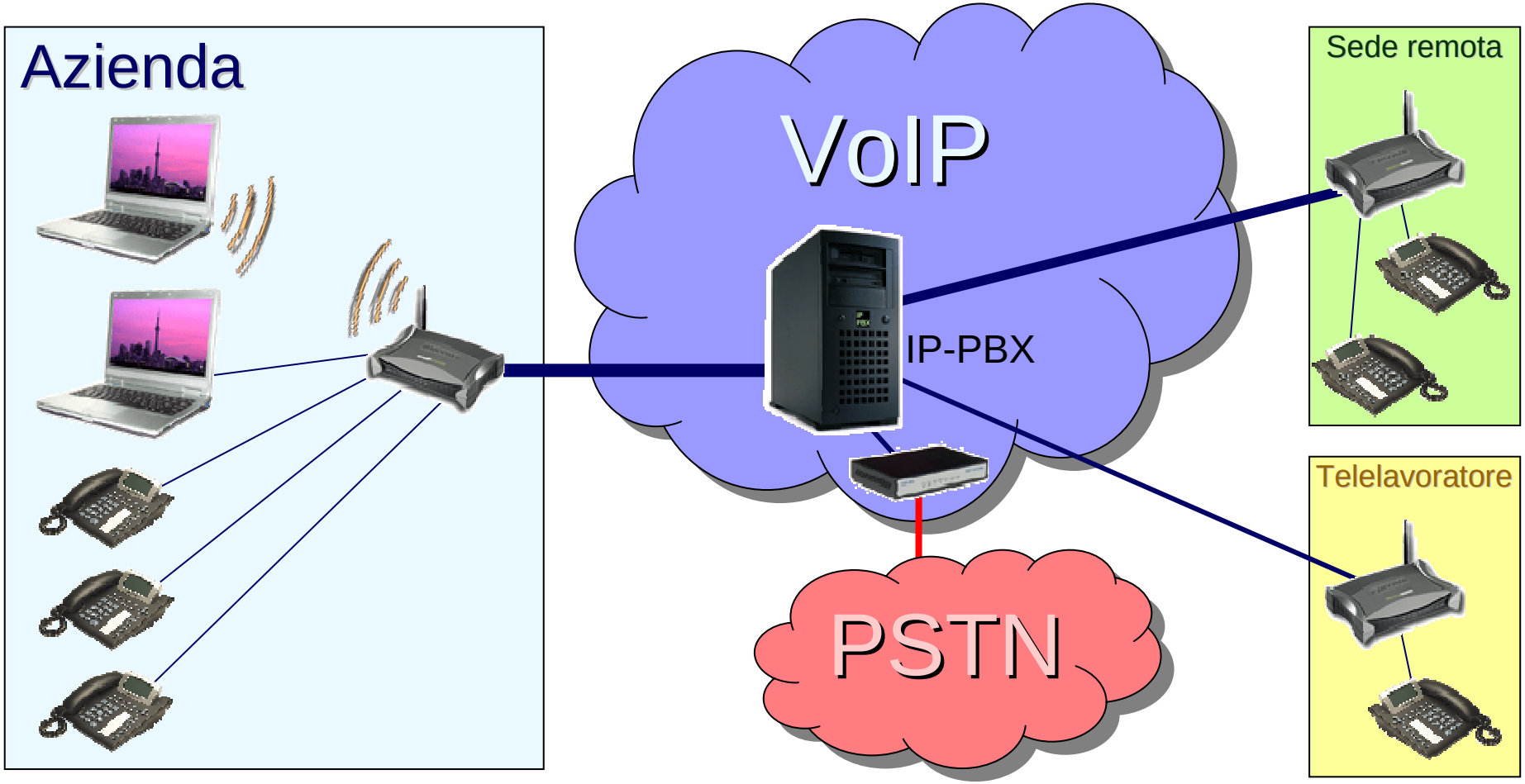
Esempi di scenari di implementazione: Gateway IP



Esempi di scenari di implementazione: IP-PBX (Softswitch)



Esempi di scenari di implementazione: IP Centrex



Esempi di servizi implementabili

- Trattandosi sostanzialmente di soluzioni di networking su IP, con i dovuti accorgimenti è possibile utilizzare tutte le tecnologie di comunicazione e connessione esistenti o di prossima disponibilità
- Esempio: è possibile connettere diverse sedi remote al medesimo IP-PBX ubicato nella sede principale utilizzando reti private virtuali (VPN)
- Esempio: è possibile delineare soluzioni di telelavoro, dove l'utente può fruire da casa di tutti i servizi presenti in azienda
- Esempio: è possibile gestire da remoto le modifiche di configurazione dell'IP-PBX
- Esempio: è possibile controllare via web il traffico generato e la spesa

Convergenza delle tecnologie di comunicazione

- Per rendere fruibili le innovative soluzioni apportate dal VoIP la tecnologia da sola non è sufficiente: va integrata con i servizi
- In Italia l'operatore *incumbent* ha lanciato primo in Europa un servizio che permette, con un solo terminale mobile che adotti la tecnologia UMA (*Unlicensed Mobile Access*), di effettuare e ricevere chiamate sia su rete GSM che su rete IP tramite connessione Wi-Fi, con un meccanismo di LCR che predilige l'instradamento su VoIP quando è disponibile
- Un altro servizio integrato offerto da un operatore mobile è la disponibilità di Skype sui propri smartphone che consente agli utenti di utilizzare la connessione UMTS per usufruire di tutti i servizi gratuiti che Skype offre

Sommario

1. Introduzione
2. Stato dell'arte della tecnologia
3. Contesto di riferimento in Italia
4. Implementazione di soluzioni VoIP
5. Sicurezza delle comunicazioni
6. Riferimenti bibliografici e sitografici

Premessa

- L'utilizzo di reti a commutazione di pacchetto per il transito di flussi multimediali in tempo reale introduce nuove vulnerabilità, non presenti nei sistemi di telefonia tradizionali né sempre rilevanti in ambito IP
- Nuove vulnerabilità, e dunque nuove minacce, possono compromettere la riservatezza e l'integrità delle comunicazioni ed inoltre la disponibilità dei servizi e delle applicazioni
- Non esistono ancora soluzioni definitive o consolidate per tutte le problematiche di sicurezza del VoIP
- La sensibilità verso i problemi di sicurezza del VoIP è ancora poco sviluppata, per cui occorre aumentare la consapevolezza dei nuovi rischi

Sicurezza delle comunicazioni

Preservare riservatezza, integrità e disponibilità

- Una prima categoria di minacce è quella relativa alle vulnerabilità delle reti di trasmissione basate sul protocollo IP
- Tuttavia le stringenti esigenze di qualità del servizio, peculiari dei sistemi VoIP, rendono rilevanti alcune vulnerabilità delle reti IP non considerate nella trasmissione dati
- Inoltre sempre i vincoli sulla QoS rendono inefficaci o poco praticabili le soluzioni ai problemi di sicurezza ormai consolidate nell'ambito delle trasmissioni di dati su reti IP
- Altro fattore da considerare è l'evoluzione dei terminali di comunicazione, che da telefoni *stupidi* sono divenuti *smart* e quindi passibili di attacchi

La sicurezza dello standard SIP

- Dalla specifica RFC3261: *SIP non è un protocollo semplice da rendere sicuro. Il suo uso di intermediari, le variegate relazioni di fiducia e le operazione che si compiono utente-utente rendono la messa in sicurezza niente affatto banale.*
- Già nella sua definizione si è consapevoli delle debolezze e vulnerabilità del protocollo SIP, che essendo aperto non permette di conoscere a priori tutti i componenti del sistema e i relativi problemi di sicurezza
- Rappresentare nella specifica RFC3261 non solo le minacce alla sicurezza dei sistemi basati su SIP, ma anche alcune possibili soluzioni, è indice di una sensibilità verso questi aspetti

Minacce e vulnerabilità tipiche di una rete dati IP

- Principali minacce che possono sfruttare le vulnerabilità delle reti e dei sistemi informatici
  - Virus, worm, trojan horses
  - DoS (Denial of Service)
  - Sniffing
  - Spoofing
  - MITM (Man-In-The-Middle)
  - Exploiting vulnerabilità del S.O. su cui è installata l'applicazione IP
  - Connessioni wireless non sufficientemente sicure
  - Corretto utilizzo dei terminali da parte degli utenti

Minacce e vulnerabilità tipiche di una rete dati IP

- Virus, worm, trojan horses
  - Già minaccia per gli apparati centrali delle reti VoIP che normalmente sono server con sistemi operativi commerciali, saranno la prossima minaccia anche per i terminali IP
  - Come accaduto per i cellulari, all'aumentare della complessità dei dispositivi di comunicazione, si ricorrerà a terminali IP che sono di fatto dei piccoli computer con un sistema operativo e del software applicativo, quindi esposti alle minacce che già incombono sugli attuali computer
  - Questo renderà vulnerabili non solo gli elementi centrali della rete, ma ogni singolo dispositivo che ne fa parte e quindi occorrerà adottare soluzioni di sicurezza distribuite ed effettuare audit su tutti gli apparati

Minacce e vulnerabilità tipiche di una rete dati IP

- DoS (Denial of Service)
  - La tecnica più comunemente usata per negare i servizi di un sistema informatico consiste nell'esaurire le risorse disponibili in modo che l'intero sistema risulti non accessibile o addirittura provocandone il blocco
  - È possibile ad esempio saturare la banda disponibile del sistema in modo che diventi irraggiungibile e quindi non più in grado di erogare i servizi
  - In una rete dati la saturazione della banda non è semplice da ottenersi, in quanto l'attuale tecnologia permette di processare grandi quantità di dati
  - In una rete IP dove transita la voce, con i vincoli di una trasmissione in tempo reale e con stringenti requisiti di QoS, è molto più semplice rendere inintelligibili le conversazioni, pur non bloccandole del tutto

Minacce e vulnerabilità tipiche di una rete dati IP

- Sniffing del traffico
  - Lo sniffing del traffico IP, ovvero l'intercettazione passiva, consente ad un terzo estraneo ad una comunicazione di prelevare il contenuto della comunicazione stessa senza che né il mittente né il destinatario se ne accorgano
  - In presenza di apparati switch lo sniffing del traffico IP non è banale, in quanto le comunicazioni non transitano per tutti i terminali della rete
  - Avendo accesso fisico allo switch è possbile utilizzare le porte di mirroring per duplicare il traffico di una porta e dunque captarlo
  - È comunque possibile ricorrete a tecniche quali il MAC flooding o l'ARP poisoning per alterare il funzionamento dello switch e poterne captare il traffico

Minacce e vulnerabilità tipiche di una rete dati IP

- Spoofing
  - Consiste nell'impersonificare qualcun altro, quindi far credere di essere chi non si è in realtà
  - È possibile effettuare lo spoofing dell'IP, dell'indirizzo MAC, etc.
  - Esempio: può essere utilizzato per impersonificare elementi fidati e quindi superare alcune difese o protezioni che si basano unicamente sulla provenienza delle comunicazioni
  - Esempio: può essere utilizzato per non essere rintracciati e lasciare nei log un'identificazione fasulla
  - Esempio: può essere utilizzato per effettuare un attacco DoS di tipo *smurf*, in cui si utilizzano reti mal configurate per amplificare il traffico generato

Minacce e vulnerabilità tipiche di una rete dati IP

- MITM (Man-In-The-Middle)
  - L'attacco uomo-nel-mezzo consiste nella possibilità di prelevare il traffico destinato ad un soggetto, modificarlo e reinviarlo al soggetto stesso senza che né il mittente né il destinatario si accorgano dell'alterazione
  - La prima fase è detta di *hijacking*, ovvero di dirottamento del traffico verso l'attaccante, che così potrà captarlo per poi alterarlo e reinviarlo
  - Il MITM attack permette di aggirare buona parte delle soluzioni di sicurezza adottate, in quanto il mittente comunica con l'attaccante credendo che sia il destinatario e viceversa
  - Eventuali procedure di autenticazione e cifratura vengono effettuate tra il mittente e l'attaccante e tra l'attaccante ed il destinatario

Minacce e vulnerabilità tipiche di una rete dati IP

- Exploiting delle vulnerabilità del S.O. su cui è installata l'applicazione IP
  - Normalmente un sistema di comunicazione su IP utilizza tecnologie hardware e software multi purpose, commercialmente disponibili
  - Quindi la sicurezza del sistema dipende anche da quella dei componenti esterni all'applicativo IP in sé, in particolare dal sistema operativo utilizzato
  - Occorre quindi adottare tutti gli opportuni accorgimenti per evitare che si possano sfruttare le vulnerabilità del S.O. per compromettere l'intero sistema
  - Si raccomanda l'aggiornamento periodico tramite le *patch* di sistema, l'*hardening* dell'apparato, l'analisi del traffico e dei log, l'esecuzione di audit per verificare la sicurezza del sistema, l'impiego di soluzioni ridondanti, l'ubicazione sicura dell'apparato sia fisica che logica

Minacce e vulnerabilità tipiche di una rete dati IP

- Connessioni wireless non sufficientemente sicure
  - La soluzione di connettività wireless oggi più utilizzata in ambito networking è il Wi-Fi (IEEE 802.11)
  - Il Wi-Fi non nasce sicuro, lo diviene in seguito all'adozione di ulteriori tecnologie quale la soluzione nativa WEP (Wired Equivalent Privacy), o le più recenti WPA e WPA2 (Wi-Fi Protected Access)
  - Il WEP è comunque il sistema più diffuso, ma è anche il più vulnerabile
  - Il WPA se ben configurato è sufficientemente robusto ma richiede più risorse e non è supportato dai primi dispositivi Wi-Fi
  - L'adozione di tecnologie di sicurezza decrementa significativamente il throughput medio della connessione

Minacce e vulnerabilità tipiche di una rete dati IP

- Corretto utilizzo dei terminali da parte degli utenti
  - Da non sottovalutare le minacce alla sicurezza del sistema provenienti dall'interno della rete, da parte degli utenti
  - Gli *insiders*, grazie ai privilegi ed al rapporto di fiducia di cui godono, sono in grado di provocare danni maggiori di quelli derivanti da attacchi esterni
  - Spesso sono inconsapevoli delle proprie potenzialità, poco sensibili ai problemi relativi alla sicurezza e dunque causa involontaria di eventi nocivi
  - La crescente complessità degli apparati, l'utilizzo della tecnologia da parte di un pubblico sempre più vasto, la semplificazione della gestione dei terminali sono tutti fattori che impattano significativamente sulla consapevolezza degli utenti riguardo ai potenziali pericoli e ai rischi derivanti da un utilizzo improprio

Minacce e vulnerabilità relative alle soluzioni VoIP

- Principali minacce che possono sfruttare le vulnerabilità della tecnologia VoIP a standard SIP
  - Riservatezza
    - Eavesdropping (*sniffing*)
    - Phreaking (*spoofing*)
    - Call hijacking
  - Integrità
    - MITM (Man-In-The-Middle)
  - Disponibilità
    - SPAM over Internet Telephony
    - DoS (Denial of Service)

Alimentazione elettrica

Chiamate d'emergenza

Minacce e vulnerabilità relative alle soluzioni VoIP

- Riservatezza: **eavesdropping**
  - Letteralmente origliare, è la capacità di captare le conversazioni su IP
  - La vulnerabilità risiede nel protocollo di trasporto, che normalmente è RTP
  - RTP non offre alcuna protezione dei dati che trasporta, non essendo implementato alcun meccanismo di cifratura
  - Su Internet si trovano software gratuiti che registrano le conversazioni RTP
  - Per ottenere la sicurezza dei dati trasmessi è possibile utilizzare SRTP (Secure Real-time Transport Protocol RFC3711)
  - SRTP garantisce la riservatezza del payload (AES), l'autenticazione e l'integrità del messaggio (HMAC SHA1), la protezione contro attacchi di tipo reply (sliding window + replay list), oltre che il controllo del traffico già di RTP

Minacce e vulnerabilità relative alle soluzioni VoIP

- Riservatezza: **eavesdropping**
  - SRTP non cifra l'header del pacchetto, ma ha un overhead contenuto
  - In alternativa ad SRTP è possibile utilizzare connessioni VPN con IPSec
  - IPSec garantisce la cifratura anche dell'header, in modo da rendere riservate anche le informazioni circa i soggetti coinvolti nella comunicazione
  - IPSec aumenta l'overhead dei pacchetti, l'implementazione richiede maggiori risorse computazionali, gestisce peggio l'allocazione delle risorse
  - Se l'apparato che genera il flusso cifrato non è sufficientemente veloce, è possibile introdurre ritardi sulla conversazione o degradare la QoS (es. jitter)
  - La creazioni di VPN è generalmente più complessa rispetto all'abilitazione di SRTP sui telefoni IP che supportano questo protocollo di sicurezza

Minacce e vulnerabilità relative alle soluzioni VoIP

- Riservatezza: **sniffing della segnalazione**
  - Un altro attacco alla riservatezza della comunicazione VoIP riguarda la possibilità di captare la segnalazione SIP tra i vari elementi
  - Benché dalla segnalazione non sia possibile risalire al contenuto della conversazione è comunque possibile avere informazioni sui soggetti coinvolti nella comunicazione, violandone la *privacy*
  - Inoltre all'interno dei pacchetti SIP sono contenute le stringhe hash di autenticazione, normalmente generate con l'algoritmo MD5, molto semplice da rompere anche per la disponibilità su Internet di tool gratuiti creati ad hoc
  - È possibile utilizzare TLS con SIP (SSIP), opzione obbligatoria per i SIP Server ma facoltativa per gli UA: richiede necessariamente il TCP, no UDP

Minacce e vulnerabilità relative alle soluzioni VoIP

- Riservatezza: **phreaking**
  - Con il termine *phreaking* si intende chi storicamente utilizzava le falle del sistema telefonico tradizionale per il proprio tornaconto
  - In ambito VoIP si possono considerare *phreakers* coloro che adottando ad esempio tecniche di spoofing generano frodi o comunque raggirano le difese
  - Di recente sono stati scoperti in Florida dei *phreakers* che hanno rivenduto traffico VoIP abusivo per oltre un milione di dollari
  - Uno spoofing molto semplice da realizzare riguarda l'identificativo del chiamante (CLI - Calling Line Identifier), così da presentarsi al destinatario della comunicazione con un numero di telefono che per lui risulta fidato e quindi by-passare gli eventuali filtri sul chiamante applicati

Minacce e vulnerabilità relative alle soluzioni VoIP

- Riservatezza: **phreaking**
  - Lo spoofing della segnalazione SIP è anche il primo passo de compiere per effettuare alcune tipologie di attacchi all'integrità delle comunicazioni ed alla disponibilità dei sistemi
  - Un elemento che concorre al successo di questi attacchi è la mancanza di reciproca autenticazione: normalmente uno UA si autentica a quello che crede essere un SIP Server, ma non ha alcuna informazione circa la sua autenticità
  - L'impersonificazione di un SIP Server rende vani tutti gli altri accorgimenti presi, in quanto si forniscono informazioni riservate ad un sistema infido
  - Come per l'eavesdropping, la soluzione è utilizzare TLS con SIP (SSIP)

Minacce e vulnerabilità relative alle soluzioni VoIP

- Riservatezza: **call hijacking**
  - Attacco di spoofing che può riguardare tanto la segnalazione quanto la fonìa
  - Nel caso un Registrar server non utilizzi meccanismi di autenticazione è possibile per un attaccante impersonificare un utente e variare i suoi parametri di registrazione, in particolare le informazioni di connettività
  - In questo modo le chiamate dirette all'utente attaccato saranno dirottate dal SIP Server stesso verso l'attaccante, senza che il chiamante se ne accorga
  - Intercettando una richiesta di INVITE è ancora possibile rispondere con un messaggio SIP di ridirezionamento, temporaneo o permanente, in modo che il chiamante reinvii la sua richiesta di connessione ad una terza parte, che nella fattispecie è l'attaccante

Minacce e vulnerabilità relative alle soluzioni VoIP

- Riservatezza: **call hijacking**
  - Esistono ancora ulteriori tecniche per dirottare altrove le comunicazioni, che sfruttano le vulnerabilità degli altri sistemi coinvolti
  - ENUM poisoning: si basa sull'attacco classico di DNS poisoning, per cui ad esempio alterando l'associazione dei record all'interno del data-base ENUM è possibile dirottare altrove la comunicazione
  - DHCP spoofing: nel caso si utilizzi un server DHCP per l'assegnazione dinamica degli indirizzi IP, è possibile alterare la tabella di associazione MAC-IP in modo da appropriarsi di un indirizzo presente sul Registrar Server
  - Come per il phreaking una possibile soluzione consiste nell'utilizzare l'autenticazione reciproca, ad esempio con TLS (SSIP)

Minacce e vulnerabilità relative alle soluzioni VoIP

- Integrità: **MITM (Man-In-The-Middle)**
  - Estende gli attacchi di tipo call hijacking inoltrando la comunicazione, eventualmente alterata opportunamente, al destinatario originario
  - Sfrutta le medesime vulnerabilità dei componenti l'intero sistema VoIP che consentono il dirottamento delle comunicazioni
  - E' particolarmente pericoloso perché più difficile da rilevare del solo dirottamento, in quanto nel call hijack la comunicazione tra i due soggetti non avveniva e quindi ad un confronto diretto era semplice che se ne accorgessero
  - Nel caso di attacchi MITM le informazioni transitano realmente tra chiamante e chiamato, ma opportunamente alterate

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **SPAM over Internet Telephony**
  - Il termine SPAM è utilizzato per indicare l'invio di un numero eccessivo di e-mail, per lo più pubblicitarie, non richieste né desiderate dal destinatario
  - Il risultato è che le caselle di posta elettronica sono piene di e-mail spazzatura e quindi senza una continua manutenzione sono destinate a riempirsi e a divenire così inutilizzabili
  - In analogia il termine SPAM è utilizzato relativamente alle comunicazioni su IP per indicare la ricezione di una quantità eccessiva di telefonate, non richieste né desiderate
  - Anche se il fenomeno dello SPAM in ambito telefonico è già conosciuto, è tuttavia di dimensioni modeste se paragonato alle potenzialità del VoIP

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **SPAM over Internet Telephony**
  - La possibilità di effettuare chiamate gratuite a livello internazionale amplia di molto il numero delle società interessate a promuovere un prodotto sfruttando la tecnologia VoIP
  - L'utilizzo sempre più diffuso di caselle vocali personali (*voice mailbox*) rende ancora più efficace questo tipo di attacco
  - In questo contesto non risulta praticabile in maniera semplice il filtro dei contenuti, come avviene per le e-mail
  - Inoltre l'apertura alla reti estere rende molto più difficile, se non impossibile, l'esercizio del proprio diritto alla riservatezza ed alla protezione dei propri dati personali (*privacy*)

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - Relativamente agli attacchi che mirano alla negazione dei servizi di comunicazione basati su IP, esistono diverse forme d'implementazione sia a livello di segnalazione SIP che di fonìa RTP
  - La pluralità di forme con cui si può portare a termine un attacco di tipo DoS suggerisce di porre particolare attenzione alle vulnerabilità che possono decretarne l'efficacia
  - Anche in questo caso il destinatario dell'attacco non deve essere necessariamente un sistema centrale o un canale di comunicazione comune
  - È possibile attaccare direttamente i terminali IP con maggiore probabilità di successo per le loro esigue capacità elaborative

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - SIP bomb: il classico attacco DoS trasferito in ambito VoIP. Si invia una continua ed eccessiva segnalazione SIP verso un unico SIP server o UA, in modo che questi cessi di funzionare o perché si satura la banda disponibile, in maniera sufficiente a degradare la QoS a livelli che non permettono di utilizzare di fatto il canale per le conversazioni, oppure perché il destinatario dell'attacco non ha sufficienti risorse per processare la segnalazione in arrivo e quindi si blocca o va in crash o si riavvia, etc.
  - Per gli apparati dotati di maggiori risorse potrebbe risultare più semplice degradare la QoS sulla connessione, mentre per gli apparati più piccoli come i telefoni IP potrebbe risultare più efficace inondarli di segnalazione

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - SIP TDS (Tearing Down Session): con questo attacco è possibile inibire l'instaurazione di nuove sessioni, o chiudendole sul nascere o mentre sono già stabilite. Nel primo caso un attaccante che capta un INVITE può inviare un CANCEL al destinatario dell'INVITE, prima che questi riceva anche l'ACK. In questo modo la sessione è abbattuta prima che venga instaurata
  - Nelle medesime condizioni è possibile inviare un messaggio di BYE, una volta che la sessione è già instaurata senza avere quindi vincoli temporali per preparare l'attacco
  - È possibile richiedere l'autenticazione con l'HTTP Digest anche per i messaggi BYE, mentre non è prevista l'autenticazione di quelli CANCEL

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - SIP bindings: nel caso non vi sia un numero massimo di registrazioni che uno UA può effettuare su un Registrar Server, è possibile portare a termine registrazioni multiple dello stesso utente con indirizzi IP diversi
  - In questo modo, nel momento in cui viene il Registrar Server si troverà a terminare una chiamata verso lo UA registrato con numerosi indirizzi IP, il Registrar Server occuperà notevoli risorse, sia di calcolo che di banda, per inviare la segnalazione a tutti gli indirizzi afferenti a quella utenza
  - Con questa tecnica di amplificazione non è necessario che l'attaccante abbia alcun requisito in termini di banda o di potenza di calcolo, perché non è necessario effettuare tutte le registrazioni contemporaneamente

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - RTP synchronization source (SSRC): in un flusso RTP la sorgente dello stream sceglie in maniera casuale un codice univoco nell'ambito della sessione, che verrà utilizzato dal destinatario per gestire correttamente i pacchetti ricevuti. Questo codice è l'identificativo SSRC
  - È sempre possibile che due sorgenti diverse scelgano casualmente lo stesso SSRC per cui il protocollo di controllo RTCP è in grado di gestire le eventuali collisioni
  - Se a rilevare le collisione è una sorgente, questa invierà al destinatario un RTCP BYE relativo al vecchio SSRC e ne sceglierà un altro nuovo
  - Se la collisione è rilevata dal destinatario, questi considererà un solo flusso

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - RTP synchronization source (SSRC): per quanto detto un attaccante, che in qualche modo conosce l'identificativo SSRC di uno stream RTP, potrebbe inviare pacchetti RTP con il medesimo SSRC alla sorgente del flusso, così che questa rilevando la collisione interrompa la trasmissione per scegliere casualmente un SSRC alternativo
  - Se l'attaccante sceglie di inviare i pacchetti RTP con un SSRC già in uso al destinatario della conversazione, questi sceglierà di accettare i pacchetti provenienti da una sola sorgente, scartando quelli provenienti dall'altra
  - In entrambi i casi utilizzando le collisioni dell'identificativo SSRC, un attaccante è in grado di negare il servizio di comunicazione VoIP

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - RTP synchronization source (SSRC): è ancora possibile sfruttare la mancanza di un autenticazione forte dei soggetti partecipanti ad una conversazione per inviare pacchetti che replicano le informazioni di connettività IP (*spoofing*) insieme all'identificativo SSRC ma con diversi marcatori temporali o numeri di sequenza, generalmente successivi e più alti di quelli realmente utilizzati dalle parti in comunicazione
  - Così facendo i pacchetti iniettati nel flusso RTP verranno considerati di più recente generazione e saranno preferiti a quelli veri, perché ormai datati e dunque da scartare in una conversazione in tempo reale
  - Gli effetti che sortisce sono comunque quelli di negare una comunicazione

Minacce e vulnerabilità relative alle soluzioni VoIP

- Disponibilità: **DoS (Denial of Service)**
  - RTP codec: il meccanismo di monitoraggio del traffico di RTP consente di variare il codec multimediale utilizzato nella sessione in maniera del tutto trasparente, scegliendo il codec che meglio si adatta alle condizioni della rete rilevate
  - Un attaccante potrebbe sfruttare questo meccanismo di adattamento automatico per rendere inintelligibili le comunicazioni
  - Infatti variando continuamente le caratteristiche del traffico oppure richiedendo repentine variazioni di codec è possibile fare in modo che i sistemi coinvolti utilizzino più risorse del necessario, negando il servizio
  - Una possibile soluzione alle vulnerabilità di RTP è Secure-RTP

Minacce e vulnerabilità relative alle soluzioni VoIP

- **Alimentazione elettrica**
  - Ulteriore vulnerabilità degli apparati di comunicazione su IP, in particolare dei terminali è che per poter funzionare devono essere alimentati elettricamente, a differenza degli apparati telefonici tradizionali
  - In pratica senza le opportune precauzioni non sarà possibile comunicare su IP in caso di *black-out*
  - Soluzioni generiche possono essere gli UPS (*Uninterruptible Power Supply*), o più i gruppi elettrogeni per i sistemi con maggior consumo
  - Per sfruttare a pieno la convergenza e l'integrazione della rete telefonica su quella IP è stato definita la specifica IEEE 802.3af (Power Over Ethernet), in modo da alimentare i dispositivi predisposti direttamente via LAN

Minacce e vulnerabilità relative alle soluzioni VoIP

- **Chiamate d'emergenza**
  - Il problema più annoso per le comunicazioni basate su IP è probabilmente quello relativo all'instradamento delle comunicazioni d'emergenza
  - Risolti gli eventuali problemi sulla garanzia di effettuare comunicazioni in ogni circostanza, soprattutto se di crisi, sorge il problema della localizzazione automatica del chiamante
  - Con la telefonia tradizionale la conoscenza del distretto telefonico è sufficiente per collegare la chiamata al centro di primo soccorso di competenza territoriale; discorso analogo per la telefonia mobile e le celle
  - Su reti IP l'unico parametro identificativo è l'indirizzo IP che purtroppo non ha con sé alcuna informazione sulla posizione geografica dell'utente

Minacce e vulnerabilità relative alle soluzioni VoIP

- **Chiamate d'emergenza**
  - Non esiste al momento una soluzione definitiva
  - Possibili soluzioni coinvolgono tutti gli attori presenti in uno scenario VoIP
  - Esempio: è l'ISP a fornire all'operatore del servizio di emergenza le informazioni sulla localizzazione dell'utente
  - Esempio: è possibile utilizzare apparati dotati di GPS
  - Esempio: è possibile utilizzare gli archivi relativi alle assegnazioni geografiche degli indirizzi IP
  - Esempio: è possibile stimare la posizione dalle misure della latenza delle comunicazione
  - I dati di geo-localizzazione sono delicatissimi ai fini della *privacy* dell'individuo

Ulteriori considerazioni relative alla sicurezza del VoIP

- Una parte delle vulnerabilità dei sistemi VoIP nasce dalla possibilità di sferrare attacchi agli elementi senza averne accesso fisico
- Le esigenze di privacy e riservatezza vanno sempre bilanciate con quelle di sicurezza: realizzare soluzioni di lawful interception in presenza di connessioni cifrate non è semplice
- Non tutte le tecnologie di sicurezza sono state pensate per il transito di flussi in tempo reale
- La sicurezza dell'intero sistema VoIP non dipende solo dalla sicurezza di ogni singolo componente
- In generale una buona organizzazione vale meglio di un buon firewall

Linee guida del NIST per definire sistemi VoIP sicuri

1. Sviluppare un'infrastruttura di rete appropriata: separazione logica voce-dati
2. Assicurarsi che, nell'implementare soluzioni VoIP, l'organizzazione abbia esaminato i rischi legati alle informazioni, alle operazioni dei sistemi ed alla continuità delle operazioni essenziali, ed inoltre possa gestire questi rischi in maniera accettabile e ridurli
3. Considerare gli aspetti legati alla comunicazioni di emergenza
4. Essere consapevoli dell'importanza dei controlli sull'infrastruttura fisica
5. Provvedere a soluzioni che garantiscano la continuità dell'alimentazione elettrica
6. Utilizzare apparati di rete (es. firewall, router, etc.) che siano VoIP aware
7. Porre attenzione agli applicativi VoIP software, in particolare ai softphone
8. Nel caso si utilizzino reti Wi-Fi, WPA è da preferire al WEP
9. Porre attenzione agli aspetti legali legati alla privacy ed alla data retention

Sommario

1. Introduzione
2. Stato dell'arte della tecnologia
3. Contesto di riferimento in Italia
4. Implementazione di soluzioni VoIP
5. Sicurezza delle comunicazioni
6. Riferimenti bibliografici e sitografici

Bibliografia e sitografia

1. VoIP su Wikipedia, l'enciclopedia libera
   http://it.wikipedia.org/wiki/VoIP
2. CNIPA, Quaderno sul VoIP
   http://www.cnipa.gov.it/site/_files/Cnipa%20-%20Quaderno%2019.pdf
3. Voipex, consorzio per l'interoperabilità, la qualità, la trasparenza dei servizi IP
   http://www.voipex.it
4. NIST, Security Considerations for Voice Over IP Systems
   http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
5. VOIPSA, Voice over IP Security Alliance
   http://www.voipsa.org
6. PROTOS, Security Testing of Protocol Implementations
   http://www.ee.oulu.fi/research/ouspg/protos

Grazie per l'attenzione!

info@ingamendola.com

www.ingamendola.com