http://dx.doi.org/10.5392/JKCA.2015.15.12.018

지연된 등록 취소를 이용한 SIP 등록 취소 공격 방어

Protecting Deregistration Attack in SIP Using Delayed Deregistration

권경희
단국대학교 컴퓨터과학과

Kyung-Hee Kwon(khkwon@dankook.ac.kr)

요약

SIP 등록 취소 공격은 공격자가 정상적 SIP UA의 REGISTER 메시지를 간단히 위장함으로써 야기되지만, 그 영향력은 매우 크다. 본 논문에서는 등록 서버가 등록 취소 REGISTER 메시지를 수신하는 즉시 위치 서버로부터 바인딩을 제거함으로써 등록을 취소하는 대신에, 일정 기간을 지연한 후에 취소하게 함으로서 등록 취소 공격을 식별하고 방어하게 해주는 새로운 방법을 제안한다. 따라서 본 논문에서 제안한 이 기법은 추가적인 암호화나 인증 과정들의 오버헤드 없이 SIP 등록 취소 공격에 대응하는 안전한 SIP 환경을 구축할 수 있게 한다.

■ 중심어 : | SIP | 등록 취소 공격 | 위장공격 | 지연된 등록 취소 |

Abstract

This paper proposes a new protection technique against deregistration attack in SIP. Although it is caused by simple spoofing the REGISTER message of a legitimate SIP UA, its impact is serious. This new protection technique identifies and protects the deregistration attack by removing a binding form the location server after delaying a certain period of time instead of removing the binding immediately after receiving deregistration message. Therefore, this technique makes it possible to establish a secure SIP environment defending the deregistraion attack without any additional overhead such as an encryption or authentication.

■ keyword : | SIP | Deregistration Attack | Impersonation Attack | Delayed Deregistration |

I. 서 론

SIP(Session Initiation Protocol)는 사용자 세션(User Session)의 관리에 필요한 시그널링 과정을 규정한 응용계층의 프로토콜로서, 인터넷 전화, 화상회의, 멀티미디어 배포 등과 같은 응용(Application)들이 많이 필요로 하고 있다. 특히 최근에 들어 IP망을 이용하여 음성 데이터를 전송하는 인터넷 전화 기술인 VoIP(Voice Over Internet Protocol)[1]서비스가 널리 보급됨에 따라 VoIP에 채택된 SIP 역시 전 세계적으로 널리 사용되어지고 있다[2]. SIP는 1996년에 처음 고안되어, 단순한 인증 기능만을 보안의 수단으로 제공했지만 현재의 SIP RFC(Request for Comments)인 3261[3]에서는 응용계층에서는 HTTP(Hypertext Transfer Protocol) 다이제스트 인증 방식과 S/MIME(Secure/Multipurpose Internet Extensions), 전송 계층에서는 TLS(Transport Layer Security), 그리고 네트워크 계층에서는 IPSec(Internet Protocol Security)사용을 권

* 본 연구는 2014년 단국대학교 대학 연구비 지원으로 연구되었습니다.
접수일자 : 2015년 10월 27일
수정일자 : 2015년 12월 07일
심사완료일 : 2015년 12월 07일
교신저자 : 권경희, e-mail : khkwon@dankook.ac.kr

고 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[4], 아직 널리 사용되지 못하고 있는 실정이다. 그리고 VoIP 서비스를 이용하는 응용들이 상대적으로 강력한 보안을 요구하지 않는 경우가 많아 비용과 효과의 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.

SIP는 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 등록 취소 공격이다. 이는 매우 쉽게 시도될 수 있는 공격이지만 이로 인한 통신 장애는 심각하며 위치 서버에 위장 등록을 하기만 하면 등록 하이재킹 공격으로 이어질 수도 있다. 특히 공격 대상이 미디어 게이트웨이처럼 다수의 이용자 그룹이 사용하는 곳이라면 그 피해는 더욱 심각하다.

이러한 등록 취소 공격을 방어하기 위한 몇몇 기법들이 소개되었지만, 암호화 메커니즘을 추가하거나 인증키를 빈번히 갱신하거나 인증의 단계를 추가하는 기존 기법들은[5-7] 인증과 암호화 알고리즘으로 인한 오버헤드를 발생시키고 시스템의 부하를 증가 시키는 단점이 있다. 이에 본 논문에서는 추가적인 인증 및 암호화를 일체 사용하지 않고도 등록 취소 공격을 간단히 방어할 수 있는 새로운 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 SIP 등록 취소 공격을 하기 위해 필요한 과정을 분석한다. 3장에서는 SIP 등록 취소 공격을 방어하는 메커니즘을 제안한다. 마지막으로 4장에서는 결론을 제시한다.

II. SIP 등록 취소 메커니즘

본 장에서는 논문의 기술에 필요한 SIP의 기본적 구성과 등록 절차에 대해 알아보고 이를 취소하는 과정을 분석해 본다.

1. SIP 구성과 등록

SIP는 크게 UA(User Agent)와 서버(Server)로 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 보낸다. 등록 서버는 수신한 REGISTER 메시지에서 UA의 위치 관련 정보를 위치 서버(Location Server)로 보내 데이터베이스에 저장하게 한다. 이 때, UA는 이 등록의 유효기간을 명기할 수도 있고, 등록서버가 서버의 정책에 의해 임의로 선택 할 수도 있다. 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 언젠가는 무효화된다.

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

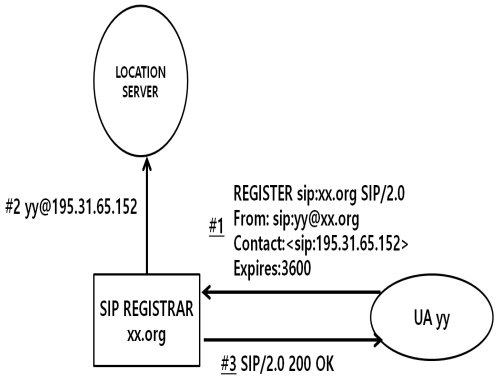

그림 1. UA 등록 과정

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

2. 등록 취소

SIP UA는 등록 서버를 통해 위치 서버에 사용자 URI인 자신의 AOR(Address of Record)과 자신이 로그인 될 실제 단말기 주소인 *'contact'* 주소를 매핑해 주는 레코드를 등록해야 한다. 이 매핑을 바인딩이라고 부르며 위치 서버에 REGISTER의 헤더 필드 들을 이용하여 [표 1]과 같이 바인딩을 저장해야한다.

위치 서버에 바인딩을 생성하는 과정은 매우 단순하다. 먼저 SIP UA가 등록 메시지를 등록 서버에게 전송하고, 이를 수신한 등록 서버는 위치 서버에 바인딩을 저장하고 200 OK 응답 메시지를 전송하면 완료된다. 바인딩은 유효기간이 지나면 소멸되기도 하지만 유효기간이 소멸되기 전 유효기간의 값을 *'0'*으로 설정한 REGISTER 메시지를 보내면 정상적인 SIP UA의 바인딩을 삭제하라는 의미이기 때문에 해당 UA의 등록이 취소된다. 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. 이렇게 RFC3261 작성 당시에 위치 서버의 성능을 높이기 위한 시도가 오늘날 SIP를 등록 취소 공격에 매우 취약한 프로토콜이 되게 한 것이다.

바인딩을 삭제하는 방법에는 두 가지가 있는데, REGISTER 메시지의 헤더 필드인 *'Expires'*에 *'0'*을 설정하는 것은 모든 바인딩을 삭제할 때 주로 사용되고, contact 헤더 파라미터 *'expire'*에 *'0'*을 설정하는 것은 하나의 URI에 한 개 이상의 *'contact'* 주소가연결된 바인딩을 삭제할 때 사용된다. 편의상, 본 논문에서는 이렇게 변조된 메시지를 DE-REGISTER 메시지라고 부르기로 한다.

표 1. 위치 서버에 저장된 바인딩의 필드

이름	내용
id	DE의 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 밧
call-id	등록 메시지의 'Call-ID' 헤더 필드의 값
cseq	등록 메시지의 'Cseq' 헤더 필드의 값

등록 취소 공격의 사나리오는 다음가 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 요구한다 하더라도 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) REGISTER 메시지의 'Contact' 헤더가 포함하는

'expire' 파라미터의 값을 '0'으로 설정한 DE-REGISTER 메시지를 보낸다. 'Expires'헤더 필드가 '0'이고 'Contact' 헤더가 "*"이면 그 UA에 해당되는 모든 바인딩을 데이터베이스에서 제거하게 되지만, 'Expires' 헤더 필드가 '0'이 아니라면 'Contact' 헤더에 "*"을 사용할 수 없다.

Ⅲ. 제안하는 메커니즘

등록 취소 공격은 DE-REGISTER 메시지에 의해 시도되는데, 실제로 위치 서버에서 바인딩을 제거하는 DE-REGISTER 메시지인지 등록 취소 공격을 위한 DE-REGISTER 메시지인지를 구분하기는 쉽지 않다. 그러나 메시지가 도착하고 난 후에, 일어나는 현상이 다르기 때문에 본 장에서는 그 차이점을 분석해 보고 그 대응 방안을 제시하고자 한다.

1. 등록 취소 공격 식별

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 기본 값(Default)으로 유효기간은 1시간으로, 그리고 유효기간 동안 2번 재설정하기를 권고하고 있다.

정상적으로 등록 서버와 연결이 해제되는 단말기는 경우에 따라 DE-REGISTER 메시지를 보낼 수도 있고 그렇지 않을 수도 있지만, 유효기간의 값이 '0'이 되어 위치 서버의 데이터베이스에서 바인딩이 제거된다. 즉, 소프트 폰이 로그오프 될 때는 DE-REGISTER메시지를 보내는 과정을 거칠 수 있다 그러나 갑작스러운 전원 차단과 같은 예기치 않은 일로 IP 폰과 같은 단말기의 연결이 해제되면 전원이 없어 DE-REGISTER 메시지를 보낼 수가 없는데 이럴 경우엔 유효기간이 경과할 때까지 기다릴 수밖에 없다.

이 두 가지 경우는 DE-REGISTER 메시지를 보내건 보내지 않던, 재설정을 위한 REGISTER 메시지가 도착되는 일이 없이 유효기간의 값이 '0'이 되어 위치 서버의 데이터베이스에서 바인딩이 제거된다.

그러나 공격자에 의해 변조되어 등록 취소 공격을 위한 DE-REGISTER 메시지는 뒤를 이어 재설정을 위한 REGISTER 메시지가 정상적 UA로부터 도착하게 되어 있다.

따라서 DE-REGISTER 메시지가 도착한 뒤 일정 시간을 기다려 보면 등록 취소 공격용 DE-REGISTER 메시지를 식별할 수 있다.

2. 지연된 등록 취소

등록 취소 공격을 위해 공격자는 위조된 DE-REGISTER 메시지를 등록 서버에 보내 위치 서버에 저장된 바인딩을 삭제하려 할 것이다. 그리고 정상적 사용자는 위치 서버에 저장된 바인딩을 유지하기 위해 첫 번째 REGISTER 메시지의 *'Expires'* 헤더 값에 설정된 유효기간이 끝나기 전에 REGISTER 요청을 다시 해서 *'Expires'* 헤더 값을 재설정(Refresh)하게 되어 있다. 따라서 [그림 2]의 네모 부분에서와 같이 *'Expires'* 헤더 값에 REGISTER 메시지가 전송되는 주기 시간 T를 설정해 주면, 위치 서버에 저장된 바인딩 값을 즉시 삭제하지 않고 재설정을 위한 REGISTER 메시지가 정송되는 주기 시간 T 만큼 지연시킨 후, 재설정을 위한 REGISTER 메시지가 도착되면 DE-REGISTER 메시지는 무시되어지고 등록 취소 공격은 방어되어진다. 그리고 정상적으로 등록 서버와 연결이 해제되는 단말기가 보낸 DE-REGISTER 메시지인 경우에는 T 만큼 지연 후에 위치 서버에서 바인딩이 삭제될 것이다. 즉, 등록 취소 공격이 아닌 정상적인 SIP UA에 전송된 등록 취소 메시지일 경우 바인딩 삭제가 주기시간 만큼 지연될 뿐 어떠한 문제점이 발생하지 않는다.

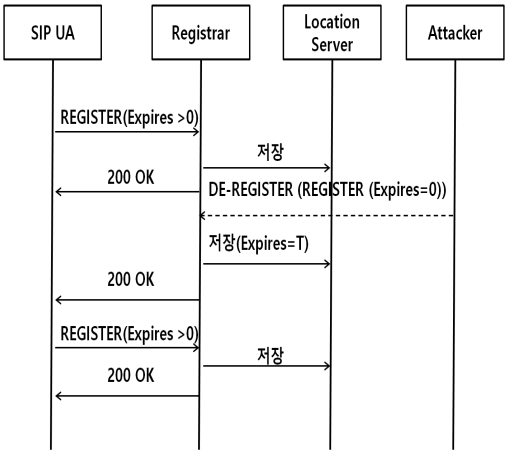

그림 2. 등록 취소 공격을 탐지하고 방어하는 과정

[그림 2]의 점선으로 표시된 부분에서 공격자는 바인딩 삭제를 시도하지만 네모로 표시된 부분에서 Expires에 0 대신 T를 할당함으로써 시간 T 만큼 기다리게 해준다. 그 시간 동안에 유효기간 재설정을 위한 REGISTER 메세지가 정상적 사용자로부터 반드시 도착하게 되어 있으므로 공격자의 공격은 실패로 돌아가게 된다. 이는 SIP UA가 위치 서버에 저장된 바인딩을 유지하기 위해 주기적으로 REGISTER 요청을 하여 위치 서버에 저장된 바인딩의 유효기간 *'expires'* 값을 재설정해 주기 때문이다.

Ⅳ. 결론

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 등록 취소 공격은 현재처럼 용이하지 않을 것이다. 본 논문에서 제안한 대응 방안은 현재의 SIP를 존중하면서, UA와 등록 서버 사이에 TLS나 IPSec등과 같이 추가적인 메시지 교환이나. 암호화 그리고 인증 절차 없이 구현 과정의 하나의 할당문에서 [그림 2]의 Expires에 해당되는 값을 '0' 대신 'T'로 할당함으로써 바인딩 제거를 지연시키고, 그리고 그것만 으로 등록 취소 공격을 방어하는 것이다. 따라서 기존의 다른 연구에서 제시된 대응 방안보다 간단하며, 추가 비용이 전혀 발생하지 않는 것이라 할 수 있다. 또한 등록 취소 공격보다 더 큰 피해를 줄 수 있는 등록 하이재킹 공격의 대부분이 등록 취소 공격의 선행을 필수로 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 SIP 등록 서버에 대한 취소 공격은 앞으로도 새로운 방법으로 계속 되어질 것이고 이에 대한 경제적 대응 방안에 대한 연구도 계속되어야 할 것이다.

참 고 문 헌

[1] ETRI, "VoIP technology and market trends," ETRI 2006.

[2] 고윤미, 권경희, "SIP에서의 강화된 사용자 인증 방식," 한국콘텐츠학회논문지, 제11권, 제12호, pp.88-98, 2011.

[3] Rpsemberg, H. Schulzrinne, G. Camarillo, A. Johnstion, J. Peterson, R. Sparks, M. Handly, and E. Schooler, "SIP: Session Initation Protocol," RFC 3261, 2002(6).

[4] 고윤미, 권경희, "IEEE 802.11에서의 복제된 AP 탐지 및 차단 기법," 한국콘텐츠학회논문지, 제10권, 제5호, pp.17-22, 2010.

[5] Ruhul Islam and 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.

[6] 최재덕, 정수환, "효율적이고 안전한 SIP 사용자 인증 및 키 교환," 정보보호학회, 제19권, 제3호,

pp.73-82, 2009.

[7] 윤하나, 이형우, “SIP 공격 대응을 위한 보안성이 강화된 Stateful SIP 프로토콜,” 한국콘텐츠학회 논문지, 제10권, 제1호, pp.46-58, 2010.

[8] 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.

[9] Yijun Zeng and Omar Cherkaoui, “Performance Study of COPS over TLS and IPSec Secure Session,” LNCS2506, Springer-Verlag, Berlin, Heidelberg, pp.133-144, 2002.

[10] https://www.k2esec.com/network-security-protocols-ipsec-vs-tlsssl-vs-ssh-part-ii/

저 자 소 개

권 경 희(Kyung-Hee Kwon) 정회원

- 1976년 : 고려대학교 물리학과 (이학사)
- 1986년 : Old Dominion Univ. Dept. of Computer Science(M.S.)
- 1992년 : Louisiana State Univ. Dept. of Computer Science(Ph.D)
- 1979년 ~ 1984년 : 산업연구원(KIET) 연구원
- 1993년 ~ 현재 : 단국대학교교수

<관심분야> : 컴퓨터 네트워크, 알고리즘분석 및 설계, 네트워크 보안