Analisi e sviluppo di un analyzer per protocollo SIP

Università degli Studi del Sannio

A.A. 2006 / 2007

Misure su reti di calcolatori

Laurea specialistica in Ingegneria Informatica

Francesco Cioffi
Ausilio Di Prizito
Silvio Greco
Giorgio Mennitto
Luca Perrotta

Prof. Luca De Vito

[CRB]

26 luglio 2007

Indice

- obiettivi
- SIP
- SipAnalyzer
  - stato dell'arte
  - agent ed analyzer
- JSipAna2
  - architettura
  - componenti
- conclusioni
- sviluppi futuri

Obiettivi

- analisi di comunicazioni in rete, basate su protocollo SIP
- utilizzo ed estensione di un software esistente per le esigenze di progetto
- sviluppo di un software general-purpose

SIP 1 / 2

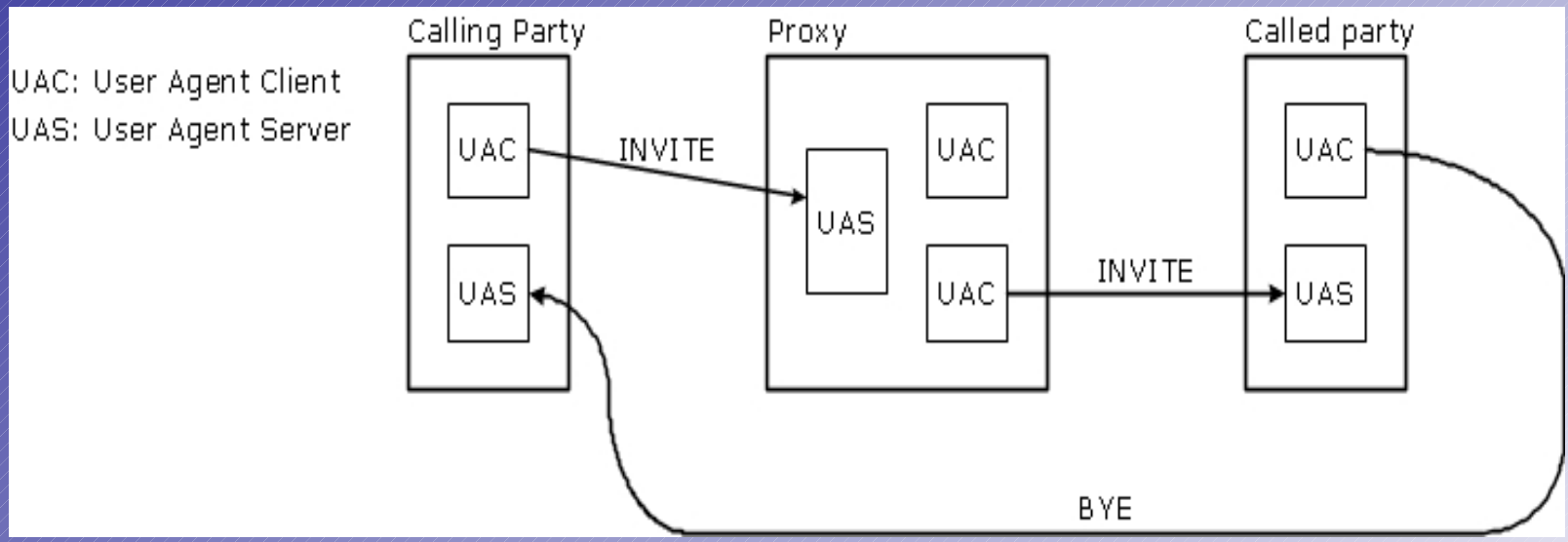
- SIP (RFC 3261) è un protocollo di segnalazione di livello applicativo sviluppato a partire dal 1999 per iniziativa dell'IETF. Esso è utilizzato per instaurare, modificare, o chiudere comunicazioni in tempo reale tra due o più entità, attraverso reti di tipo IP.
- Trova applicazione nella telefonia su IP e nei servizi telefonici supplementari, nella video-comunicazione, nei giochi interattivi, nella messaggistica istantanea.

SIP 2 / 2

- UDP / TCP / TLS
- Si basa su un'architettura client/server
- Funzionalità principali:
  - localizzare degli utenti
  - nagoziare i parametri di sesisone
  - instaurare una sessione (thee-way-handshaking)
  - gestire modifiche ai parametri di sessione
  - rilasciare le parti e cancellare la sessione

Architettura

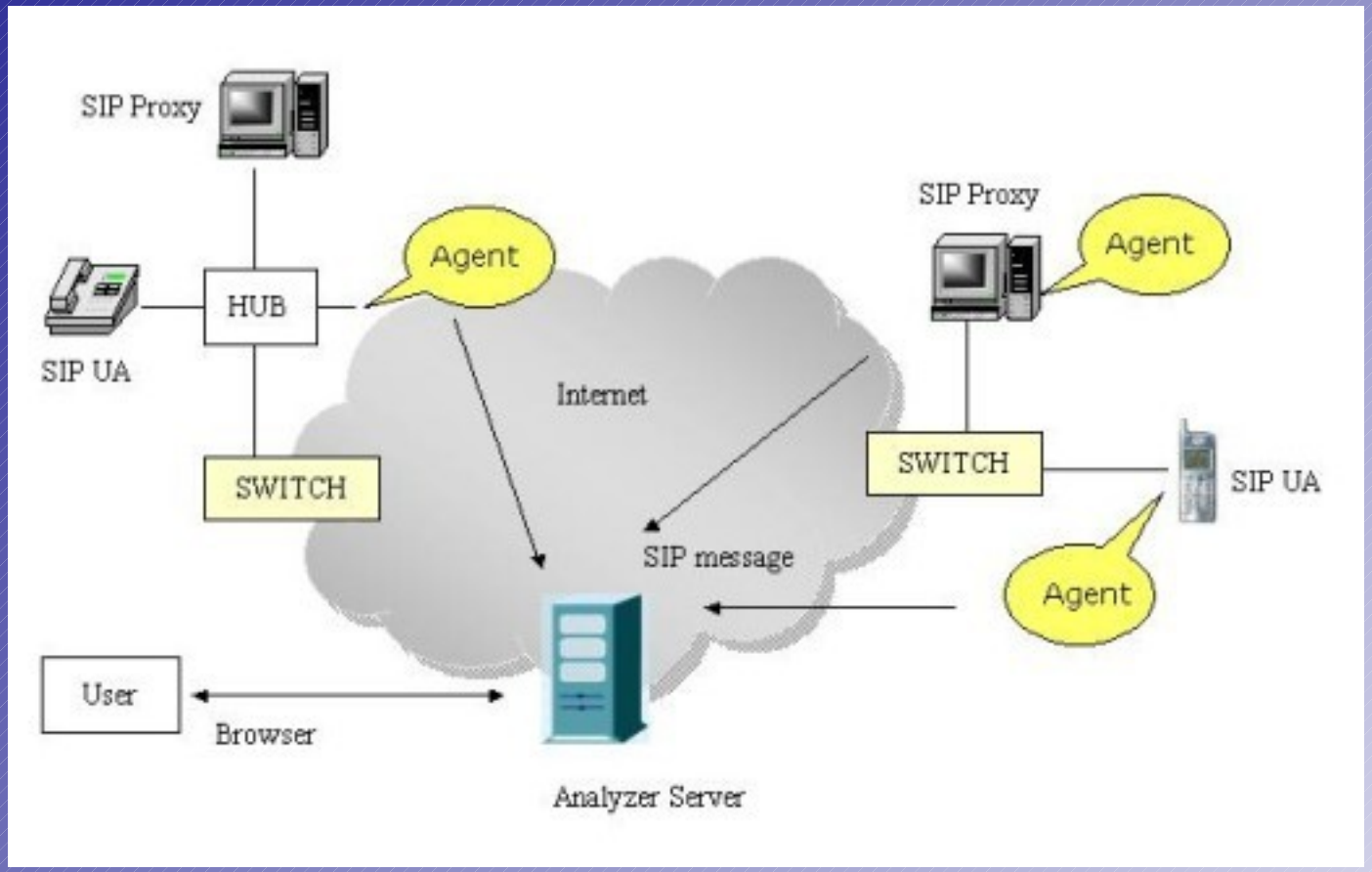
- SIP User-Agent
- Proxy Server



Stato dell'arte

- Il software preso in esame è il **SIPAnalyzer** della Advanced Network Technology.
- *Il progetto, seppur incompleto, è stato abbandonato nel 2000!*

SipAnalyzer: agent ed analyzer



Adattamenti ed estensioni

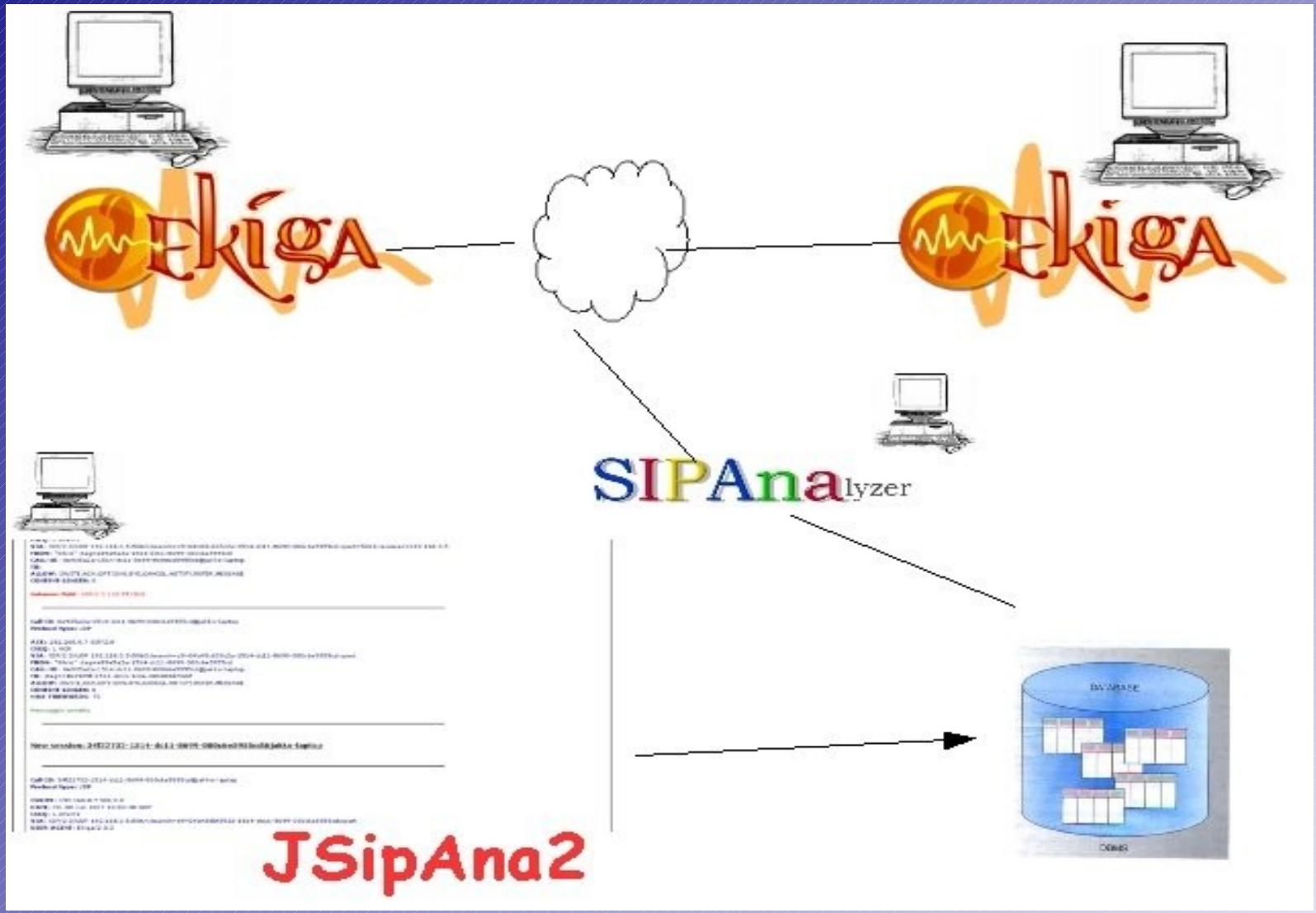
- aggiornamento del modulo di acquisizione dei pacchetti per il supporto di MySQL 5

- progettazione di un nuovo Analyzer

JSipAna2

- Java
- MySQL
- agent di SipAnalyzer
- motore di regole statiche e dinamiche
- interfaccia web

Architettura



Componenti

- WWW: Java Servlet e JSP
- Web Server: Apache Tomcat 5
- Database: MySQL
- Agent: C

- componenti modulari

Regole statiche

- ERROR_UNKNOWN_FIELD
- ERROR_FIELD_NOT_FOUND
- ERROR_DUPLICATED_FIELD
- ERROR_UNKNOWN_MESSAGE

Regole dinamiche

- applicazione di regole dinamiche sui metodi

Esempi ...

List messages | Dynamic rules

Messagges list

Call-ID: 62e1d6a3-1314-dc11-8937-000fb06abfda@none
Protocol type: UDP

INVITE: 192.168.0.7 SIP/2.0
DATE: Fri, 08 Jun 2007 09:52:30 GMT
CSEQ: 1 INVITE
VIA: SIP/2.0/UDP 192.168.0.2:5061;branch=z9hG4bK6c3fd8a3-1314-dc11-8937-000fb06abfda;rport
USER-AGENT: Ekiga/2.0.3
FROM: "LuCa" ;tag=c299d7a3-1314-dc11-8937-000fb06abfda
CALL-ID: 62e1d6a3-1314-dc11-8937-000fb06abfda@none
TO:
CONTACT:
ALLOW: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,REFER,MESSAGE\r\nContent-Length: 336
CONTENT-TYPE: application/sdp
MAX-FORWARDS: 70
SDP CONTENT:

```
v=0
o=- 1181296350 1181296350 IN IP4 192.168.0.2
s=Opal SIP Session
c=IN IP4 192.168.0.2
t=0 0
m=audio 5000 RTP/AVP 101 96 3 107 110 0 8
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:96 SPEEX/16000
a=rtpmap:3 GSM/8000
a=rtpmap:107 MS-GSM/8000
a=rtpmap:110 SPEEX/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
```

Mandatory field not found: CONTENT-LENGTH
Error Dynamic Rule: Found Ekiga in USER-AGENT: Test

... esempi

VIA: SIP/2.0/UDP 192.168.0.5:5063;branch=z9hG4bK8c635c2a-1514-dc11-8699-000c6e5955cd;rport=5063;received=192.168.0.5
FROM: "Silvio" ;tag=a89e5a2a-1514-dc11-8699-000c6e5955cd
CALL-ID: 0e935a2a-1514-dc11-8699-000c6e5955cd@jakko-laptop
TO:
ALLOW: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,REFER,MESSAGE
CONTENT-LENGTH: 0

Unknown field: SIP/2.0 100 TRYING

Call-ID: 0e935a2a-1514-dc11-8699-000c6e5955cd@jakko-laptop
Protocol type: UDP

ACK: 192.168.0.7 SIP/2.0
CSEQ: 1 ACK
VIA: SIP/2.0/UDP 192.168.0.5:5063;branch=z9hG4bK8c635c2a-1514-dc11-8699-000c6e5955cd;rport
FROM: "Silvio" ;tag=a89e5a2a-1514-dc11-8699-000c6e5955cd
CALL-ID: 0e935a2a-1514-dc11-8699-000c6e5955cd@jakko-laptop
TO: ;tag=74b2905f-1514-dc11-9c3a-00108bbf3ddf
ALLOW: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,REFER,MESSAGE
CONTENT-LENGTH: 0
MAX-FORWARDS: 70

Messaggio corretto

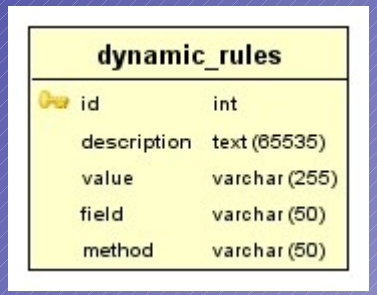
New session: 34f22732-1514-dc11-8699-000c6e5955cd@jakko-laptop

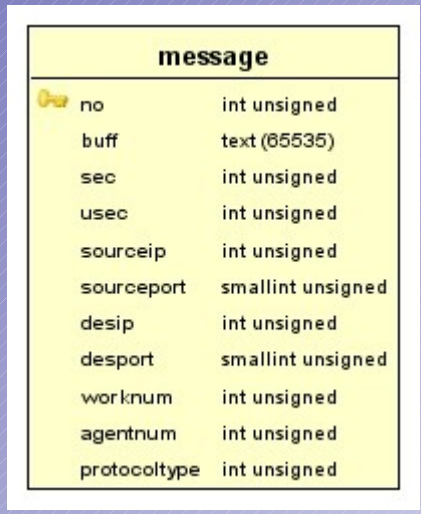
---

Call-ID: 34f22732-1514-dc11-8699-000c6e5955cd@jakko-laptop
Protocol type: UDP

INVITE: 192.168.0.7 SIP/2.0
DATE: Fri, 08 Jun 2007 10:03:38 GMT
CSEQ: 1 INVITE
VIA: SIP/2.0/UDP 192.168.0.5:5064;branch=z9hG4bK88bf2932-1514-dc11-8699-000c6e5955cd;rport
USER-AGENT: Eliga/2.0.3

Database





MESSAGE	FIELD	RULE	ID
INVITE	VIA	MANDATORY	1
INVITE	MAX-FORWARDS	MANDATORY	3
INVITE	TO	MANDATORY	4
INVITE	FROM	MANDATORY	5
INVITE	CALL-ID	MANDATORY	6
INVITE	CSEQ	MANDATORY	7
INVITE	CONTACT	MANDATORY	8
INVITE	CONTENT-TYPE	MANDATORY	9
INVITE	CONTENT-LENGTH	MANDATORY	10
INVITE	DATE	MANDATORY	52

id	description	value	field	method
2	(MEMO)	Ekiga	USER-AGENT	INVITE

Conclusioni

- analisi del protocollo SIP
- implementazione di un sistema di analisi delle comunicazioni SIP
- utilizzo di un software già esistente, per la cattura dei pacchetti e la memorizzazione su database MySQL
- sviluppo di un nuovo analizzatore in Java con interfaccia web
- motore di regole statiche e dinamiche

Sviluppi futuri

- Controllo di coerenza dei metodi in una sessione
- Implementazione di un parser di regole dinamiche
- Ristrutturazione dell'agent
- Storicizzazione dei risultati