http://dx.doi.org/10.5392/JKCA.2011.11.12.088

SIP에서의 강화된 사용자 인증 방식

Expanding the User Authentication Scheme in SIP

고윤미, 권경희
단국대학교 전자계산학과 컴퓨터과학

Yun-Mi Go(alice8105@dankook.ac.kr), Kyung-Hee Kwon(khkwon@dankook.ac.kr)

요약

공격자는 SIP의 취약한 인증구조로 인해 정상적인 사용자로 위장하는 공격이 용이하다. 이러한 위장공격을 대응하기 위해 HTTP Digest 인증 기법 또는 제 3의 기관에서 발급된 개인키를 이용하고 있다. 그러나 기존의 제안된 방법들은 보안상 취약점을 가지고 있거나 추가적인 오버헤드로 인한 서비스 지연의 문제점이 있다. 본 연구에서는 사전에 공유한 패스워드와 SIP UA(User Agent)가 SIP 등록 서버(Registrar)에 등록 시에 주고받는 메시지들의 시간 정보를 이용하여 자동적으로 일회용 패스워드를 생성하고 이를 이용하여 위장공격에 대응하는 인증 방식을 제안한다. 이 방식은 SIP의 인증절차를 크게 수정하지 않고도 보다 안전한 SIP 환경을 구축할 수 있다.

■ 중심어 : | SIP | 위장공격 | 일회용 패스워드 |

Abstract

Due to vulnerable authentication scheme of SIP, intruders can easily impersonate legitimate user. HTTP Digest authentication scheme or private key issued by trust third parties has been used to prevent impersonation attack. However, these methods have suffered security vulnerability or service delay due to computation overhead. In this paper, we propose new authentication method to generate automatically one-time password using the pre-shared password and time information of messages exchanged between SIP UA(User Agent) and SIP Registrar. This method protects against impersonation attack without significant modification of exiting SIP authentication procedure to build securer SIP environment.

■ keyword : | SIP | Impersonation Attack | One-time Password |

I. 서 론

VoIP(Voice Over Internet Protocol)서비스는 IP망을 이용하여 음성 데이터를 전송하는 기술로서 인터넷망에 접속 가능한 장소 어디에서든지 음성 전화 서비스를 이용할 수 있다는 편리함을 가지고 있다. 더욱이 저렴한 통신비용으로 인해 사용자들에게 빠르게 확산되어 가고 있는 추세이다. 그러나 사용자들은 VoIP의 관리 또는 정책상의 오류, 취약한 인증구조, 비 암호화와 같은 취약점으로 인해 개인의 프라이버시가 위협받고 있음을 인식하지 못하고 있는 실정이다. 이러한 취약점으로 인해 VoIP는 크게 네 가지 보안 위협이 발생한다[1-4]. 첫 번째로는 해킹을 통한 불법도청이다. 해킹도구를 이용하여 통화내용을 도청하는 공격이다. 두 번째로는 서비스 거부 공격(DoS: Denial of Service)이다. VoIP의 단말기나 서버를 해킹하여 악의적인 패킷을 전

* 본 연구는 2010년 단국대학교 대학 연구비의 지원으로 연구되었습니다.
접수번호 : #110816-002
접수일자 : 2011년 08월 16일
심사완료일 : 2011년 12월 01일
교신저자 : 권경희, e-mail : khkwon@dankook.ac.kr

송함으로써 장애를 유발하여 정상적인 서비스를 받지 못하게 하는 것이다. 세 번째로는 스팸발송이다. 불특정 다수에게 음성광고나 메시지를 전송하여 사생활을 방해한다. 네 번째로는 서비스 오용 공격이다. 즉 정상적인 사용자의 등록정보를 이용하여 인증 받지 않은 사용자가 정상적인 사용자로 위장하여 서비스를 불법적으로 이용하는 것이다.

위와 같은 보안 위협을 방어하기 위한 연구들이 활발히 진행되고 있지만 공격자가 정상적인 사용자로 위장하는 공격에 대한 능동적 해결방안은 없는 실정이다. 이에 본 논문에서는 위장 공격을 방어하기 위해 일회용 패스워드를 사용한다. 일회용 패스워드는 SIP 등록서버 (Registrar)와 SIP UA(User Agent) 의 등록 과정에서 주고받는 메시지의 시간 정보를 이용하여 생성된 값과 사전에 공유한 패스워드를 이용하여 생성된다. 이때 사용 되는 시간 입력 값은 기존의 사용되는 등록 메시지들을 이용하여 생성되기 때문에 추가되는 오버헤드가 최소화되었다. 또한 일회용 패스워드는 SIP 등록서버에 SIP UA가 등록할 때 마다 자동으로 생성되므로 사용자의 편의성이 높아진다. 더욱이 제안한 인증 방식은 해쉬 함수를 이용하여 일회용 패스워드를 생성하기 때문에 암호학적 연산량을 최소화하여 서비스의 지연 문제를 해결하였다.

본 논문의 구성은 다음과 같다. 2장에서는 SIP 보안 기법들을 분류하고 각 기법들에 대한 취약점을 분석한다. 3장에서는 효율적인 SIP 인증 메커니즘을 제안한다. 4장에서는 제안한 메커니즘의 안전성 분석하였다. 마지막으로 5장에서는 결론 및 향후 과제에 대해서 살펴본다.

II. 관련연구

IETF SIP[5][6] 표준에서는 사용자 인증과 SIP 메시지를 보호하기 위하여 HTTP Digest 인증기법, TLS (Transport Layer Security), IPsec, S/MIME(Secure /Multipurpose Internet Mail Extension)보안 프로토콜을 사용한다. HTTP Digest 인증 기법은 메시지에 대한 인증과 재사용(replay)공격을 방지하지만 메시지에 대한 무결성이 보장되지 않는다. 더욱이 기존의 HTTP Digest는 Challenge-Response 방식을 사용하고 있기 때문에 사전에 공유된 패스워드를 제외한 나머지 값들이 공격자에게 쉽게 노출되어 패스워드 유추가 가능하다. 이에 홉 간의 보안 기술인 TLS을 동시에 사용하여 안전한 인증 서비스를 제공한다. TLS는 SIP 메시지에 대한 암·복호화를 통해 홉 간의 보안채널을 형성하기 때문에 메시지의 무결성과 기밀성이 제공된다.

S/MIME프로토콜은 SIP 사용자간의 보안 기능을 제공하여 사용자 인증, 메시지의 무결성, 기밀성을 제공한다.

그러나 표준에서 정의한 TLS, S/MIME 보안 프로토콜들은 PKI(Public Key Infrastructure) 기반의 보안 프로토콜이기 때문에 PKI 환경이 구축되지 않은 환경에서는 적용할 수 없다. 더욱이 많은 메시지 교환과 암호학적 연산량을 요구하는 TLS 보안 프로토콜은 성능 문제로 실제 네트워크에 적용하기 어렵다[7]. 이러한 SIP 보안 프로토콜의 문제점을 해결하기 위하여 다양한 연구가 진행되고 있다.

먼저, PKI를 요구하지 않는 홉 간의 보안기술을 살펴본다. 기존 HTTP Digest 인증 기술에 DH(Differ-Hellman) 키 교환 암호 알고리즘을 사용하여 SIP 단말과 서버 사이에서 안전한 사용자 인증 및 키 교환 기술이 제안되었다[8]. 기존 HTTP Digest 인증 기법의 취약점인 사전 공격에 대해서 DH 기반의 SIP 보안 기술이 문제점을 해결해주었다. 하지만 DH 알고리즘은 지수 모듈러 연산을 사용하기 때문에 암호학적 연산량을 요구하는 단점이 있다.

SIP의 취약점인 패킷에 대한 변/복조와 기존의 공격에 대응하기 위해 SIP Firewall을 제시하고 있다[9]. SIP Firewall은 사용자 인증을 위한 키 관리, 세션키 생성, 암/복호문의 길이를 결정하기 위한 협상, 각 호 상태 정보 관리 기능을 추가하여 SIP의 취약점을 해결하고 있다.

다음으로는 SIP 취약점의 문제해결로 Kerberos[10][11]을 사용한다. 즉 제 3자 인증 서비스로서 인증을 수행하는 것으로 사용자들의 인증에 의존하지 않고 네트워크 상의 모든 사용자들이 패킷을 언제든지 읽고 수정하고 삽입할 수 있다는 가정 하에 ID를 검증할 수 있는 수단

을 제공하고 있다.

마지막으로는 IBC(ID-based Cryptosystem) 방법을 이용한 SIP 보안기술이 있다[12][13]. IBC는 사용자의 이메일주소 또는 IP 주소와 같은 식별자 기반의 메커니즘으로 KGC라는 제 3의 가관을 통해 자신의 비밀 마스터키와 사용자 ID를 이용하여 개인키를 사용한다. 이때 사용자 ID는 메시지를 암호화하거나 서명된 메시지를 인증하는 공개키로 사용하기 때문에 인증서 교환과 유효성 검사 절차가 이루어질 필요가 없다. 따라서 네트워크 기반구조가 없는 Ad-hoc 환경에서 많이 사용된다.

이와 같이 다양한 방면으로 SIP 보안 기술이 연구되어왔다. 그러나 SIP 단말과 서버 사이에서 사용자 인증과 키 교환 기능을 제공하는 기존 기술들은 암호학적 연산량 때문에 시스템 과부하 및 서비스 지연 그리고 SIP 이동 단말의 배터리 소모와 같은 자원 활용 측면에서 비효율적이다. 이러한 문제점을 해결하기 위해 본 논문에서는 기존의 HTTP Digest 인증 기법을 보완하여 해쉬 함수로 생성된 일회용 패스워드를 이용하는 새로운 인증 방법을 제안한다.

Ⅲ. 제안하는 메커니즘

본 논문에서는 공격자가 사전에 공유된 패스워드를 유추하여 정당한 SIP UA또는 프록시 서버로 위장하여 인증을 시도하는 공격을 차단하기 위하여 기존 HTTP Digest 인증 기법에 취약점을 보완한 새로운 인증 기법을 제시하고자 한다. 보완한 인증 기법은 두 단계를 거쳐 이루어진다. 첫 번째로 일회용 패스워드를 생성하기 위한 입력 값을 생성하는 단계이다. 두 번째 단계는 생성된 입력 값과 사전에 공유한 패스워드를 이용하여 일회용 패스워드를 생성하고 이를 이용하여 사용자를 인증한다.

1. 시간 입력 값 생성과정

그림1은 SIP 단말과 Registrar 간의 일회용 패스워드 생성을 위해 사용되는 시간 입력 값을 생성하는 과정이다. SIP UA가 서버 등록 과정에서 사용되는 메시지 교환 절차는 표준 SIP에서 제안하는 절차와 동일하다. 이때 A(Sender)에서 B(Receiver)로 보내는 메시지를 표시하기 위해 A->B 와 같은 기호를 사용한다.

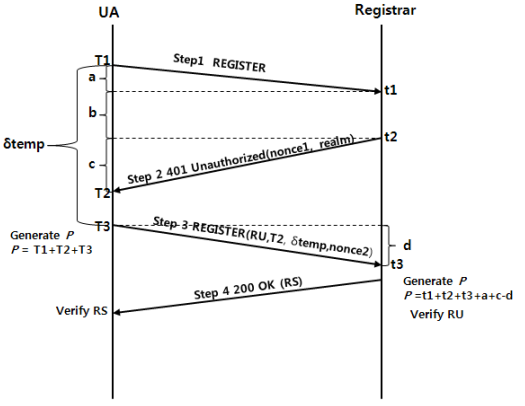

그림 1. SIP 일회용 패스워드 생성 절차

step1. SIP UA -> Registrar

SIP UA는 REGISTER 요청 메시지를 서버에게 전송한다.

step2. Registrar -> SIP UA

SIP 서버는 요청 메시지를 수신 후 401 unauthorized 메시지 헤더에 nonce1, realm을 포함하여 SIP UA에게 전송한다. 이때 nonce1은 Registrar가 생성한 문자 난수열이며 realm은 SIP 서버의 도메인 정보이다.

step3. SIP UA-> Registrar

SIP UA는 401 unauthorized 메시지를 수신한 T2 시간을 저장하고 P값은 식(1), RU(Response UA)값은 식(2)과 같이 생성한다. RU는 T2 타임스탬프, $\delta temp$, nonce2를 포함하여 SIP 서버에게 전송한다. 이때 사용되는 pw는 사전에 공유한 패스워드, $\delta temp$는 T1과 T3의 시간 간격을 의미한다. h( )는 일 방향 해쉬 함수이며 nonce2는 SIP UA에서 생성한 문자 난수열이다. P는 일회용 패스워드를 생성하기 위한 시간 입력 값이다.

P = T1+T2+T3 식(1)

RU = h(P, nonce1, pw, realm) 식(2)

step4. Registrar -> SIP UA

SIP 서버는 SIP UA 전송받은 RU의 T2 값과$\delta temp$을 이용하여 식(3),(4)을 통해 P를 생성한다. 이때 생성된 P와 nonce1을 RU에 포함된 h(P, nonce1, pw, realm)로 검증한다. 이를 통해 SIP UA와 서버는 동일한 P가 생성됨을 확인한다. 그 후 식(5)을 이용하여 RS(Response Server)를 생성하고 200 OK 메시지 헤더에 포함하여 SIP UA에게 전송한다. SIP UA는 200 OK 메시지를 전송받은 후 서버와 동일한 P를 생성하였는지를 h(P, nonce2, pw)를 통해 확인한다. 이때 사용되는 a는 T1과 t1의 시간 간격을 의미하고 b는 t1과 t2의 시간 간격을 의미한다. c는 t2와 T2의 시간 간격을 의미하고 d는 T3과 t3의 시간 간격을 의미한다.

$$a+c-d = \delta temp-(t3-T2)-b \quad \text{식(3)}$$

$$P = t1+t2+t3+a+c-d \quad \text{식(4)}$$

$$RS = h(P, nonce2, pw) \quad \text{식(5)}$$

SIP UA가 Registrar에 등록과정이 끝나면 SIP UA와 Registrar는 동일한 P를 저장한다.

2. 일회용 패스워드를 이용한 사용자 인증단계

[그림 2]는 콜 설정 시에 사용자 인증 과정을 보여준다. 이때 저장된 P는 프록시 서버로 안전한 채널에 의해 전송된다고 가정한다. 사용자 인증 과정은 기존의 SIP에 사용되는 메시지 교환 방식과 동일하지만 패스워드 값과 저장된 P값을 이용하여 생성된 일회용 패스워드를 사용한다.

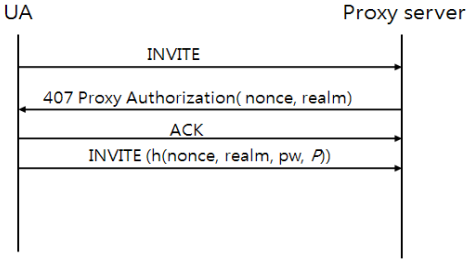

그림 2. SIP 콜 설정 단계에서 인증 과정

먼저 SIP UA는 콜 설정을 위해 INVITE 요청 메시지를 프록시 서버에게 전송한다. INVITE 요청 메시지를 받은 프록시 서버는 Proxy Authentication Required 응답 메시지를 SIP UA에게 전송한다. 이때 nonce와 realm이 헤더 필드에 포함되어 전송된다. SIP UA는 nonce, realm, username, 패스워드 그리고 저장된 P를 이용하여 해시한 값을 INVITE 요청 메시지의 "Proxy-Authorization"헤더 필드에 포함하여 재전송한다. 이때 프록시 서버는 값을 검증하여 SIP UA를 인증한다.

SIP UA와 SIP 등록 서버는 SIP UA가 유효 시간이 지나 재등록 할 때 마다 새로운 P 생성하고 이를 이용하여 일회용 패스워드를 생성한다. 이 과정에서 새로운 P를 사용하기 때문에 패스워드 재사용 공격이 불가능하게 된다. 더욱이 패스워드와 P 을 공격자 유추하기 이전에 유효시간이 지나 P 값이 변경되므로 공격자에게 일회용 패스워드가 노출되는 것은 어렵다.

Ⅳ. 안전성 분석

이 장에서는 제안 기법의 안전성과 성능을 분석 한다. 공격자는 정당한 SIP UA 또는 서버로 위장하여 인증을 시도하는 위장공격을 수행할 수 있다. 본고에서 제안한 기법에서는, SIP UA와 서버 사이의 등록 과정에서 생성된 P를 이용하여 정당한 사용자와 서버를 구별할 수 있기 때문에 안전성이 보장된다. 공격자에게 전송되는 T2 타임스탬프, $\delta temp$값이 노출되어도 SIP UA의 T1, T2값과 등록서버의 t3, b값을 유추할 수 없기 때문에 P를 생성할 수 없게 된다. 이에 기존이 HTTP Digest 인증 기법의 취약점인 공유된 패스워드 유출시 에 P를 공격자가 생성할 수 없기 때문에 사용자 인증이 가능하지 않다. 또한 재생 공격이 이루어져도 P을 이용하여 일회용 패스워드를 생성하기 때문에 쉽게 차단될 수 있다. 더욱이 등록 서버의 유효시간이 지나면 재등록 할 때마나 새로운 P를 생성하기 때문에 공격자에게 P가 노출되는 것이 어렵다.

표 1. SIP UA에서 암호학적 총 연산량 비교

메커니즘	시간비용
제안한 메커니즘	Negligible (hash function)
Yang et al.[7]	$\sum_{i=1}^{n} 2\,T_E$
Ring et al.[10]	$\sum_{i=1}^{n} 2(T_P + T_M)$
Wang et al.[11]	$\sum_{i=1}^{n} (6\,T_P + 5\,T_M)$

T_E : modular exponentiations

T_M : EC point multiplication

T_P : tate pairing

[표 1]에서는 제안하는 기법과 기존에 연구된 다른 기법들의 암호학적 연산량을 비교하였다[7]. TE, TM, TP는 각 암호 알고리즘에서 수행되는 지수모듈러, 포인터 곱셈, 페어링 연산의 단위시간을 의미한다. SIP UA에서 매번 SIP 등록 서버 에 등록 단계와 콜 설정 단계에서 인증 및 키 교환 과정을 수행한다고 가정할 경우 n번 수행할 때 요구되는 암호학적 총 연산량이다. 제안한 기법은 기존 등록 과정에서 사용되는 메시지를 이용하여 일회용 패스워드를 자동으로 생성한다. 이때 해쉬 함수를 이용하기 때문에 기존 방식에 비해 암호학적 연산량이 적다. 따라서 기존에 SIP 보안 기술들의 많은 암호학적 연산량에 의해 서비스 지연의 단점을 해결할 수 있게 된다. 또한 제안된 기법은 제 3의 기관을 통해 키를 발급받지 않아도 등록 메시지의 시간정보를 이용하여 일회용 패스워드를 자동으로 생성하기 때문에 사용자가 계속 패스워드를 변경하지 않아도 되는 장점이 있다.

V. 결론

VoIP는 편리함과 저렴한 통신비용의 장점으로 사용자들에게 빠르게 보급되고 있다. VoIP에서 사용되는 SIP 프로토콜의 확정성의 장점을 갖은 반면 손쉽게 패킷을 수정, 삭제가 가능한 취약점을 가지고 있다. SIP의 취약점을 이용하여 다양한 공격이 이루어지고 있는 실정이다. 이에 공격을 탐지하고 방어하는 보안 메커니즘이 필요하다. 본 논문에서는 제 3의 기관을 통해 개인키를 발급받는 형태가 아닌 SIP 등록 서버에 SIP UA가 등록하는 과정에서 주고받는 메시지의 시간 정보를 이용하여 생성된 입력 값과 사전에 공유된 패스워드를 이용하여 일회용 패스워드 생성한다. 일회용 패스워드는 공유된 패스워드가 유출되어도 재생 공격 불가능하기 때문에 기존 HTTP Digest 인증 기법의 취약점을 보완하였다. 더욱이 제안한 방안은 자동으로 일회용 패스워드를 생성할 수 있는 장점이 있고 일회용 패스워드 생성을 위한 추가적인 오버헤드가 적기 때문에 서비스의 지연 문제를 해결할 수 있다.

참 고 문 헌

[1] Keromytis and D. Angelos, "A Comprehensive Survey of Voice over IP Security Research," Communication Surveys & Tutorials, IEEE, Issue:99, pp,1-24, 2011(4).

[2] A. D. Keromytis, "Voice over IP: Risk, Threats and Vulnerabilities," in Proc. Cyber Infrastructure Protection (CIP) Conference, 2009(6).

[3] A. D. Keromytis, "A Look at VoIP vulnerabilities," USENIX ; login: Magazine Vol.35, pp.41-50, 2010(2).

[4] A. D. keromytis," Voice over IP Security: Research and Practice," IEEE Security Privacy Mag, Vol.8, pp.76-78, 2010(3)(4).

[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, 2002(6).

[6] 권경희, 김진희, 고윤미 "셀룰러 망에서 SIP 재전송 간격조절에 의한 성능 개선과 이를 이용한 홈 네트워크 구현", 한국콘텐츠학회논문지, 제8권,

제2호, 2008(2).

[7] 최재덕, 정수환 “효율적이고 안전한 SIP 사용자 인증 및 키 교환”, 한국정보보호학회논문지, 제19권, 제3호, 2009(6).

[8] C. Yang, R. Wang, and W. Liu, "Secure authentication scheme for session initiation protocol," Computers & Security, Vol.24, No.5, pp.381-386, 2005(8).

[9] 윤하나, 이형우 “SIP 공격대응을 위한 보안성이 강화된 Stateful SIP 프로토콜”, 한국콘텐츠학회논문지, 제10권, 제1호, 2010(1).

[10] J. Y. Migeon, *"The MIT Kerberos Administrator's How-to Guide,"* Kerberos consortium, 2008.

[11] C. Neuman, J. Kohl, and T. Ts'o, "The Kerberos Network Authentication Service(V5)," Internet draft(work in progress), draft-ietf-cat-kerberos-revisions-06.txt, 2000.

[12] J. Ring, K. Choo, E. Foo, and M. Looi, "A new authentication mechanism and key agreement protocol for SIP using Identity-based cryptography," Proceeding of AusCERT Asia pacific Information Technology Security Conference, pp.57-72, 2006(5).

[13] F. Wang and Y. Zhang, "A net probably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography," Computer Communications, Vol.31, No.10, pp.2142-2149, 2008(6).

저 자 소 개

고 윤 미(Yun-Mi Go) 정회원

- 2004년 : 단국대학교 전자계산학과(이학사)
- 2007년 : 단국대학교 전자계산학과 컴퓨터과학(이학석사)
- 2008년 ~ 현재 : 단국대학교 전자계산학과 컴퓨터과학(박사과정)

<관심분야> : 컴퓨터 네트워크, 네트워크 보안

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 : 단국대학교 교수

<관심분야> : 컴퓨터 네트워크, 알고리즘 분석 및 설계, 네트워크 보안