공개키를 이용한 VoIP 환경에서의 보이스피싱 탐지

신승용, 이명락, 이동현, 인호
*고려대학교 정보통신대학 컴퓨터학과
e-mail : {seneru,lmr2010,tellmehenry,hoh_in}@korea.ac.kr

Detecting Voice Phishing using Public Key Cryptography in VoIP

Sungyong Shin, Myongrak Lee, Donghyun Lee, Hoh Peter In
Department of Computer Science & Engineering, Korea University

요 약

'보이스피싱(Voice Phishing)'은 전화를 통해 자신을 신뢰할 수 있는 대상으로 위장하여 개인 정보를 훔치는 행위이다. 최근 들어 보이스피싱 피해 사례가 급증하고 있으며 아직 딱히 대안이 없는 상태이다. 또한, IP 환경에서의 전화통화는 보이스피싱을 더욱 용이하게 하고 있다. 본 논문에서는 VoIP 환경에서 공개키 암호화 기법을 이용하여 발신자의 신원을 정확히 밝히는 인증을 통해 사용자가 악성 발신자에게 정보를 제공하거나 금전적 피해를 피할 수 있는 방법론을 제시한다. 이를 통해 사용자는 발신자의 정확한 신원 정보를 제공 받아 보이스피싱 당할 가능성을 줄일 수 있다.

1. 서론

피싱(Phishing)은 악성 사용자가 자신을 신뢰할 수 있는 대상으로 위장하여 금융정보(비밀번호, 신용카드 정보)와 같은 기밀 정보를 훔치려는 사회공학이다[1]. 이 악성행위는 원래 메신저, 이메일, 또는 위장 사이트를 통해서 이루어져 왔었다. 그러나 최근 들어 전화를 이용한 보이스피싱 피해 사례가 급증하고 있다. 최근 3 년간 1 만 8 천 건이 발생하였고 피해 금액만 1 천 888 억원에 달하는 것으로 조사되고 있다 [3]. 이러한 보이스피싱은 공인 기관이나 금융 기관을 사칭하는 경우가 많으며, 우체국을 사칭한 보이스피싱 피해액만 362 억원에 달한다.

현재 기술적인 보이스피싱 방지 방안으로는 휴대폰에 국제 전화 문구를 표시해주는 방법과 ATM 근처 전파 방해 장치를 설치해 ATM 근처에서 휴대폰을 사용하지 못하게 하는 방법이 있다. 국제 전화 표시 서비스의 경우 발신자가 VoIP 를 사용시 IP Spoofing 을 통해 쉽게 우회될 수 있으며 휴대폰을 대상으로 하는 보이스피싱이 아닌 경우에는 방지가 힘들며 전파 방해 방법은 근본적인 해결책이 되지 못한다.

본 논문에서는 최근에 급증세를 보이고 있는 VoIP 기반에서의 보이스피싱 방지법을 제공한다. 보이스피싱이 대부분 국가 공인 기관이나 금융 기관을 사칭한다는 것을 기반으로 하여 공개키 기법을 이용하여 발신자를 인증하여 보이스피싱을 방지하고자 하는 방법이다. 이로 인해 사용자는 발신자가 공인 기관임을 밝히는 경우 간단한 버튼 동작이나 음성인식으로 해당 기관의 공개키를 검색하고 공개키를 통한 암호화 인증 단계를 거쳐 발신자의 신원을 정확히 밝힐 수 있다.

2. 관련 연구

현재 국내에서는 국제전화번호 표시 서비스를 핸드폰 사용자들에게 제공하여 보이스 피싱을 방지하고 있다. 그러나 이 방법론은 핸드폰 서비스에 제한 되어있고 VoIP 환경에서는 IP Spoofing 같은 우회 방법이 존재하여 적용하기 힘들다. 그리고 현재 보이스피싱 시도가 국제에서만 일어난다는 제약 조건이 따른다. 따라서 본 논문은 보이스피싱을 원천적으로 방지할 수 있게 공개키 암호화 방법론을 도입하였다.

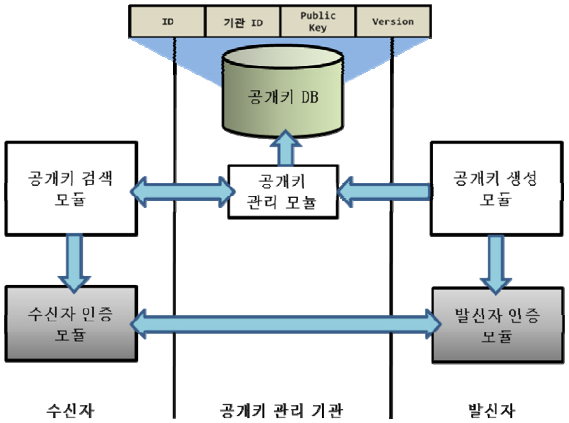
공개키 암호화 방법론(Public Key Cryptography)은 정보를 암호화하는 키와 복호화하는 키가 다른 기법이다. 비밀키(Private Key)만 사용하는 암호화 방법론의 경우 암호화 키와 복호화 키가 동일하여 해당 암호를 복호화해야 하는 대상에게 직접 비밀키를 전송함으로써 취약성을 드러내었다. 그러나 공개키 암호화 방법론의 경우 암호화하는 키를 공개적으로 분산 시키고 복화화하는 키는 자신만 소유하여 암호 통신 대상에게 쉽게 암호화 키를 제공하면서 비밀키 유실 취약성을 줄일 수 있어 용이하다[2].

공개키 암호화 방법론은 일반적으로 전자서명이나 메시지 암호화에 쓰인다. 전자서명의 경우 비밀키를 이용하여 암호화를 하고 상대방이 공개키를 이용해 복호화를 했을 경우 암호화를 한 대상을 인증할 수 있는 방법이다. 메시지 암호화의 경우 공개키로 암호화를 하고 메시지를 전송해 비밀키를 소지한 대상만이 복호화 할 수 있도록 메시지를 암호화하는 방법이다.

3. 보이스피싱 인증 시스템

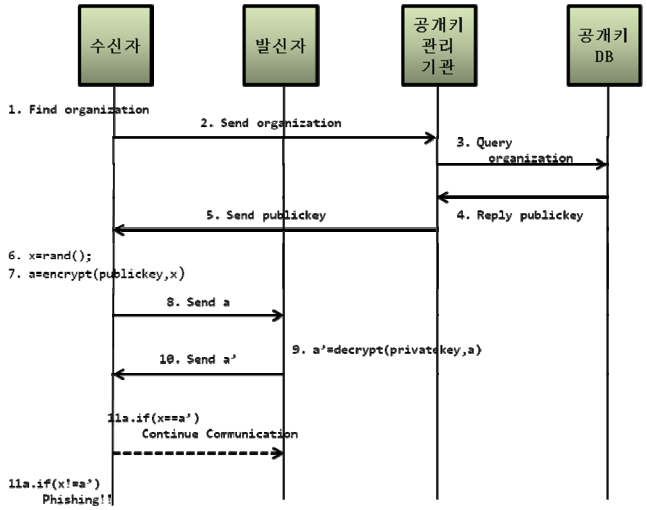
이 시스템은 공개키 암호화 방법론 통해 발신자를 인증하여 보이스피싱을 방지한다. 시스템의 전체 구성

도는 (그림 1)과 같다.



(그림 1) 보이스피싱 인증 시스템 전체 구성도

수신자는 보이스피싱 피해 예상자이며 발신자는 보이스피싱을 시도하는 악성 사용자이거나 실제 공인 기관일 수 있다. 공개키를 안전하게 관리하기 위해서는 공개키 관리 기관이 있어야 한다. 실제 공인 기관의 경우, 공개키와 그에 해당하는 비밀키를 생성하고 업데이트하는 공개키 생성 모듈이 필요하다. 이 모듈은 비밀키에 대한 보안을 높이기 위해 일정 시간 주기로 자신의 공개키와 비밀키를 생성하고 공개키 관리 기관에게 전송하는 기능을 한다. 공개키 관리 기관의 경우에는 각 공인 기관이 업데이트 하는 공개키를 실시간으로 데이터베이스에 저장하고, 발신자가 해당 기관의 공개키를 요청하면 보내주는 기능을 하는 공개키 관리 모듈이 필요하다. 공개키 DB 의 경우 기관의 ID, 해당 기관의 공개키, 그리고 최신의 공개키를 실시간으로 업데이트 하기 위해서는 해당 공개키 버전을 저장하고 있어야 한다. 발신자 쪽 모듈에서는 사용자가 발신자의 기관을 검색하고 해당 기관에 대한 공개키를 공개키 관리 기관에 요청할 수 있는 사용자 인터페이스가 포함된 공개키 검색 모듈이 있다. 이 모듈은 키워드 검색 인터페이스부터 음성 인식 인터페이스 등 여러 가지로 응용되어 개발 될 수 있다.
실제 인증 과정을 진행하는 모듈은 수신자 인증 모듈과 발신자 인증 모듈이다. 이 두 모듈 사이의 인증 순서와 시스템 전체적인 진행 순서는 (그림 2)를 통해서 알 수 있다.
발신자가 공인 기관이라고 밝힐 경우 수신자는 먼저 해당 기관을 검색한다. 그러면 수신자는 해당 기관의 공개키를 공개키 관리 기관에게 요청한다. 공개키 관리 기관에서는 해당 기관의 공개키를 DB 에서 검색하여 정보를 수신자에게 전송하다. 수신자는 이 공개키(publickey)를 이용하여 임의로 생성하는 수 (x) 를 암호화하고(encrypt) 이 암호화된 인증키(a)를 발신자에게 전송한다. 발신자는 a 를 자신만 가지고 있는 비밀키를 이용하여 복호화(decrypt)하여 다시 수신자에게 전송한다(a'). 수신자는 x 와 a'를 비교하여 같을 경우 발신자를 신용하고 아닌 경우 발신자가 보이스피싱 의심 IP 로 간주하고 사용자에게 경고를 준다.
위 과정을 통해 발신자가 실제 공인 기관이면 인증이 가능하여 사용자가 안심하고 발신자를 신용할 수 있고, 발신자가 악성 행위자이면 인증번호가 틀리거나 Timeout 되기 때문에 악성 행위자와 실제 공인 기관을 쉽게 구별할 수 있다.



(그림 2) 보이스피싱 인증 시스템 프로세스

4. 결론

보이스피싱 인증 시스템을 이용하면 사용자는 간편하게 발신자의 신원을 인증할 수 있다. 이것은 사용자 보이스피싱을 쉽게 판단할 수 있게 도와준다. 또한 간단한 인증 방법론으로 사용자가 전화하는데 있어 불편함이 없을 것이다. 기존의 간단한 발신자 위치를 토대로 한 국제 전화 번호표시 방법론 보다 더 정확한 발신자 정보를 알 수 있으며 VoIP 환경에서 IP Spoofing 을 하는 경우에도 발신자를 인증 할 수 있으므로 용이하다.
향후의 연구에서는 제안 시스템의 공개키 검색 모듈을 개선하여 음성인식을 통해 사용자가 어떠한 인위적인 검색 없이 자동으로 보이스피싱 인증 과정을 진행하는 방법을 연구 할 것이다. 이로 인해 사용자의 의사결정 없이 자동으로 보이스피싱을 탐지하고 방지할 수 있어, 무지한 사용자의 경우에도 보이스피싱에서 해방 될 수 있다.

사사(謝辭)
본 연구는 지식경제부의 IT R&D 사업의 일환으로 수행하였음. (2008-S-001-02, Development of WiBro Network Reliability and location Awareness technologies)

참고문헌

[1] Tan, Koon, "Phishing and Spamming via IM (SPIM)", *Internet Storm Center*. December 5, 2006.
[2] N. Ferguson, B. Schneier , "*Practical Cryptography*", Wiley
[3] 최두성, " 보이스피싱 피해 급증…알고도 속는다" , 매일신문 2009.8.18