쿠키를 이용한 802.11i 4-Way Handshake

엄성현° 최형기
성균관대학교 정보통신공학부
sheum@ece.skku.ac.kr, hkchoi@ece.skku.ac.kr

4-Way Handshake in 802.11i using cookie

Sunghyun Eum° Hyoungkee Choi
School of Information and Communication Engineering
Sungkyunkwan University, Suwon, South Korea

편리하게 인터넷에 접속할 수 있는 장점으로 인하여 최근 무선랜 사용자의 수가 급증하고 있다. 무선랜은 유선에 비해 이동성과 설치 비용 측면의 장점이 있기 때문에, 향후 무선랜의 가입자 수는 더욱 늘어날 것으로 전망된다. 높은 인기에도 불구하고 무선랜은 무선환경에서 필연적인 공격들에 심각하게 노출이 되어있다. 무선의 매체 특성상 암호화 기능이 제공되지 않으면 민감한 데이터가 제3자에게 노출되는 취약성이 있다. IEEE는 무선랜에서 암호화 통신을 지원하기 위해 802.1x를 발표하였다. 하지만, 802.1x가 제공하는 무선랜 보안에서 개인 정보가 침해되거나, man-in-the-middle 공격, denial of service (DoS) 공격에 대한 취약성이 알려지게 되었다. IEEE는 보다 강화된 보안을 제공하기 위해 802.11i를 발표하였다. 802.11i는 세션키 분배 방식과 상호 인증 메커니즘을 정의하고 있다. 그러나 802.11i의 세션키 분배 과정에서 사용되는 메시지의 취약점이 발견되었고, 이를 악용한 DoS 공격이 가능한 문제점이 있다.

802.11i는 4개의 메시지를 사용하여 세션키 분배 과정을 정의하고, 이를 4-way handshake로 부른다. 4-way handshake를 통해, 단말과 AP간에 동일한 마스터키 Pairwise Master Key (PMK)를 생성하였음을 확인하고, PMK를 인자로 하여 Pairwise Transient Key (PTK)를 생성한다. Changhua He는 4-way handshake에 사용되는 메시지 중, 보호되지 않는 첫 번째 메시지에 주목하였다. 그들은 첫 번째 메시지에 대한 DoS 공격이 가능함을 보였으며, 이 공격을 4-Way Handshaking Blocking라 한다 [1]. 공격자는 쉽게 MAC 주소를 위조할 수 있으므로, 임의로 만들어 낼 수 있는 첫 번째 메시지의 수는 이론적으로 한계가 없다. 공격은 첫 번째 메시지의 인자를 저장해야 하는 Access Point (AP)의 메모리를 고갈시키게 되고, 정상적인 서비스를 진행할 수 없게 된다. 그들은 4-way handshake Blocking을 제거하기 위해 몇 가지 해결책을 제안 하였다. 첫째, 취약한 첫 번째 메시지를 암호화하는 방법을 제안하였다. 암호화를 위한 키로 PMK를 사용하는 해결책이 제안될 수 있으나, PMK는 상대적으로 긴 시간 동안 변하지 않기 때문에 재전송 공격에 취약하다. 둘째, 단말이 생성하는 임의의 Nonce 값을 재사용하여 메모리 소모 공격을 계산 자원 소모 공격으로 바꾸는 방법이 있다. 대부분의 단말이 고성능의 CPU를 가지고 있기 때문에 공격을 무력화 시킬 수 있지만, key freshness를 보장하기 위한 랜덤 값을 재사용하기 때문에 잠재적인 문제점을 가지고 있다.

본 논문은 쿠키의 개념을 적용하여 단말에 대한 메모리 소모를 제거하는 방식을 제안한다. 제안된 해결책은 쿠키에 포함되는 내용에 따라 두 가지로 구분된다. 첫 번째 방법은 PTK를 암호화하여 전송하는 방법이고, 두 번째 방법은 PTK의 hash 값만 전송하는 방식이다. 4-way handshake 공격은 단말이 첫 번째 메시지에 포함되는 Nonce값과 PTK를 저장하는 점을 이용한다. 따라서 근본적으로 Nonce값과 PTK를 저장하지 않는 방식으로 공격을 제거할 수 있다.

우선, 단말이 PTK를 암호화 하여 전송하는 방식은, 첫 번째 메시지를 받은 단말이 PTK를 생성하면, 이

를 비밀키 *Kc*로 암호화하여 쿠키로 사용한다. 생성된 쿠키는 두 번째 메시지를 통해 AP로 전송되고, AP는 쿠키를 세 번째 메시지를 통해 다시 단말로 전송한다. 쿠키를 받은 단말은 이를 복호화 하여 PTK를 얻을 수 있으며, PTK를 통해 세 번째 메시지의 무결성을 확인할 수 있다. 세 번째 메시지의 무결성이 확보되면, 이에 대한 응답으로 네 번째 메시지를 보내고, 단말과 AP사이에 PTK로 보호되는 비밀 채널이 생성되게 된다. 암호화된 PTK를 쿠키로 이용하면, 기존 4-way handshake의 메모리 소모 공격을 제거할 수 있다. 반면, 이러한 방식은 암호화 및 복호화를 위한 추가적인 계산 자원 소모가 필요하고, 단말의 비밀키 Kc가 설정되어 있어야 한다. 실제 대칭키를 통한 암호화 및 복호화는 전체 인증과정에 비해 계산 자원 소모가 극히 적으며, 비밀키 Kc는 단말 자신만이 사용하는 키이므로 쉽게 설정할 수 있다.

PTK의 hash 값을 통한 방식은 이미 언급한 암호화된 PTK를 사용하는 방식과 유사하다. 다만 PTK를 암호화하여 직접 전송하지 않고, PTK에 대한 hash 값을 전송한다. 보다 상세히 설명하면, 첫 번째 메시지를 받은 단말은 PTK를 생성하고, 이에 대한 hash값을 쿠키로 두 번째 메시지에 첨부한다. AP는 쿠키를 세 번째 메시지를 통해 다시 단말에 돌려준다. 세 번째 메시지를 받은 단말은 PTK를 다시 계산하고, 계산된 PTK에 대한 hash값이 세 번째 메시지에 포함된 쿠키와 동일한지 확인한다. 이 때, 단말은 PTK를 만들 때 사용한 단말의 Nonce 값을 알 수 없기 때문에, AP는 세 번째 메시지에 해당 Nonce값을 포함하여 전송한다. PTK의 hash값을 전송하는 방식을 통해 4-way handshake 메모리 소모 공격을 제거할 수 있다. PTK의 hash 값을 이용하는 방식은 PTK를 암호화하는 방식과 달리, 단말이 비밀키를 설정하지 않아도 되는 장점이 있다.

PTK를 암호화 하여 쿠키를 만드는 방식은 기존 4-way handshake와 비교하여, 대칭키로 PTK를 암호화하고 복호화하는 시간이 추가적으로 소요된다. 또한, PTK의 hash값을 이용하여 쿠키를 만들 경우 PTK의 hash값 계산은 비교적 빠르지만, PTK의 재계산을 위한 시간이 추가로 필요하다. Pentium 4 2.1GHz 프로세서에서 시험한 결과에 따르면, DES와 MD5는 각각 초당 21.340MB, 216.674MB를 계산할 수 있다 [2]. 802.11i 환경에서 PTK는 암호화 방식에 따라 384bit 또는 512bit을 가질 수 있다. 따라서, 가정된 환경에서 512bit PTK에 대해 암호화 방식을 사용하면, 약 4.2μs의 추가적인 시간이 소모된다. PTK hash 방식에서 MD5를 사용하는 경우에는 약 0.2μs의 추가 시간과 PTK를 재계산하는 시간이 소모된다. 즉, 논문에서 제시하는 두 가지 방식은 4-way handshake를 보호하기 위해 추가적인 계산 시간이 소모되지만, 전체 인증 시간에 미치는 영향은 매우 작다.

본 논문은 802.11i 인증 과정 중, 세션키 분배 과정인 4-way handshake를 분석하였다. 4-way handshake는 인증 메시지의 일부가 보호되지 않은 상태로 전송되는 취약점을 가지고 있다. 이러한 취약점은 4-way handshake에 대한 DoS 공격을 가능하게 하고, 공격이 성공하게 되면 802.11i 전체 인증 과정이 취소되게 된다. 논문에서는 4-way handshake의 취약점을 제거하기 위해 쿠키의 개념을 적용하였다. 제안된 알고리즘은 쿠키에 포함되는 정보에 따라 두 가지로 구분되지만, 근본적으로 단말이 저장해야 할 정보를 쿠키로 만들어서 전송하는 기본 알고리즘은 동일하다. 해결책으로 제시된 두 알고리즘은 소요 시간에 차이가 있으나, 이러한 차이는 키 길이 및 사용되는 암호화 알고리즘과 관련하여 가변적이다. 802.11i은 무선랜의 대표적인 인증 메커니즘이며, 본 논문은 802.11i 인증 과정 중 4-way handshake에 대해 분석하였다. 논문은4-way handshake에 대한 DoS 공격을 무력화시킬 수 있는 두 개의 알고리즘을 제시하고 있다. 4-way handshake를 통한 안전한 키 분배가 보장되면, 802.11i은 사용자 서비스에 대해 강화된 무선랜 보안을 제공할 수 있게 된다.

참고문헌

[1] Changhua He, John C. Mitchell, "Analysis of the 802.11i 4-Way Handshake", In Proceedings of the Third ACM International Workshop on Wireless Security 2004

[2] Crypto++ Library 5.5.1, available at http://www.cryptopp.com/