A Light Reading Webinar

SIP & Its Application In Next-Gen Services

Thursday, June 5, 2008

Hosted by

Jim Hodges
Senior Analyst
Heavy Reading

Sponsored by:
Speakers

Ben Campbell
Principal Engineer, Tekelec Inc.

Jonathan Cumming
Director of VOIP Product Mgmt., Network Protocols Division, Data Connection Ltd.

Todd Mersch
Senior Product Line Manager, Trillium Software, Continuous Computing Corp.

Adam Stein
VP Marketing, Mu Dynamics Inc.
About Tekelec

- Signaling
- Session Management
- Number Portability
- Messaging
- Service Mediation
- Flexible Routing
- Service Assurance
- Revenue Assurance
- Service Creation

Tekelec’s solutions are in 7 of 10 of the world’s largest wireless carriers and in 6 of 10 of the world’s largest wireline carriers.
Data Connection (DCL)

- DCL provides portable protocol software for system vendors

**Products & Customers**
- IP Routing: BGP, OSPF-TE, ISIS-TE, RIP, PIM, IGMP
- MPLS: RSVP-TE, LDP, VPNs, VPLS
- Optical: GMPLS, O-UNI/NNI, E-NNI, LMP
- VoIP / IMS: SIP, Megaco/H.248, MGCP, Diameter, SBC
- ATM: PNNI, SVCs, UNI, IISP, ILMI
- SNA/APPN: SNA/IP, SNAP-IX, HIS Applications

**Revenue & Profit**
- $m
- Profit
- Total Revenue

**Employees**
- 0
- 50
- 100
- 150
- 200
- 250
- 300
- 350
- 400
- 82
- 84
- 86
- 88
- 90
- 92
- 94
- 96
- 98
- 00
- 02
- 04
- 06

**Technology**
- IP Routing
- MPLS
- Optical
- VoIP / IMS
- ATM
- SNA/APPN

**Brands**
- Ciena
- ZTE
- NEC
- Fujitsu
- Siemens
- BARCLAYS
- IBM
- Microsoft
- Continuous Computing
- DATA CONNECTION
- Mu Dynamics
- TEKELEC
Continuous Computing

TRILLIUM
Software from Continuous Computing

Protocol Software

Integrated Systems

AdvancedTCA & CompactPCI Hardware

Trillium Professional Services

Over 150 Customers Worldwide

www.ccpu.com
Who Is Mu?

Founded, 3 years ago

1st product ships, 2 years ago

Product 2.0, 1 year ago

Product 3.0, Today

• Focus on Network security devices, Layer 2-4 Routing development
  • US Telco and their NEMs

• Extended focus to VoIP, Integrated Security systems, Storage
  • International customer adoption

• Customer engagements with Stateful VoIP, IMS, IPTV, Web Apps
  • Significant expansion within specific Network Operator & NEM accounts

“Great Promise”

“Great Technology”

“Great Product/Solution”

Top Security Firm

---
Agenda

• SIP history and role in standards
• SIP call setup scenarios
• SIP as a next-generation applications enabler
• Reliability, authentication, and security considerations
• Q&A
Session Initiation Protocol

- **Purpose**
  - Session establishment
  - Mobility support
  - Capability negotiation

- **Scalable**
  - Function distribution
  - Any device

- **Flexible**
  - Extensible
  - Over ANY IP network

- **Flexible**

---

**Any Application**

- SIP

**Session Control**

- UDP
- TCP
- SCTP

**Any Transport**

- IP

**Any Access**

- 802.11
- DSL
- 3G

**Any Device**

- Continuous Computing
- Data Connection
- Mu Dynamics
- TEKELEC
How Is SIP Defined?

- SIP defined by many IETF RFCs and drafts
  - RFC 3261 Session Initiation Protocol
  - RFC 3262 Reliable Provisional Responses
  - RFC 3263 Server Location
  - RFC 3264 Offer / Answer Model
  - RFC 3265 Events / Presence
- Many organizations define SIP subsets for particular applications
- SIP Interoperability Test Events (SIPit)
  - 22 SIPits since 1999

Standards bodies

Industry forums

Fixed

Mobile

Internet

SIPit 22
2008
UNH-IOL
SIP Terminology

• Endpoints are SIP User Agents (UAs)
  • User Agent Clients (UACs) send requests
  • User Agent Servers (UASs) process requests and send responses

• Proxies & redirect servers route messages
  • They cannot generate new requests
  • B2BUA (Back-to-Back User Agent) can generate new requests

• Registrars record endpoint location
  • Normally collocated with a proxy or redirect server
Session Establishment Features

- Routing
- Authentication
- Capability Negotiation

1a. Challenge
1b. Registration

2. Forwarding
3. Redirection

End-to-end capability negotiation
Modes of Operation

• Media sessions (VOIP)

• Subscriptions (Buddy list)

• Transaction only (SMS, IM)
Call Center ‘Click-to-Dial’

1. SIP URI on Web page
2. REFER
3. Phone calls SIP URI
4. Call forwarded to next free agent
5. Reference identifies Web page context

Company Web server

Company SIP server
SIP Architecture Challenges

Internet Design
- Many-to-many relationships
  - Interoperability
  - Security (DDOS / scalable authentication)
- Internet is not flat
  - NAT/firewall traversal
  - Privacy / confidentiality
- Commercial realities
  - Failure detection
  - Billing
  - Lawful intercept

One Solution
- Managed network (IMS)
  - Domain-based security
- SBC polices border
  - Tracks and bills resources
  - Protocol normalization
  - NAT/Firewall traversal
  - Lawful intercept
  - Privacy controls
- Single point of control
  - Users have someone to ask!
Anatomy of a SIP Message

**Header Fields**

- INVITE sip:ben.campbell@tekelec.com SIP/2.0
- Via: SIP/2.0/UDP 172.17.1.247:2078;branch=z9hG4bK-6vi6sa58smfx;rport
- To: "Ben Campbell" <sip:ben.campbell@tekelec.com>
- From: "Adam Stein" <sip:adam.stein@mudynamics.com>;tag=4at3wehz8c
- Call-ID: 3c58339ed1f6-lvfo12ixa8h
- CSeq: 1 INVITE
- Max-Forwards: 70
- Contact: <sip:adam.stein@172.17.1.247:2078>
- Accept: application/sdp
- Content-Type: application/sdp
- Content-Length: 168

**SDP**

- v=0
- o=- 1411917766 1411917766 IN IP4 172.17.1.247
- c=IN IP4 172.17.1.247
- t=0 0
- m=audio 61586 RTP/AVP 0 101
- a=rtpmap:0 pcmu/8000
- a=rtpmap:101 telephone-event/8000
Session Setup Example

Redirect

This proxy does not choose to remain in signaling path for the rest of the dialog

Proxy

These proxies insert Record-Route header fields to ensure they remain in the signaling path

App Server

Proxy/Registrar

Adam

2 Way RTP

Ben
Interacting With the PSTN

- Request-URI in the **INVITE** contains a telephone number, which is sent to PSTN gateway.
- The gateway maps the **INVITE** to a SS7 ISUP IAM (Initial Address Message).
- **183 Session Progress** establishes early media session so caller hears ring tone.
- Two-way speech path is established after ANM (Answer Message) and **200 OK**.
Roles of the Proxy

- Pre-IMS proxy similar to CFCS in IMS networks
- Session routing
  - Rules-based routing
  - Service brokering to application servers or local applications
  - Parallel and sequential forking applications
  - Registrar/location service
  - ENUM
  - May insert other devices into call path using loose-routing mechanism
- Load balancing
- Congestion management
- Authentication/security
ENUM Example

DNS Query NAPTR
0.9.8.7.6.5.4.3.2.1.e164.arpa

IN NAPTR 10 100 "u" "E2U+sip"
"!.*$!sip:ben.campbell@tekelec.com!"

INVITE sip:ben.campbell@tekelec.com

INVITE tel:+1234567890
caller domain

proxy.tekelec.com
• DNS service records (a.k.a. SRVs) allow named “clusters”
  • SRV supports weighted statistical load distribution
  • SIP will route around congested devices
Dominant SIP-Based Architectures
## Applications Driving New SIP Requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Drivers</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Scalability</td>
<td>• New applications creating greater demand on core network</td>
<td>• Optimization for multi-core / multi-threaded processors</td>
</tr>
<tr>
<td></td>
<td>• Cost reduction to ignite faster operator adoption</td>
<td>• “SIP-light” implementations</td>
</tr>
<tr>
<td></td>
<td>• Smaller footprint for use in consumer devices</td>
<td></td>
</tr>
<tr>
<td>Security Extensions</td>
<td>• Proliferation of SIP into new devices</td>
<td>• Support for latest security extensions</td>
</tr>
<tr>
<td></td>
<td>• Leveraging customer broadband access</td>
<td>• TLS, IPSec, S/MIME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Denial of Service (DOS) apps</td>
</tr>
<tr>
<td>Domain Applicability</td>
<td>• Operator need to leverage benefits of SIP for mobile applications</td>
<td>• Interworking between SIP &amp; wireless protocols</td>
</tr>
<tr>
<td></td>
<td>• Converged core network</td>
<td>• Mapping of mobile CC/MM to SIP messaging</td>
</tr>
</tbody>
</table>

---
Femtocell: Deployment Architectures

Tunneled Iub

AAA System (e.g. HSS)

UMA/UNC Based

Security Gateway

UMA-based Network Controller

Security Gateway

GANC

3G RAN

SIP Based

UMA/UNC Based

Security Gateway

GANC

IMS Call Control

AAA System (e.g. HSS)
SIP/IMS-Enabled Femtocell

SIP-IMS Based

SIP-Based Femtocell Drivers
- Leveraging operators’ existing or planned NGN and/or IMS core networks
- Provides extension for mobile service innovation over home base stations
- Common billing infrastructure supporting innovative tariff schemes
- SIP extensions supporting common femtocell requirements
  - Presence
  - Event frameworks
  - Access control
  - Authentication

UMTS call termination

UMTS Uu interface towards MS

Control Application
- RRC
- RLC
- MAC-b, MAC-d, MAC-sh
- MAC-HS, MAC-ES, MAC-E*

Forwarding Application
- PDCP
- GMM/SM
- SIP
- SRTP
- SCTP
- TCP / UDP
- IPSec

Stack Manager
- GMM / SM & CC/MM to support mobility
- SIP UA for IMS / SIP call initiation
- Secure RTP for bearer plane
Key SIP Features for IMS/LTE

• Globally Routable UA URI (GRUU)
  • Same public identity associated with multiple devices (e.g., softphone, mobile, landline, etc.)
  • Service convergence

• Voice Call Continuity (VCC)
  • Clean handover to/from legacy mobile to IMS core
  • Service continuity

• Standardization of “enabling” applications like presence & messaging
  • Service building blocks to be reused in new applications
  • Accelerates new service delivery over mobile broadband like LTE
Enterprise Automation Based on SIP

- Converged instant messaging, presence, file sharing, and voice & video conferencing
  - SIP + SIMPLE (instant messaging extensions) for signaling
  - Secure RTP / RTCP for bearer plane
  - Utilize hybrid client – server and pure P2P model
  - “Federation” to integrate different clients and servers
- Examples include
  - Microsoft Office Live Communications Server
  - IBM Lotus Sametime
  - Cisco Unified Communications & Presence Servers
Audience Poll #1

Which of the following architectures do you view as driving mass adoption of SIP-based applications?

- IMS – SIP application server
- NGN-based softswitch – SIP application server
- Peer-to-peer services
- Femtocells
- Not sure
SIP NGN
Reliability Considerations

- Reliable SIP “hotspots” widespread
  - Inherent SIP protocol ASCII weaknesses; latency issues, optional settings, new moving parts
  - Weaknesses due to vendor implementations, transport variations, version control
  - Authentication issues
    - Registration/call hijacking
    - Man in the middle – impersonating a SIP-entity
    - Denial of service (DOS) hardening
**Threat:** Third-party IP address information is appended in the Contact header, which points to the attacker's device.

**Solution:** Service-level traffic variations to remove any weaknesses in SIP deployments on all proxy and SIP register servers; leverage TLS/SSP in SIP servers.

Contact: adam.stein@172.17.1.247:2078@ rogue IP address
SIP DOS (Denial of Service)

**Threat:** Falsified route headers used in a request that identifies the target host and then sends such messages to a forking proxy that amplifies target messaging.

**Solution:** Subject SIP products to service-level traffic to validate correct proxies, harden any weak spots, and control all assets; leverage stronger encryption.
SIP Authentication Capabilities: S/MIME

- **S/MIME** for email uses encryption in proxy server to ensure mail is not tampered, end-to-end SIP application assurance.

- **Drawback**: Not trustworthy unless end-to-end authentication occurs.

The signature is valid because the email address in the From: header does match the certified email address. But Aunt Tillie can't see the mismatch between the address and the friendly name. The forger, relying on the fact that Outlook’s “friendly” display hides the actual email address, misdirects Aunt Tillie. She is tricked into believing that the signature binds to killg@microsoft.com rather than to judell@myrealbox.com.
SIP Authentication Capabilities: TLS

- **Transport Layer Security (TLS)** handshake protocol, allows the server & client to authenticate each other and to negotiate an encryption algorithm & cryptographic keys before the application protocol transmits or receives its first byte of data

- **Drawbacks:**
  - SSL relies on TLV structures that are easy to abuse and maliciously exploit
  - SSL relies on X.509 certificates, which are encoded using Abstract Syntax Notation number one (ASN.1)
SIP Authentication Capabilities: IPSec

- **IP Sec**: IPSec uses a Diffie-Hellman exchange to perform authentication and establish session keys for strong cryptography

- **Drawbacks**:
  - IMS usage between proxies suffers; proxy pollution via malware allows bad traffic over IPSec-enabled networks
  - Large hop-by-hop overhead for every proxy, client & server touched
Authentication or Assurance?

• Authentication “Best Practice”
  • IPSec (enterprise – no chain of trust),
  • TLS (operator – certificate control),
  • S/MIME (end to end, SIP Digest algorithm)

• Assurance “Best Practice”
  • Millions of variations on authenticated service traffic
  • Known vulnerabilities or using DOS

• How to look?
  • Monitoring, automation, integration
  • Interact with live applications, products or services (targets)
Audience Poll #2

How do you ensure your SIP-based services or products are free from reliability weaknesses that cause service degradation or downtime?

- Customer feedback, repair on incident only
- Product acceptance criteria in place (operator)
- Quality assurance benchmarks in place (vendor)
- Nothing. We haven’t had customer support complaints, customer churn, or authentication issues for SIP-based services
Q&A