클라우드 SNS상에서 Proxy Re-Encryption을 이용한 사용자 모바일 인증 프로토콜

조승현*, 문종호, 남윤호, 전웅렬, 원동호1)
*성균관대학교 정보보호연구소
{shc,jhmoon,yhnam,wrjeon}@security.re.kr

The User Authentication Protocol of Using the Proxy Re-Encryption for Mobile Cloud SNS

Seunghyun Cho*, Jongho Mun, Yoonho Nam, Woongryul Jeon, Dongho Won+
*Information Security Group, Sungkyunkwan University

요 약

최근 분산 시스템의 기술이 발전하면서 소셜 네트워크 서비스(SNS)도 분산방식으로 전환해가는 추세이다. 특히, 모바일 기기 발전과 공급 확산으로 인해 모바일 기기의 분산 SNS에 대한 연구로 클라우드 컴퓨팅 기술을 응용한 모바일 클라우드 SNS가 연구되고 있다. 또한, 제 3자의 미인증 모바일 기기를 사용한 SNS 접속으로 인한 피해가 증가되고 있는 반면, 이를 방지하는 사용자 모바일 기기 인증에 대한 연구는 미흡하다. 따라서 본 논문은 Proxy Re-Encryption 기술을 응용하여 안전한 모바일 기기 인증 프로토콜을 제안한다.

*Key word : 모바일 분산 시스템, 클라우드, Proxy Re-Encryption, SNS, 소셜 네트워크 서비스

1. 서론

소셜 네트워크 서비스(Social Network Service : SNS)는 사용자간의 의사소통 및 정보공유를 위한 수단으로 개발되었고, 단순한 의사소통 및 정보공유의 매개체뿐만 아니라 상업, 정치, 언론, 교육 등 다양한 분야에서 활용되고 있다. 이러한 SNS는 중앙집권방식에서 분산 시스템과 SNS을 융합한 분산형 SNS 방식으로 전환되는 연구가 진행 중이다. 또한, 스마트폰과 같은 모바일 기기의 확산으로 인해 모바일 분산 SNS에 대한 연구도 진행되고 있다. 특히, 모바일 기기의 연산 처리 한계 및 메모리 한계를 극복하기위해 클라우드를 이용한 분산형 SNS 모델에 대한 연구가 진행되고 있지만 클라우드 보안에 대한 신기술이나 사용자 모바일 기기 인증에 대한 연구는 미흡하다.[1][3]

본 논문은 모바일 기기의 클라우드 SNS 사용자 인증을 위해 Proxy Re-encryption 기술을 적용한 인증 프로토콜을 제안한다. 본 논문의 구성은 서론에 이어 2장에서는 클라우드 컴퓨팅 기술에 대해서 소개하고, 3장에서는 Proxy Re-encryption 기술을 소개하며 4장에서는 모바일 기기와 클라우드 SNS 사이의 Proxy Re-encryption 기술을 적용한 사용자 모바일 인증 모델 및 프로토콜을 제안한다. 마지막 5장에서는 결론을 다룬다.

1) 교신저자, dhwon@security.re.kr

2. 클라우드 컴퓨팅

클라우드 컴퓨팅은 1965년 John McCarthy가 처음으로 제안한 개념으로 유저가 사용하는 모든 정보가 인터넷 상의 서버에 저장되고, 보유하고 있는 IT 기기의 하드웨어 구애를 받지 않고 언제 어디서든지 이용할 수 있는 기술을 의미한다.

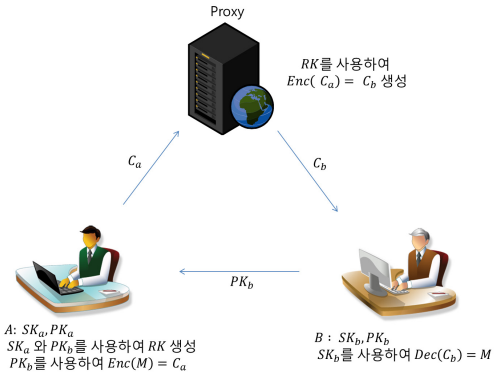
(그림 1) 클라우드 서비스

(그림 1)은 클라우드 서비스의 개념을 도식화 한 것으로 웹 2.0, SaaS(Software as a Service)와 같이 최근 잘 알려진 기술을 사용하고 있다. 구입비용이 적으며 휴대성 및 컴퓨터 가용성이 높고, 다양한 기기를 단말기로 사용하는 것이 가능하며 서비스를 통한 일치된 사용자 환경을 구현

할 수 있기 때문에 최근 각광받고 있는 기술이다. 하지만 클라우드 서버의 데이터 손상 시 복구가 어렵다는 점과 통신환경이 열악하면 서비스의 한계가 존재하며 특히, 클라우드 서버가 공격당하면 서버에 저장된 모든 정보가 유출될 수 있는 등 다양한 보안 위협이 존재한다. 이러한 보안 위협에 대응하기 위해 클라우드 보안 기술에 대한 많은 연구가 진행 중지만 현재까지는 기존의 보안 기술을 적용하는 수준이다.[3][4][5]

3. Proxy Re-Encryption

Proxy Re-Encrtption은 암호문의 복호권한을 위임하는 기술로서 1997년 Mambo, Okamoto가 처음으로 제안하였지만 송신자가 부재 중 일 경우, 암호문을 변환할 수 없다는 문제가 있다. 이와 같은 문제를 해결하여 1998년에 Blaze, Bleumer, Strauss은 ElGamal 암호방식을 사용한 BBS 기술을 제안하였다. BBS방식은 Proxy가 Re-Encryption key를 이용하여 A의 암호문을 B의 암호문으로 변환하는 방식이지만 Proxy와 B의 공모공격에 취약한 점과 A의 비밀키를 계산할 수 있다는 취약점이 발생하였고, 2003년 Dodis, Ivan에 의해 BBS방식의 문제점을 개선한 DI방식을 제안했다. DI방식은 A의 비밀키 일부를 B에게 분배하는 방식으로 B가 메시지를 복호할 때 A의 비밀키 일부를 사용하는 방식이지만 키 분배 문제와 Proxy와 B의 공모공격에 취약하다는 문제점이 발생하였다. 2005년 Ateniese 등이 DI방식을 개선한 AFGH방식을 제안했다.



(그림 2) AFGH 방식

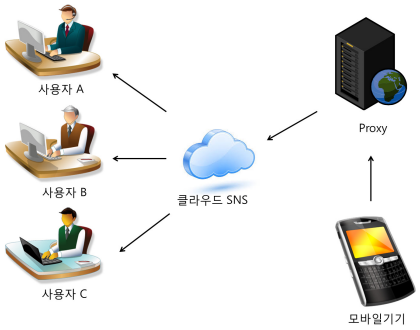
(그림 2)는 AFGH 방식을 나타낸 그림으로 만약, A가 B에게 메시지를 전송하려면 A는 메시지(M)를 자신의 공개키로 암호화(C_a)하여 Proxy에 전송을 하게 되며 Proxy는 암호화 된 메시지(C_a)를 Re-Encryption Key(RK)로 재암호화(C_b)하여 B에게 전송을 하게 된다. 재암호화를 위한 RK는 Proxy 또는 A가 A의 비밀키와 B의 공개키를 이용하여 생성하게 된다. C_b를 전송받은 B는 자신의 비밀키를 이용하여 메시지(M)를 복호하게 된다.[2][6]

AFGH 방식은 A 관점에서는 A의 비밀키와 B의 공개키를 이용하여 RK를 생성하고 B 관점에서는 B의 비밀키와 A의 공개키를 이용하여 RK를 생성하기 때문에 사전에 서로의 비밀키를 공유하지 않으며 Proxy가 $g^{b/a}$ 값을 이용하여 $g^{a/b}$ 값을 계산할 수 없기 때문에 단방향이라 할 수 있다. 또한, 공모공격을 위해 Proxy가 A와 결탁한다고 하여도 RK 값으로부터 B의 비밀키를 얻기가 어렵기 때문에 공모공격에도 안전하다는 이점이 있다.

4. 제안 모델 및 프로토콜

클라우드 SNS를 사용하기위해 모바일 기기를 메인 서버로 사용하게 되면 모바일 기기는 콘텐츠 데이터를 비롯하여 개인 및 친구 정보 등 민감한 정보를 저장해야한다. 하지만 연산 과부하를 비롯하여 모바일 기기 분실 시, 모바일 기기 메모리에 저장된 정보가 외부로 노출 될 수 있는 위협이 존재하게 된다.[3] 따라서 본 모델은 클라우드에 콘텐츠 데이터를 저장하는 방법을 사용했고 저장된 데이터는 외부 공격으로부터 안전하다고 가정했다.

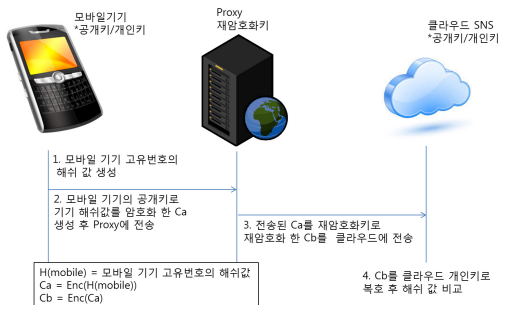
본 논문에서 제안하려는 모델은 AFGH 방식의 Proxy Re-encryption 기술을 분산방식의 클라우드 SNS에 적용시킨 것으로 아래 (그림 3)과 같다.



(그림 3) 구상 모델

(그림 3)은 모바일 기기의 연산 부담, 키 관리 및 메모리 감소를 위하여 클라우드를 기본 연산도구 및 콘텐츠 데이터 저장 장치로 이용하였고, 모바일 기기와 클라우드 사이에는 Proxy 서버를 사용했다.

사용자가 클라우드 SNS에 처음 접속하면 모바일 기기 고유번호의 해쉬 값을 생성하여 클라우드에게 전송함과 동시에 모바일 기기와 클라우드는 각각 공개키와 개인키를 생성 보관하게 된다. 또한, 모바일 기기는 클라우드의 공개키를 이용하여 재암호화키(RK)를 생성하고 Proxy에 보관을 하게 된다.



(그림 4) 프로토콜

(그림 4)는 모바일과 클라우드 사이의 프로토콜을 나타낸 것으로 모바일 기기를 이용하여 클라우드 SNS에 접속 시 모바일 기기의 해쉬값을 모바일 기기의 공개키로 암호한 암호문 C_a을 생성하여 Proxy에 전송을 하게 된다. 전송 완료된 C_a을 Proxy가 재암호화키(RK)로 다시 암호하여 C_b를 생성하고 클라우드에게 전송을 하게 된다. C_b를 전송받은 클라우드는 클라우드의 개인키를 사용하여 C_b를 복호하게 되고 클라우드가 가지고 있는 해쉬값과 비교하게 된다.

만약, 악의적인 목적을 가진 누군가가 사용자의 ID와 비밀번호를 획득하여도 해쉬값이 다른 미등록 모바일기기로 접속을 시도하기 때문에 클라우드 SNS 서비스를 이용할 수 없게 된다. 또한, C_a을 획득하여 모바일 기기 고유번호 정보를 획득하려고 시도해도 해쉬함수의 특성 및 AFGH 방식의 특성상 알 수가 없게 된다. 또한, 모바일 기기 분실 시 사용자는 분실 신고를 통해 클라우드 서버에 저장된 모바일 기기 고유번호 해쉬값을 파기할 수 있게 하여 분실로 인한 2차 피해를 줄일 수 있게 한다.

5. 결 론

SNS의 활용 방법이 다양해지면서 기존의 중앙집권방식의 SNS가 분산방식 클라우드 SNS로 변화해가려는 연구가 활발히 진행되고 있다. 또한, 모바일 기기의 확산으로 모바일 기기를 사용하여 SNS에 접속하는 사람도 증가하고 있는 추세이다. 하지만 모바일 기기와 클라우드 간의 인증 모델, 프로토콜 연구가 미흡하다.

따라서 본 논문은 클라우드 SNS에 대비하여 모바일 기기와 클라우드 간의 안전한 모바일 기기 인증을 위해 AFGH방식의 Proxy Re-Encryption 기술을 적용한 모델을 제안했고, 그로 인한 사용자 인증효과를 기술하였다. 향 후 연구에서는 본 모델과 프로토콜에 대한 추가적인 취약점을 분석하고 암호 연산에 필요한 시간을 비교한다.

참고문헌

[1] 신종희 “클라우드 보안 인증 스킴과 해결과제”, 2012년 10월 한국정보보호학회

[2] 송유진 외 1명 “Proxy Re-encryption 기술”, 2009년 한국정보보호학회

[3] 이정훈 외 2명 “모바일 클라우드기반 UCC IPTV 서비스 및 SNS 제공에 관한 연구”, 2010년 한국인터넷정보학회

[4] Celesti 외 1명 "Security and Cloud Computing : Intercloud Identity Management Infrastructure", 2010 19th IEEE International Workshop

[5] Micheal Armbrust 외 10명 "A View of Cloud Computing", April 2010 Communications of the ACM

[6]Kevin Fu 외 1명 “Proxy Re-encryption", 2005 CSAIL Research Abstracts

Acknowledge

"본 연구는 방송통신위원회의 방송통신융합미디어원천기술개발사업의 연구결과로 수행되었음"
(KCA-2012-12-912-06-003)