
3rd Party SIP Registration 기능 지원을 위한 Registrar 서버

기능 설계

현 옥 · 강신각*

*한국전자통신연구원

Design of Registrar Server capable of 3rd party SIP Registration

Wook Hyun* · Shin-Kak Kang**

*Electronics and Telecommunications Research Institute

E-mail : whyun@etri.re.kr

요 약

인터넷 상에서 SIP을 사용한 VoIP 서비스를 제공하기 위해서는 사용자의 위치 정보 추적 및 Call의 적절한 전달을 위한 사용자의 현재 위치에 대한 정보를 Registrar 서버에 등록을 해야 한다. SIP의 REGISTER 메시지를 사용하여 사용자의 SIP URI 주소와 하나 이상의 현재 접근 가능한 주소를 등록을 하게되며, 이때 등록되는 주소는 SIUP URI에만 제한된 것이 아니라 mailto, http, tel 등 여러 스킴을 등록할 수 있다. 사용자의 위치 정보 들고의 과정에서는 인증에 대한 고려가 필수적으로 이루어져야 한다. 본 논문에서는 이 과정에서 이루어지는 서버와 클라이언트간의 트랜스액션에 대한 내용과 제 3자에 의한 등록 기능을 가능토록 하게 하기 위한 서버측에서의 고려사항과 이를 지원하기 위한 서버의 기능 설계에 대한 내용을 다루도록 하겠다.

ABSTRACT

In order to provide VoIP service that using SIP on the Internet, users must register their current location to receive call from other caller. By using REGISTER method, users register his or her SIP URL address and currently contactable addresses to registrar server. The registered addresses are not only SIP URI but also mailto, http, tel, and so on. In these procedures, we must consider authentication mechanism whether he/she has authority to handle the record or not. In this paper, we will briefly describe authentication mechanism that used in SIP and design of registrar server that support the 3rd party registration.

키워드

VoIP, SIP, Registrar, 3rd party Registration

1. 서 론

VoIP 서비스를 제공하기 위한 세션 제어 프로토콜로는 크게 H.323과 SIP (Session Initiation Protocol)[1] 두가지로 나누어 볼 수가 있다.

H.323 은 ITU-T의 표준으로써 이미 표준화가 오랜기간동안 진행되어 왔으며 현재의 VoIP를 위한 시그널로서 가장 많이 사용되고 있다. 그러나 IETF에서 제안된 SIP은 프로토콜의 단순함과 다양한 확장성의 제공을 장점으로 하여 H.323 의

영역을 대체해 나가고 있다. 원래 SIP는 멀티캐스트 상에서의 세션 설정을 위해 사용되던 프로토콜이었으며, 이 당시에는 그리 각광 받지 못하다가 VoIP를 위한 프로토콜로 사용되면서 급격한 발전을 이루고 있으며, 현재도 지속적인 표준화가 진행 중이다. 멀티캐스트를 위한 SIP에 VoIP 서비스를 위한 기능들을 추가 및 수정함으로써 SIP-bis 버전의 형태로 현재 개발되어지고 있다. SIP을 사용한 VoIP Call 설정을 위해서는 사용자의 위치 정보에 대한 접근이 가능해야만 한다. 사용자는 주기적 또는 원칙에 근거한 방식으로 자신의 현재 위치를 Registrar 서버에 알려주어야 하며, 이 정보를 토대로 다른 사용자로부터의 Call을 받을 수가 있게 된다. 이 과정에서 위치 정보의 제한적 접근 및 갱신을 위해서는 반드시 인증 과정을 통해 등록 요청의 유효 여부를 판단하여야 하며, RFC 2543-bis-04에 정의된 인증 알고리즘으로는 Basic, Digest 두가지가 있다. 본 고에서는 각 알고리즘이 SIP의 등록과정에서 적용되는 방식과 제 3자를 통한 등록대행 기능 지원을 위한 Registrar 서버의 설계에 대한 내용을 다루도록 하겠다.

2. SIP Registration

1. SIP Registration Procedure

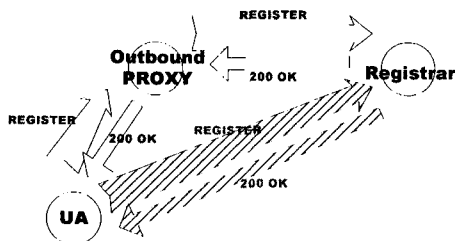


그림 1 SIP registration procedure

UA가 자신의 위치 정보를 등록하는 방법을 크게 두가지로 나누어 보면, local outbound proxy를 통해 등록하는 방법과 직접 Registrar로 REGISTER 메시지를 통해 등록하는 방법이 있다. REGISTER 메시지에 대하여 Registrar는 자신의 데이터베이스 내의 해당 사용자의 위치정보를 삽입, 갱신, 삭제 등의 처리를 통해 최종 결과를 200 OK 응답에 실어서 보내게 되며, 외부에서 Call을 전달할 때 이 정보를 토대로 현재 사용자에게 접근할 수가 있게 된다.

2. REGISTER Message

REGISTER에 사용되는 주요 헤더 및 정보들은 다음과 같다.

- Request-URI : Register 하는 도메인이나 registrar의 주소를 나타낸다.

- To 헤더 : Register 될 address-of-record를 의미하며 해당 사용자에게 유일하게 부여된 주소를 나타내며, 이 정보를 키값으로 사용하여 데이터베이스 내의 데이터를 처리하게 된다.

- From 헤더 : Register를 실제 수행하는 사용자의 address-of-record를 의미한다. 일반적으로 자신의 정보를 자신이 직접 등록할때는 To 헤더의 내용과 같은 값을 가지나, 제 3자 등록의 경우에는 다른 값을 가지게 된다.

- Contact 헤더 : 이 헤더가 존재하지 않을 경우에는 등록 내용이 변경되지 않으며, 현재 등록된 내용을 알고자 할 때 유용하게 사용될 수 있으며, 현재 등록된 정보와 다르면 추가를 하며 같은 경우에는 갱신의 작업을 한다. '*'을 사용하여 ALL의 의미를 나타낼 수 있으며, Expires 헤더의 값에 따라 특정 레코드 또는 전체 레코드를 삭제 또는 갱신을 할 수가 있다.

- Expires 헤더 : 해당 레코드의 유효 시간을 지정한다. 특별히 지정이 없을 경우에는 디폴트로 3600초를 사용한다. 헤더의 값이 0 일 경우에는 Contact 헤더에 명시된 주소들에 대한 정보를 삭제한다.

3. Authentication mechanism for SIP

현재 RFC 2543-bis-04 버전에 명시된 인증 메커니즘은 Basic 방식과 Digest 방식이 있다. [2] 03버전 이전에는 PGP도 포함되어 있었으나 03버전 이후부터 PGP는 제외되었으며, 각 메커니즘의 동작 방식은 다음과 같다.

3.1 Basic

Basic 인증 스킴을 사용한 WWW-Authenticate 헤더의 문법은 아래와 같다.

```

challenge = "Basic" realm
credentials = "Basic" basic-credentials
    
```

UA로부터의 REGISTER 메시지에 대해 Registrar는 401 응답에 challenge를 실어서 보내게 되면, 이를 수신한 UA에서 credentials 정보를 실어서 보내주게 되어 있으며, 일반적으로 basic-credentials의 내용은 ID와 비밀번호의 문

자열을 base64 인코딩 방식으로 변환한 내용을 보내주게 된다. 그러나 이 방식은 이 메시지의 내용을 용이하게 디코드할 수 있으므로, 스니퍼링 등의 네트워크 스캐닝을 통한 접근에는 치명적이므로 그리 안전하지는 않은 방식이다.

3.2 Digest

Digest 방식을 사용한 WWW-Authenticate 헤더의 문법은 아래와 같다.

```
challenge = "Digest" digest-challenge
digest-challenge =
1#[realm|domain|nonce|opaque|stale|
algorithm|qop-options|auth-param]
```

Registrar로부터 인증에 관련된 challenge는 401 응답에 넣어져서 보내지는데, 이 헤더를 가진 응답을 받으면, Authorization헤더를 포함한 request를 다시 보내어 인증 검증을 재시도 하게 된다.

domain에는 해당 서버의 도메인명을 기록을 하며 realm에는 사용자에게 자신을 구분하기 용이하게 하기 위한 문자열이, nonce에는 401 메시지가 생성될 때마다 유일하게 생성되는 서버측 데이터 문자열로써 네트워크 스캐닝을 통한 인증 정보 유출을 막기위해 항상 새로운 값이 설정이 된다. opaque는 서버에서 생성된 문자열로서 클라이언트는 이 값을 바꾸지 말고 바로 리턴시켜 주어야 한다. algorithm은 관련 정보들을 인코딩할 때 사용되는 알고리즘을 의미하는데 일반적으로 MD5가 가장 많이 사용되고 있다.

```
credentials = "Digest" digest-response
digest-response =
1#(username|realm|nonce|digest-uri|response|algorithm|cnonce|opaque|message-qop|nonce-count|auth-param)
```

이에 대한 credential 정보를 생성할 때, username에 자신의 아이디를 입력을 하며 realm은 서버로부터 수신한 문자열을 그대로 사용하며, digest-uri는 Request-Line의 Request-URI값을 그대로 사용한다. challenge를 통해 받은 인증을 위해 필요한 정보들과 함께 사용자의 password를 함께 algorithm에 명시된 알고리즘을 통해 인크립션을 한 후 전송을 하게 되며, 이를 수신한 Registrar 서버는 자신이 유지하고 있는 데이터베이스내의 해당 사용자의 아이디와 password 정보를 사용해 헤더에 포함된 정보와 함께 one-way encryption을 수행하고 이 결과와 response에 기록된 결과와의 일치여부를 판단하는 방식으로

수행된다.

4. 3rd Party Registration

제 3자 등록기능은 일종의 비서 기능으로써 사용자의 아이디와 비밀번호를 통하여 해당 사용자의 정보를 타인이 수정할 수 있게 하는 기능이다. SIP 상에서의 이 기능 지원을 위하여 From에는 등록을 대행하는 사용자, 즉 비서,의 SIP URL이 들어가며 To 헤더에 실제 변경하고자 하는 SIP URL이 들어가게 된다. 인증 처리를 위하여 Authorization 헤더에 알맞은 스킴으로 인코딩된 데이터들이 들어감으로써 Registrar 서버에서의 인증이 가능하게 한다. 이러한 기능이 지원되려면 Registrar에서는 인증 기능을 수행 할 수 있어야 하며 해당 사용자에 대한 정보를 유지하고 있어야 한다. 특히 사용자의 아이디, 비밀번호 그리고 그 사용자의 SIP URL을 하나의 데이터베이스에서 유지 또는 접근 가능하게 하여야 한다.

5. Design of Registrar Server for 3rd party Registration

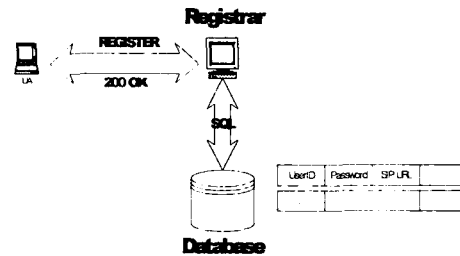


그림 2 3rd party registration

제 3자에 의한 등록을 가능하게 하기 위해서는 Registrar가 유지하는 Database내에 해당 사용자에 대한 인증정보와 함께 그 사용자에게 할당된 address-of-record, 즉 그 사용자의 SIP URL을 함께 유지하고 있어야 한다.

제 3자가 등록시에는 From헤더에는 실제 등록을 행하는 사용자의 SIP URL을 명기하며, 변경하고자 하는 address-of-record는 To 헤더에 기록을 하여, Authorization 헤더에 Basic 또는 Digest기법을 사용하여 사용자의 인증정보를 함께 넣어서 보낸다. 이를 수신한 Registrar는 먼저 Authorization 헤더내의 인증에 관련된 정보의 유효성을 점검하고 해당 사용자가 To 헤더에 명기된 주소에 대한 접근 권한이 있는지 점검을 해주어야 한다.

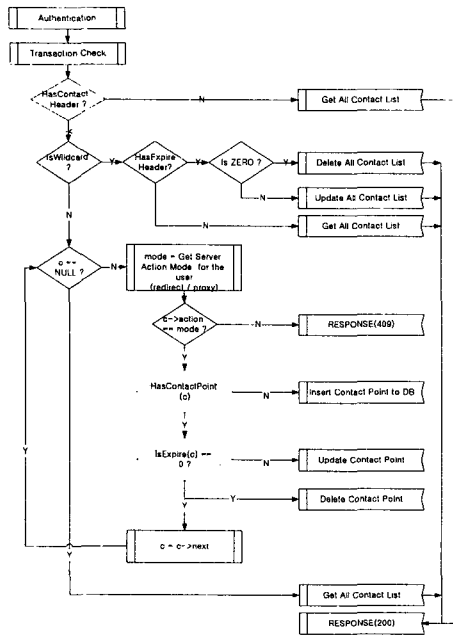


그림 3 Registrar operations

Registrar에서는 이상과 같은 과정을 거친 후 그림 3과 같은 Registration 처리를 거쳐 생성된 응답을 전송하게 된다.

6. 결론

본 고에서는 3rd party SIP Registration을 지원하기 위해 기본적으로 제공되어야 할 SIP Registrar 서버의 인증 기능과 3자 등록을 위해서 추가적으로 유지되어야 할 정보들과 동작 흐름에 대하여 논하였다. Registrar 는 SIP을 통한 Call의 전달에 있어서 필수적인 component이며 해당 도메인내의 사용자들에 대한 위치정보에 대한 관리를 수행하며, 제 3자 등록등을 포함한 다양한 부가적인 기능을 추가함으로써 사용자에게 여러 부가서비스들을 제공할 수 있다.

참고문헌

- [1] RFC2543-bis-04, "Session Initiation Protocol"
- [2] RFC2617, "HTTP Authentication: Basic and Digest Access Authentication"