반도체디스플레이기술학회지 제15권 제4호(2016년 12월)
Journal of the Semiconductor & Display Technology, Vol. 15, No. 4. December 2016.

SIP 등록취소 공격에 대한 단순한 방어 기법

권경희†
†단국대학교 소프트웨어학과

Simple Protection Method against Deregistration Attack in SIP

Kyung Hee Kwon†
†Department of Software Science, Dankook University

ABSTRACT

Although deregistration attack is caused by simple spoofing the REGISTER message of a legitimate SIP UA, its impact is serious. The root cause of this attack is based on the fact that RFC 3261 allows the UA to remove the *binding* from the Location Server. In this paper, we propose a simple protection method to allow Registrar or Location Server just to ignore deregistration messages. We also show that this method works well by analyzing the process of registration and deregistration. Without any additional overhead such as an encryption or authentication, this method is able to establish a secure SIP environment efficiently protecting against the deregistration attack.

Key Words : SIP, Deregistration Attack, Impersonation Attack, Ignoring Deregistration Message, Removing Binding

1. 서 론

VoIP(Voice over IP)는 음성을 광대역 인터넷 연결을 통해 전달해주는 기술로써, 그 저렴한 이용료로 인해 기존의 아날로그 전화 회선을 급속하게 대체하고 있다. 인터넷 전화라고 불리기도 하는 이 기술이 실용화되기 위해서는 인터넷에 연결된 서버가 원격지에 서로 떨어져 있는 통신 기기를 찾아내고, 그들 사이에서 음성의 흐름을 제어해 주는 많은 프로토콜이 필요하다. 가장 핵심적인 프로토콜은 콜 시그널링 프로토콜(Call Signaling Protocol)로써, 1990년대 중반 이후부터 이러한 용도의 프로토콜로 SIP(Session Initiation Protocol), H.323, RAS(Registration Admission Status), TRIP(Telephony Routing over IP)이나 ENUM(E.164 Number to URI Mapping) 등이 제안되었다. 이 중에서도 IETF(Internet Engineering Task Force)가 제안한 SIP는 그 단순함, 멀티미디어로의 확장성, 이동성, 양방향 인증 등의 이점으로 인해 가장 많은 주목을 받고 있으며 VoIP에 채택되어 전 세계적으로 널리 사용되어지고 있다.

†E-mail: khkwon@dankook.ac.kr

SIP[1]는 사용자 세션(User Session)의 관리에 필요한 시그널링 과정을 규정한 응용계층의 프로토콜로써, 전송계층으로는 UDP와 TCP를 모두 사용할 수 있으며 HTTP (Hypertext Transfer Protocol)와 유사한 요구-응답 프로토콜이다.

1996년에 처음 고안되어, 단순한 인증 기능만을 보안의 수단으로 제공했지만, SIP RFC(Request for Comments) 3261[1]에서 응용계층에서는 HTTP 다이제스트 인증 방식과 S/MIME(Secure/Multipurpose Internet Extensions), 전송계층에서는 TLS(Transport Layer Security), 그리고 네트워크 계층에서는 IPSec(Internet Protocol Security)의 사용을 권고 하고 있다. 그러나 다이제스트 인증 방식은 메시지의 헤더와 파라미터가 암호화되지 않아 공격자에 노출될 수 있고, S/MIME는 공개키 배포에 문제가 있으며 TLS와 IPSec은 성능에 심각한 저하가 있어[3], 아직 널리 사용되지 못하고 있는 실정이다. 그리고 VoIP 서비스를 이용하는 응용들이 상대적으로 강력한 보안을 요구하지 않는 경우가 많아 비용과 효율의 측면에서 완벽한 보안을 제공하는 VoIP 시스템이 많지 않기도 하다. 이로 인해 SIP는 재연공격(Replay Attack)이나 요구 메시지(Request Message)

스푸핑에 너무 쉽게 노출되어 있다.

이렇게 SIP가 갖고 있는 많은 보안상 취약점 가운데에서도 가장 쉽게 공격자에게 노출될 수 있는 것이 등록취소 공격이라 볼 수 있다. SIP를 통해 통신하고자 하는 통신 기기들은 반드시 SIP를 구성하는 서버(Server)들 중의 하나인 위치 서버Location Server)에 그 위치를 등록해야 하는데, SIP에서는 위치 서버에 등록된 레코드를 제거할 수 있는 요구 메시지가 허용되고 있기 때문에, 공격자가 요구 메시지를 스푸핑하여 위치 서버에 등록된 레코드를 삭제하는 공격이 가능한데 이것이 바로 등록취소 공격이다. 이는 매우 쉽게 시도될 수 있는 공격이지만, 공격받은 이용자는 통신 불능 상태가 되며 특히 공격 대상이 미디어 게이트웨이처럼 다수의 이용자 그룹이 사용하는 곳이라면 그 피해는 더욱 심각하다고 볼 수 있다. 또한 위치 서버에 위장 등록을 하기만 하면 쉽게 등록 하이재킹 공격으로 이어질 수 있는 공격이다.

이러한 등록취소 공격을 방어하기 위한 몇몇 기법들이 소개되었지만, 암호화 메커니즘을 추가하거나 인증 키를 빈번히 갱신하거나 인증의 단계를 추가하는 기존 기법들은[4-7] 인증과 암호화 알고리즘으로 인한 오버헤드를 발생시키고 시스템의 부하를 증가 시키는 단점이 있다.

[2]에서는 추가적인 인증 및 암호화를 일체 사용하지 않고도 등록취소를 단순히 지연시킴으로써, 등록취소 공격을 간단히 방어할 수 있는 새로운 기법을 제안하였으나, 이 또한 유효기간이 “0”인 경우 만을 고려하였기 때문에 완벽하게 등록취소 공격을 방어할 수 없을 뿐만 아니라 등록취소를 지연시키는 오버헤드를 갖는 문제점이 있다.

따라서 본 논문에서는 단순히 등록취소 요청을 무시함으로써 등록취소 공격을 방어하는 메카니즘을 제안하고 이 메카니즘이 잘 작동하는 것을 보여 준다. 본 논문의 구성은 다음과 같다. 2장에서는 SIP 등록취소 공격을 하기 위해 필요한 과정을 분석한다. 3장에서는 SIP 등록취소 공격을 방어하는 메커니즘을 제안한다. 마지막으로 4장에서는 결론을 제시한다.

2. SIP 등록취소 메커니즘

2.1 SIP 구성과 등록

SIP는 크게 UA(User Agent)와 서버(Server)들로 구성되어 있다. UA는 SIP 세션에서 호출자와 피호출자인 단말기의 논리적 표현이다. 즉 IP전화기나 컴퓨터 등을 지칭하며 요청 메시지를 보내는 UAC(User Agent Client)와 요청 메시지를 받아 들여 이에 응답하는 UAS(User Agent Server)로 구성된다. 서버는 UA들 간의 세션을 관리해주기 위한 일종의 중계 장치로 프록시 서버(Proxy Server), 리다이렉트 서버(Redirect Server)와 등록 서버(Registrar) 등의 세 종류가 있다. 프록시 서버는 UA로부터 수신한 접속 요청 메시지가 해당되는 UA로 전달될 수 있게 하는 기능을 수행하고 과금(billing)을 위한 정보를 유지한다. 리다이렉트 서버는 수신한 접속 요청 메시지를 다른 UA나 프록시 서버에게 직접 전달하지 않고, 접속 요청 메시지를 재전송해야 할 UA나 프록시 서버의 주소를 알려주는 역할을 한다.

등록 서버는 SIP UA의 정확한 위치 정보를 유지하기 위해 위치 정보를 등록하고, 필요에 따라 수정 및 삭제 작업을 수행하기도 한다. UA가 다른 UA로부터 메시지를 수신하기 위해서는 사전에 반드시 등록 서버에 등록되어야만 하므로 UA는 부팅되자마자 등록 요청 메시지인 REGISTER 메시지를 등록 서버로 보내어 등록해야한다.

SIP를 이용한 멀티미디어 세션을 관리하기 위해 필요한 서버의 개수나 구성의 복잡도는 그 응용에 따라 다르지만, UA의 등록을 살펴보기 위해서는 Fig. 1과 같은 단순 구성만 고려해 보면 된다.

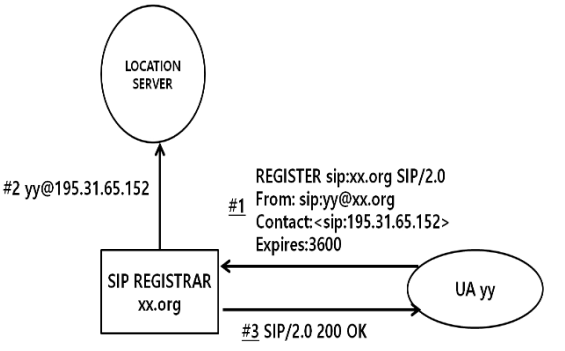

Fig. 1. Procedure of UA Registration.

Fig. 1은 UAyy가 REGISTER 메시지를 보내고 등록 서버가 이를 받아 UAyy의 위치를 위치 서버에 저장하는 순서를 나타낸 것이다. 이 위치 서버는 추상적인 개념으로 Fig. 1과 같이 등록 서버와 별로도 분리되어 있을 수도 있고 등록 서버 내에 존재할 수도 있다. 그리고 Fig. 1의 #1 다음에 등록 서버와 UA 사이에 인증하는 절차가 추가될 수도 있으나 그것은 인증을 위한 메시지 교환만 추가될 뿐 네트워크의 구성은 같다.

2.2 등록 취소

REGISTER 메시지를 수신한 등록 서버는 그 메시지를 보낸 UA의 위치 정보를 위치 서버(Location Server)로 보내 데이터베이스에 저장하게 한다. 이 때 위치 정보란

UA의 URI인 AOR(Address of Record)과 UA 자신이 로그인 될 실제 단말기 주소인 *'contact'* 주소를 매핑해 주는 레코드의 매핑(*Mapping*)이며 이를 바인딩(*Binding*)이라 부르는데, REGISTER의 헤더 필드 들을 이용하여 Table 1과 같이 저장한다.

이 때 UA는 이 등록의 유효기간을 명기할 수도 있고, 등록서버가 서버의 정책에 의해 임의로 선택 할 수도 있다.

Table 1. Fields of Binding Stored in Lacation Server

이름	내용
id	DB의 고유 ID
username	등록 메시지의 'From' 헤더 필드의 값
domain	등록 메시지의 도메인
contact	등록 메시지의 'Contact' 헤더 필드의 값인 SIP URI
received	전송받은 IP:PORT
path	등록 메시지의 'Path' 헤더 RFC 3327
expires	등록 메시지의 만료시간
q	우선시되는 라우팅 값
call-id	등록 메시지의 'Call-ID' 헤더 필드의 값
cseq	등록 메시지의 'Cseq' 헤더 필드의 값

UA가 유효기간을 명기하는 방법으로는 REGISTER 메시지의 헤더 필드인 *'Expires'*나 *'contact'* 헤더 파라미터인 *'expires'*에 값을 설정하는 두 가지가 있으며 어떤 값도 설정되어 있지 않다면 등록 서버가 서버 정책에 의해 독자적으로 값을 설정하게 된다. 어느 경우든 등록은 시간이 지나면 위치 서버에서 위치 정보가 삭제되어 등록은 무효화된다.

SIP에서 등록취소 공격이 쉽게 가능한 주된 이유는, 위치 서버에 저장된 바인딩의 유효기간을 '0'으로 설정하여 등록을 삭제하는 메시지를 현재의 SIP RFC 3261이 허용하고 있기 때문이다. 이는 유효기간 전에 종료된 UA를 위치 서버의 데이터베이스에 계속 유지함으로써 생기는 부하를 줄이기 위한 것이다. 예를 들면 소프트 폰을 로그오프(Logoff)한다던가 IP 폰의 전원을 끄는 경우, 이들의 바인딩을 위치 서버에서 삭제하는 것이다.

바인딩을 삭제하는 방법에는 두 가지가 있는데, REGISTER 메시지의 헤더 필드인 *'Expires'*에 *'0'*을 설정하는 방법은 모든 바인딩을 삭제할 때 주로 사용되고, contact 헤더 파라미터 *'expire'*에 *'0'*을 설정하는 방법은 특정 바인딩을 삭제할 때 사용된다. 편의상, 본 논문에서는 이렇게 변조된 메시지를 등록취소 메시지라고 부르기로 한다. 그리고 *Expires'*와 *'expire'*에 *'0'*보다 큰 값이 설정되더라도 그 크기가 SIP에서 설정한 값보다 작을 경우에는 그 설정된 시간이 경과한 후에는 등록이 취소되므로 등록취소 메시지와 같은 효과를 가진다. 따라서 본 논문에서는 *Expires'*와 *'expire'*에 *'0'*보다 큰 값이 설정된 등록메세지를 편의상 확장된 등록취소 메시지라 부르기로 한다.

등록취소 공격의 시나리오는 다음과 같다.

1) 먼저 등록 서버와 정상적인 SIP UA 사이의 REGISTER 메시지를 스푸핑한다. 통상적으로 SIP 는 TCP보다는 UDP 상에서 수행되므로 요구 메시지 스푸핑은 매우 용이하다. 그리고 현재 많은 SIP의 등록 서버는 인증을 반드시 요구하지도 않고, 인증을 요구한다하더라도 이용자 이름, 패스워드, 그리고 넌스(Nonce)의 MD5 다이제스트를 사용한다. 이용자 이름은 일상의 생활에서 유출되기 쉽고 패스워드는 기계적으로 생성되는 일정한 패턴을 갖고 있어 유추하기 쉬워 강력한 인증 수단은 되지 못한다.
2) 등록취소 메시지나 확장된 등록취소 메시지를 보낸다.

이처럼 등록 메세지를 스푸핑하여 등록취소 메시지나 확장된 등록취소 메세지를 만들기만 하면 등록취소 공격은 매우 쉽게 이루어지며, 그로 인한 피해는 심각하기 때문에 이에 대한 대책이 절실하지 않을 수 없다.

3. 제안하는 메커니즘

등록취소 공격이 쉽게 이루어지는 만큼 그 방어 방법도 간단한데, 그것은 단순히 등록취소 메시지를 무시하는 것이다. 즉, 현재에는 등록취소 메시지를 수신하면 위치 서버에서 바인딩을 제거하지만 이를 무시하면 약간의 시간적 지연이 있은 후에 저절로 위치 서버에서 바인딩을 제거되어 지며, 등록취소 공격은 일어날 수 없다는 것이다. 본 장에서는 등록취소 공격을 분석해보고 새로운 메케니즘을 제안한다.

기술의 편의상 본 논문에서는 정상적 UA가 위치 서버에서 바인딩을 제거하려는 등록취소 메시지를 선의의 등록취소 메시지라 하고, 공격자에 의해 만들어진 등록취소 메시지를 악의의 등록취소 메시지로 부르기로 한다. 그리고 확장된 등록취소 메시지는 모두 위조된 것이기 때문에 악의적 등록취소 메시지로 간주한다.

3.1 등록취소 공격 분석

등록된 정상적 UA는 유효기간이 끝난 후, 재등록을 하는 등록 과정을 다시 되풀이하게 된다. 특히 인증을 요구하는 등록 서버에 대해서는 인증 과정까지 반복하는 부하가 있어, SIP에서는 등록을 반복하는 대신 주기적으로 유효기간만을 재설정(Refresh)하는 방법을 사용한다. 즉 UA는 위치 서버에 저장된 바인딩을 유지하기 위해 첫 번째 REGISTER 메시지에서 설정한 유효기간이 끝나기 전에 주기적으로 REGISTER 메시지를 다시 보내 유효 기간을 재설정한다. 3GPP(3rd Generation Partnership Project)는 기본값(Default)으로 유효기간은 1시간으로, 그리고 유효기간 동안 2번 재설정하기를 권고하고 있다.

등록취소 메시지의 처리 과정을 경우에 분석해 보면 다음과 같다.

1) 선의의 등록취소 메시지를 수신한 경우, 등록은 즉시 취소되며, 유효기간 재설정을 위한 REGISTER 메시지는 오지 않는다.
2) 악의의 등록취소 메시지를 수신한 경우, 공격에 대비하지 않았다면 즉시 등록은 취소되고 통신 장애가 유발된다. [2]에서와 같이 공격에 대비했다고 하더라도, 등록 서버는 설정된 유효기간 동안 기다린 후, 위치 서버의 데이터 베이스에서 바인딩을 제거한다. 그리고 일정 시간 후에 유효기간 재설정을 위한 REGISTER 메시지는 다시 도착한다. 그러면 그 일정 시간 동안 등록은 취소된다. 이러한 공격이 반복되면 유효기간 재설정을 위한 등록 메시지는 다시 도착하더라도 계속 등록은 취소되며 그 기간 동안 등록 하이재킹 공격이 가능하게 된다.

3.2 등록취소 메시지 무시

등록취소 메시지를 완전히 무시하게 되면, 공격자로부터 등록취소 공격을 쉽게 방어할 수 있는데 이는 정상적 UA가 유효기간 재설정을 위한 등록 메시지를 주기적으로 전송하기 때문이다.

Fig. 2에서 보는 바와 같이, 시간 t3에서 선의의 등록취소 메시지를 수신한 경우에 이를 무시하면 바인딩이 즉시 제거되지 않고, 등록된 시간으로부터 유효기간 T가 경과한 후인 t4에 등록이 취소되어 원래 의도한 시간보다 t4-t3 만큼 더 위치 서버의 데이터 베이스에 바인딩이 존재하는 오버헤드가 발생한다. 그러나 이 오버헤드는 데이터 베이스라는 장소에서 미미하게 발생되는 반면 등록을 취소하기 위해 데이터 베이스에서 바인딩을 검색하여 삭제하는 시간적 오버헤드는 오히려 없어진다.

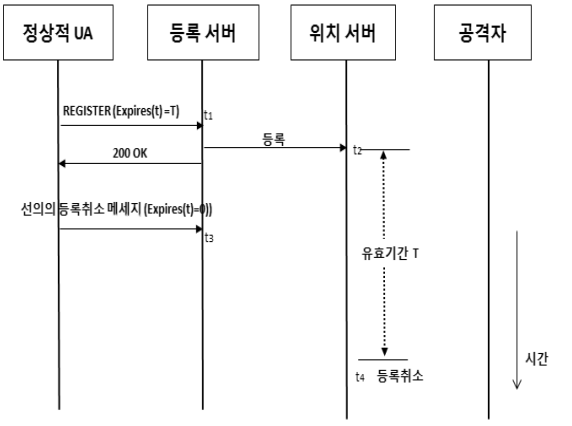

Fig. 2. Ignoring Legitimate Deregistration Message.

그리고 Fig. 3에서 보는 바와 같이 공격자로부터 악의의 등록취소 메시지를 수신한 경우에 이를 무시하면 주기적으로 도착하는 유효 기간을 재설정하는 등록 메시지에 의해 유효 기간이 재설정되어 공격자의 공격은 실패로 돌아가게 된다. 등록

취소 공격에 대해 아무런 대응을 하지 않는 전략이 어떠한 오버헤드도 발생시키지 않는 완벽한 방어 기법이라는 것을 알 수 있다.

등록취소 메시지를 완전히 무시하게 되면, 공격자로부터 등록취소 공격을 쉽게 방어할 수 있는데, 이는 정상적 UA가 유효기간 재설정을 위한 등록 메시지를 주기적으로 전송하기 때문이다.

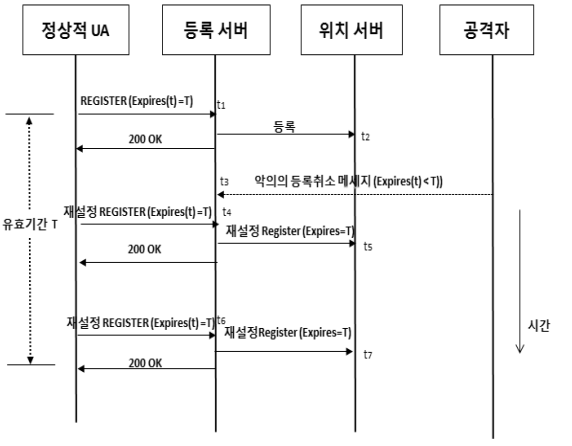

Fig. 3. Ignoring Malicious Deregistration Message.

4. 결 론

본 논문에서는 SIP에서의 UA 등록 과정을 분석해 보고 공격자에 의해 악용되어 질 수 있는 취약점을 찾아내고 그에 대한 대응 방안을 제시하였다. 취약점의 원인은 SIP인 RFC3261이 UA로 하여금 위치 서버에서 바인딩을 제거할 수 있도록 "should"로 허용하는 모순적 사실에 근거하고 있다. 만약 이를 "must not"으로 금지한다면 등록취소 공격은 현재처럼 용이하지 않을 것이다.

본 논문에서 제안한 대응 방안은 현재 SIP RFC를 존중하면서, UA와 등록 서버 사이에 TLS나 IPSec등과 같이 추가적인 메시지 교환이나. 암호화 그리고 인증 절차 없이, 등록취소 공격을 무시하는 것만으로도 완벽하게 공격을 방어할 수 있다는 것을 보여 준다. 따라서 기존의 다른 연구에서 제시된 대응 방안보다 효율적이며 매우 경제적이다. 또한 등록취소 공격보다 더 큰 피해를 줄 수 있는 등록 하이재킹 공격의 대부분이 등록취소 공격의 선행 조건으로 하고 있기에 본 연구의 결과는 등록 하이재킹 공격에 대한 좋은 대책이 될 수도 있다. 현재 VoIP는 전 세계적으로 널리 보급되고 있고, 시그널링 프로토콜 가운데에서도 SIP 는 VoIP의 지배적 프로토콜이 되어가고 있다. 따라서 본 연구의 결과는 SIP 등록 서버에 대한 취소 공격에 대한 매우 경제적 대응 방안이라 할 수 있겠다.

감사의 글

이 연구는 2015년도 단국대학교 대학연구비 지원으로 연구되었음.

참고문헌

1. Rsemberg, H.Schulzrinne, G Camarillo, A.Johnstion, J,Peterson, R.Sparks, M.handly, and E. Schooler, "SIP: Session Initation Protocol." RFC 3261, June 20, 1996.
2. Kyung-Hee Kwon, "Protecting Deregistration Attack in SIP Using Delayed Deregistration", Journal of the Korea Contents Association, Vol. 12, No.12, pp.18-23, 2015.
3. Mirko Raimondi,https://hakin9.org/voip-hacking-techniques.
4. http://www.voip-info.org/
5. Yun-Mi Go, Kyung-Hee Kwon, "Expanding the User Authentication Scheme in SIP", Journal of the Korea Contents Association, Vol.11, No.12, pp.88-98, 2011.
6. ETRI, "VoIP technology and market trends", ETRI 2006.
7. Ruhul Islam, Smarajit Ghosh "SIP Security Mechanism Techniques on Voice over Internet Protocol(VoIP) System", International Journal of Computer Application In Engineering Science, Vol. 1, issue. 1, pp.94-99, 2011.
8. Ha-na Yun, Hyung-Woo Lee, "Stateful SIP Protocol with Enhanced Security for Proactive Response on SIP Attack", Journal of the Korea Contents Association, Vol.10, No.1, pp.46-58, 2010.
9. El Sawda S., Urien P. "SIP Security Attacks and Solutions: A state-of-the-art Review", Information and Communication Technologies, ICTTA'06. 2nd, Vol 2, pp.3187-3191, 2006.
10. Yijun Zeng, Omar Cherkaoui "Performance Study of COPS over TLS and IPSec Secure Session" LNCS2506, pp.133-144, Springer-Verlag, Berlin, Heidelberg, 2002.
11. https://www.k2esec.com/network-security-protocols-ipsec-vs-tlsssl-vs-ssh-part-ii/

접수일: 2016년 12월 14일, 심사일: 2016년 12월 21일, 게재확정일: 2016년 12월 26일