

SIP 기반 IMPP 서비스를 위한 사용자 데이터 처리를 위한 XCAP 서버 설계

이 일진, 현 옥, 강 신각

한국전자통신연구원 표준연구센터

Design of XCAP server for IMPP Service based on SIP

Il-Jin Lee, Wook Hyun, Shin-Gak Kang

Protocol Engineering Center, ETRI

E-mail : lij1024@etri.re.kr

요 약

인터넷 사용자들의 급증으로 인터넷을 이용한 다양한 부가서비스들이 창출되고 있으며 가장 대표적인 것이 인터넷 전화이다. 최근들어 인스턴트 메시징 및 프레즌스 서비스의 응용서비스가 보편적으로 확대되고 있는 추세이며 이 서비스는 IETF의 IMPP 워킹 그룹에서 표준이 개발되고 있는데 IMPP 워킹그룹에서는 인스턴트 메시징 및 프레즌스 서비스를 위한 기본 모델 및 요구사항, 공통 데이터 포맷 등에 대한 표준을 담당하고 있다. 또한, 사용자의 친구 목록 관리 및 권한 부여 등 IMPP 서비스를 위한 확장은 SIMPLE 워킹그룹에서 정의하고 있다. 본 논문에서는 IETF SIMPLE(SIP for Instant Messaging and Presence Leveraging Extensions) 워킹그룹에 대한 표준 진행 사항과 IMPP 서비스에서 친구 목록 및 사용자의 권한 설정을 관리해주는 XCAP 서버 설계를 다룬다.

Abstract

IMPP service has been a promising technology as Internet grows fast and the requirements are increasing. IETF standardize requirements, model and data format for IMPP service via IMPP WG and SIMPLE WG. In this paper, we analysis SIMPLE WG in IETF and design consideration of XCAP server for IMPP services based on SIP

1. 서 론

인스턴트 메시징 및 프리젠스(IMPP) 서비스가 인터넷 사용자들의 급증으로 점점 인기를 더해가고 있다. 가장 대표적인 예가 MSN 메신저를 들수 있는데 친구 목록을 등록하고 등록된 친구들의 상태 정보 즉 프리젠스에 대한 정보를 제공받으므로써 상대방이 현재 어떤 상태인지를 알 수 있는 서비스이다. 상대방이 현재 접속가능한 상태일 경우(예, Online) 상대방과 메시지를 서로 주고 받을 수 있는 것인 인스턴트 메시징 서비스이며 이외에서 파일 전송과 같은 응용 서비스가 추가 되는 추세이다. IETF에서는 SIP 프로토콜을 이용

하여 멀티미디어 서비스를 제공하기 위한 표준화를 진행중이며 인스턴스 메시징 및 프리젠스 서비스를 제공하기 위하여 표준화가 진행 중이다. IMPP 서비스를 제공하기 위해서는 IMPP 단말에 해당하는 PUA(Presence User Agent)와 IMPP 서버에 해당하는 PA(Presence Agent)가 존재하여 PUA는 단말에게 자신의 상태 정보를 알려주고 단말에 각각의 단말에 대한 상태 정보를 저장하고 있다. 서버에게 상대방의 상태정보를 요청하는 사람을 와치라고 하며 이 와치에 대한 정보를 처리하기 위해 WatcherInfo 패키지라는 표준이 제정되었다. SIP기반의 프리젠스 서비스는 RFC 3265표준을 기반으로 서비스가 제공되는데 RFC

3265는 서버에게 상태정보를 요청하는 Subscribe 메소드와 서버에서는 요청받은 Subscribe 메소드를 처리하여 요청된 정보를 제공하는 Notify 메소드에 대하여 정의하고 있다. 최근 들어 이 서비스는 이동통신망에서도 관심을 갖고 관련 서비스에 대한 표준화가 진행 중인데 대표적인 표준화 단체가 OMA(Open Mobile Alliance)이다. 즉 이동통신망에서 상대방의 상태정보를 알 수 있으므로 상대방이 현재 통화를 할 수 있는 상태인지를 미리 알아 전화를 함으로써 유선 네트워크망과는 달리 자원이 제한되어 있는 이동통신망에서 상대방의 부재로 인한 재발신 또는 메시지 교환의 절차를 간단하게 줄일 수 있어 사용자의 편의를 높일 수 있을 것으로 기대된다.

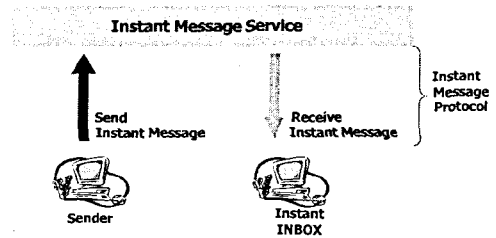
본 논문에서는 현재 IETF의 SIMPLE(SIP for Instant Messaging and Presence Leveraging Extensions) 워킹그룹의 표준화 진행 현황을 살펴보고 현재 SIMPLE 워킹그룹에서 표준화를 진행하고 있는 XCAP(XML Configuration Access Protocol) 표준기반으로 IMPP 서비스 시 사용자의 친구 그룹 목록 및 사용자 권한 설정을 관리해 주는 XCAP 서버 설계에 대해 살펴보고자 한다.

II. SIP 기반 SIMPLE 워킹그룹 표준화 현황

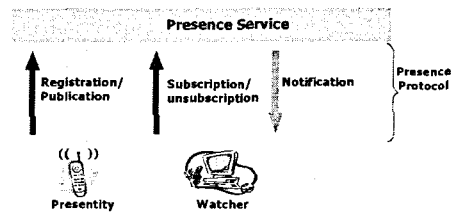
IMPP 서비스와 관련된 IETF의 워킹 그룹은 IMPP 워킹그룹과 SIMPLE 워킹그룹에서 표준화가 진행되고 있으며 IMPP 워킹그룹은 인스턴트 메시징 및 프레즌스 서비스를 위한 기본 모델 및 요구사항, 공통 데이터 포맷 등에 대한 표준을 담당하여 2004년 8월 워킹그룹에서 담당하는 것을 모두 표준화하여 클로우즈 된 상태이며, SIMPLE 워킹그룹은 SIP를 이용한 다양한 부가 서비스에 대한 관심이 증대되어 2000년 49차 IETF 회의에서 SIMPLE 워킹그룹이 발족되었으며, IMPP 워킹그룹, SIP 워킹그룹과 연계하여 SIP기반 인스턴트 메시징 및 프레즌스 서비스 관련 표준화 작업을 수행하고 있다.

SIMPLE 워킹그룹에서는 IMPP 워킹그룹에서 제시한 IMPP 모델 및 요구사항을 만족하는 범위 내에서, SIP 표준과 SUBSCRIBE/NOTIFY 메시지를 이용한 특정 이벤트 통지 표준 등을 근간으로 어떻게 서비스를 진행시킬 것인지에 대한 구체적인 표준화 작업을 수행하고 있으며, 2005년 8월 현재까지 4개의 RFC 문서와, 다수의 워킹그룹 I-D를 제안한 상태이다.

그림 1은 인스턴트 메시징을 제공하기 위한 서비스 모델을 보여 주며 그림 2는 프리즌스를 제공하기 위한 서비스 모델을 보여 준다.



(그림 1) 인스턴트 메시징 서비스 모델



(그림 2) 프리즌스 서비스 모델

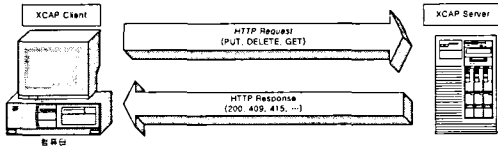
SIMPLE 워킹 그룹에서 다루고 있는 표준화 분야는 아래와 같다.

- 프레즌스 서비스 표준화 기술
- 리소스 리스트 표준화 기술
- 와쳐 정보 제공을 위한 표준화 기술
- IM 메시지 작성 상태를 통지하기 위한 기 표준화 기술
- XML기반 프레즌스 정보 데이터 포맷 확장 표준화 기술
- 세션기반 인스턴트 메시징 서비스 표준화 기술
- XCAP 표준화 기술
- Prartial Notification 표준화 기술
- 필터링 관련 표준화 기술

III. XCAP 서버 설계

그림 3은 XCAP 시스템의 일반적인 방식을 나타낸 것이다. XCAP은 HTTP 버전 1.1에서 클라이언트와 서버로 동작한다. 클라이언트에서는 사용자 정보를 읽고, 지우고, 검색할 수 있으며 이것은 HTTP의 PUT, DELETE, GET 메소드를 사용하여 처리할 수 있으며 서버에서는 사용자가 요구한 데이터를 자신의 DB에 저장하고 삭제하고 사용자가 요구한 데이터를 전송해 주는 역할을 한다. 사용자의 정보데이터는 HTTP 바디에 XML로 기술되어진다. XCAP 시스템은 여러 응용에서 사용되어 질 수 있다. IMPP 서비스를 위해 친구 목록 관리 및 사용자 권한 설정 등에 사용되어 질 수 있으며, 컨퍼런스 응용에서는 컨퍼런스에 참여하는 참여자에 대한 관리 및 컨퍼런스

생성 등에 사용되어 질 수 있다.



(그림 3) XCAP 클라이언트와 서버 시스템

본 논문에서는 IMPP 응용 서비스를 위한 XCAP 서버를 설계하였다. 그림 4은 IMPP 서비스를 제공하기 위해 사용자의 친구 그룹 목록에 대한 XML 데이터의 예를 보여주고 있다. 그림 5는 자신의 프렌즈 정보를 허용할지에 대한 권한 부여에 대한 XML 데이터의 예를 보여주고 있다.

```
<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists"
  xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance"
  <list name="friends">
  <entry uri="sip:bill@example.com">
  <display-name>Bill Doss</display-name>
  </entry>
  <entry ref="resource-lists/users/bill/mylist/~resource-lists/1
  is%2621st1%22%263dentry%26uri=%26sip:pat@example.com%22%263d"/>
  <list name="other-friends">
  <display-name>Joe Friends</display-name>
  <entry uri="sip:joe@example.com">
  <display-name>Joe Smith</display-name>
  </entry>
  <entry uri="sip:nancy@example.com">
  <display-name>Nancy Gross</display-name>
  </entry>
  <external anchor="http://www.example.org/xcap/resource-lists/users/a
  /foo/~resource-lists/1st%2621st1%22%263dentry%22%263d">
  <display-name>Marketing</display-name>
  </external>
  </list>
  </resource-lists>
```

(그림 4) 친구 목록에 대한 XML데이터 예

```
<?xml version="1.0" encoding="UTF-8"?>
<cr:ruleset
  xmlns:cr="urn:ietf:params:xml:ns:common-policy"
  xmlns:rpidd="urn:ietf:params:xml:ns:rpidd"
  xmlns="urn:ietf:params:xml:ns:pres-rules"
  xmlns:cr="urn:ietf:params:xml:ns:common-policy"
  xmlns:rs="urn:ietf:params:xml:ns:pidf:status:rpidd-status"
  xmlns:ts="urn:ietf:params:xml:ns:pidf:roid-tuple"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <cr:rule id="1">
  <cr:conditions>
  <cr:identity>
  <cr:uri>user@example.com</cr:uri>
  </cr:identity>
  </cr:conditions>
  <cr:actions>
  <sub-handling>allow</sub-handling>
  </cr:actions>
  <cr:transformations>
  <provide-tuples>
  <all-tuples></all-tuples>
  </provide-tuples>
  <provide-activity>
  <tuples-whose>
  <ts:class>friend</ts:class>
  </tuples-whose>
  </provide-activity>
  </cr:transformations>
  </cr:rule>
  </cr:ruleset>
```

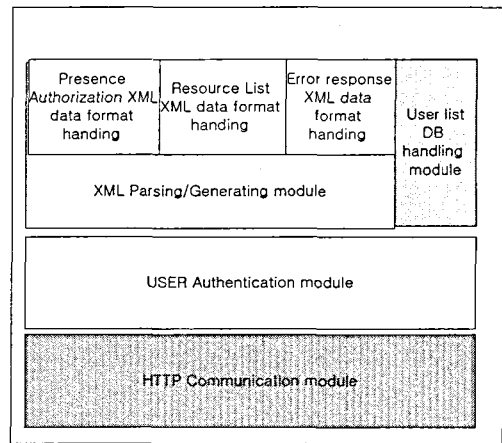
(그림 5) 프렌즈 권한 XML 데이터 예

그림 6은 IMPP 서비스를 위하여 설계된 XCAP 서버의 기능을 보여주고 있다. 설계된 XCAP 서버는 다음과 같이 클라이언트의 요구 사항을 수행하게 된다.

첫째 HTTP URL과 요청 메시지를 이해하여야 한다. 만약 클라이언트에서 요구한 application usage를 이해하지 못한다면 서버는 404(not found) 에러 응답 메시지를 클라이언트에 전송해야 한다.

다음으로 서버는 클라이언트에 대한 인증 처리를 하여야 한다. 이때 사용되는 것은 HTTP Digest 방식을 사용하여야 한다. HTTP 바디에 있는 사용자 데이터는 매우 중요한 데이터 이므로 보안에 대한 고려 사항이 있어야 한다.

HTTP 바디에 있는 XML 데이터를 처리하기 위하여 서버는 XML parsing/generating 모듈이 구현되어야 한다. XML 데이터 포맷이 well-formed XML인지 체크해야 하며 UTF-8로 인코딩되어 있는 지도 체크해야 한다. 또한 서버는 Content-Type 헤더 값이 각 application usage에서 정의한 MIME 타입과 같은 지를 체크하여야 한다. 만약 잘못 되었을 경우에는 409 에러 응답 메시지를 클라이언트에게 전송해야 하는데 이때 XML 데이터로 이루어진 바디 부분을 첨가하여 전송할 수 있다. 이 바디 정보에는 클라이언트가 이해할수 있도록 좀 더 구체적인 정보가 실려 있게 된다.



(그림 6) XCAP 서버 기능

그림 7은 HTTP 요청 메시지에 대한 XCAP 서버의 처리 절차를 보여주고 있다. 만약 서버가 POST 메소드를 수신하였을 경우에는 405 에러 응답 메시지를 전송하여야 한다. POST메시지에 대한 처리 절차는 정의되어 있지 않기 때문이다. 두 번째로 PUT 메소드를 수신하였을 경우, XCAP 서버는 해당 HTTP URL을 해석하여 클라이언트에서 요구한 특정 위치에 바디 정보를 지

장하여야 한다. 이때 전송된 바디 정보에 대한 검증 절차를 거쳐야 한다.

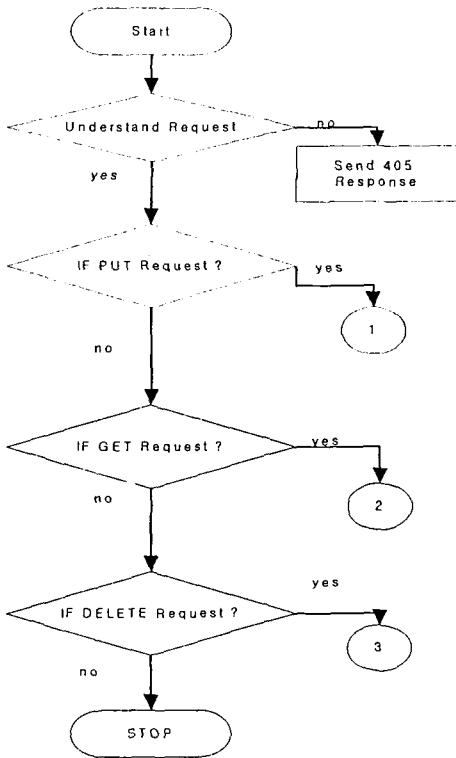
만약 GET 메소드를 수신하였을 경우, 서버는 해당하는 위치에 있는 정보를 읽어 200 OK 응답 메시지의 바디에 해당 정보를 실어 전송한다.

만약 DELETE 메소드를 수신하였을 경우, 서버는 해당 위치에 대한 정보를 삭제한 후, 수행한 결과가 성공 일 경우에는 200 OK 응답 메시지는 만약 실패하였을 경우 404 에러 응답 메시지를 클라이언트에게 전송하게 된다.

SIP 기반의 다양한 응용 서비스가 창출될 것으로 예측된다.

참고문헌

- [1] Rosenberg, et. al., "The Extensible Language (XML) Configuration Access Protocol(XCAP)", draft-ietf-simple-xcap-05(2004).
- [2] Rosenberg, " A presence Event Package for Session Initiation Protocol(SIP)", IETF RFC 3856(2004).
- [3] J. Rosenberg, "Presence Authorization Rules", draft-ietf-simple-presence-rules-01(2004).
- [4] Rosenberg, "Extensible Markup Language (XML) Formats for Representing Resource list", draft-ietf-simple-xcap-list-usage-04(2004).
- [5] J. Rosenberg, "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Manipulating Presence Document Contents", draft-ietf-simple-xcap-pidf-manipulation-usage-02(2004).



(그림 7) HTTP 요청 메시지 처리 절차

V. 결 론

본 논문에서는 현재 활발하게 표준이 제정되고 있는 인터넷 망에서의 인스턴트 메시징 및 프리젠텔스 서비스에 대한 IETF의 표준화 현황을 살펴보고 프리젠텔스 서비스를 위하여 사용자의 친구 목록을 관리하여 주는 XCAP 서버에 대한 설계를 살펴 보았다.

현재 SIP 기반의 VoIP 서비스 시장에 진출한데 이어 IMPP 서비스 및 좀더 확장된 응용 서비스에 대한 요구가 계속해서 증가할 것이며, 향후