Pay-TV 방송 시스템을 위한 Sun 등이 제안한 접근제어 시스템의 취약점 분석에 관한 연구 [1]

김정윤*, 강성용*, 장학범**, 최형기**
*성균관대학교 휴대폰학과
**성균관대학교 정보통신공학부
e-mail : {steal83, sykang, hbjang, hkchoi}@ece.skku.ac.kr

A Study on Weaknesses of Sun et al.'s Conditional Access System in Pay-TV Broadcasting Systems[1]

Jung-Yoon Kim*, Seong-Yong Kang*, Hak Beom Jang**, Hyoung-Kee Choi**
*Dept. of Mobile Systems Engineering, Sungkyunkwan University
**School of Information and Communication Engineering, Sungkyunkwan University

요 약

Sun 등은 pay-TV 를 위한 새로운 접근제어 모델을 제안하였다. 그들의 모델은 서비스 제공자와 사용자 간의 형평성 (fairness)을 보장하고, 사용자에게 편의 (convenience)를 제공한다. 또한, Sun 등은 그들이 제안한 접근제어 모델을 지원하기 위한 새로운 접근제어 시스템을 제안하였다. 그들이 제안한 시스템은 대규모 그룹에도 적용할 수 있도록 확장 가능한 (scalable) 키 관리를 수행한다. 그러나 그들의 시스템은 pay-TV 의 핵심 보안 요구사항인 후방향 안전성 및 전방향 안전성 (backward/forward secrecy)을 만족하지 못할 뿐 아니라, 공모 공격 (collusion attack)에 대한 취약점이 존재하고, 공격에 대한 낮은 복원 능력 (poor reparability)을 갖는다. 본 논문에서는 공격 시나리오를 통해 Sun 등이 제안한 시스템의 보안 문제점을 분석하고 그 결과를 제시한다.

1. 서론

접근제어 시스템 (Conditional Access System, CAS) [1], [2], [3], [4]은 사용자의 인증 및 키 관리를 통해 합법적인 사용자만이 비디오/오디오 스트림을 제공받을 수 있도록 허용하는 pay-TV 보안 시스템이다. 접근제어 시스템은, 사용자가 채널에 가입한 기간에 따라 요금을 부과하는 모델인 Pay-Per-Channel (PPC)과, 사용자가 시청한 프로그램에 따라 요금을 부과하는 모델인 Pay-Per-View (PPV)로 분류할 수 있다.

PPC 에서는 사용자가 아무런 조치를 취하지 않더라도 그룹에 대한 가입이 유지될 뿐 아니라, 가입한 그룹 내의 채널들을 언제든지 자유롭게 변경하며 시청할 수 있기 때문에, PPC 는 사용자에게 편의 (convenient)를 제공한다. 그러나 PPC 는 서비스 제공자가 일방적으로 채널들의 그룹을 구성하기 때문에, 사용자 입장에서는 원하지 않는 채널에도 가입해야 하는 비형평성 (unfairness)이 존재한다.

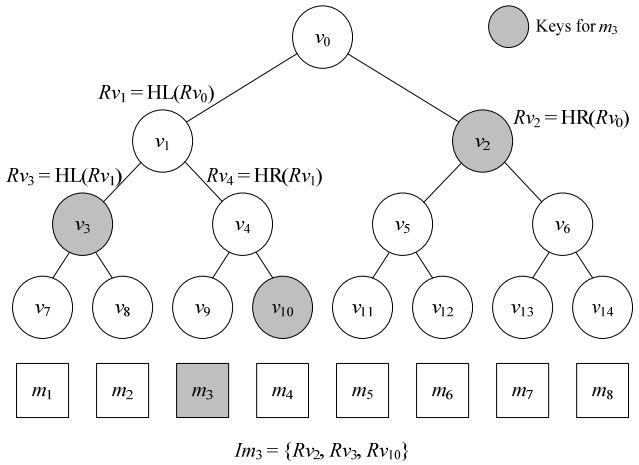
반면, PPV 에서는 사용자가 원하는 프로그램만 선택적으로 구매할 수 있기 때문에 형평성 (fairness)을 보장한다. 그러나, 프로그램마다 사용자가 구매를 요청해야 할 뿐 아니라, 자유롭게 채널들을 변경하지 못하고 구매한 프로그램만 시청할 수 있기 때문에, PPV 는 사용자에게 불편 (inconvenient)하다.

최근, Sun 등은 PPC 와 PPV 의 장점을 결합함으로써, 사용자의 형평성을 보장하고 편의를 제공하는 새로운 접근제어 모델인 Flexible Pay-Per-Channel (F-PPC)를 제안하였다 [2]. 그리고 그들은 F-PPC 를 지원하기 위한 새로운 접근제어 시스템을 제안하였다. 그러나 Sun 등이 제안한 시스템은 pay-TV 의 핵심 보안 요구사항인 후방향 안전성 및 전방향 안전성 (backward/forward secrecy) [5]을 만족시키지 못할 뿐 아니라, 공모 공격 (collusion attack)에 대한 보안 취약점이 존재한다. 또한, Sun 등이 제안한 시스템은 공격에 따른 피해를 복원할 수 있는 능력이 부족하다 (poor reparable). 본 논문에서는 Sun 등이 제안한 시스템의 보안 문제점을 분석하고 그 결과를 제시한다.

2. Sun 등이 제안한 접근제어 시스템의 동작 과정

Sun 등이 제안한 시스템에서는 스트림에 대한 사용자의 접근을 제어하기 위해, 제어단어 (Control Word, CW), 인증키 (Authorization Key, AK), 수신그룹키 (Receiving Group Key, RGK), 마스터개인키 (Master Private Key, MPK)로 이루어진 4 단계 키 체계를 사용한다. 서버는 CW 를 입력값으로 하여 의사난수생성기 (Pseudo Random-number Generator, PRG)를 수행한 결과값으로 비디오/오디오 스트림을 암호화 한다. AK 는 CW 를 암호화 하는데 사용되는 키이며, 각 방송 채널

[1] 이 논문은 2011 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(No.2011-0005037)



(그림 1) Sun 등이 제안한 시스템 [2]에서 RGK 의 갱신을 위해 사용하는 키 구조의 예시

마다 고유한 AK 가 존재한다. RGK 는 여러 방송 채널로 구성되어 있는 그룹마다 존재하는 그룹키이며, 다수 개의 AK 를 한꺼번에 분배하기 위해 사용된다. MPK 는 RGK 를 암호화 하는데 사용되며, 각 단말마다 고유한 비밀키이다. 즉, Sun 등의 시스템은 RGK 와 AK 의 갱신을 통해 접근제어를 수행한다.

Sun 등이 제안한 시스템의 경우, RGK 의 갱신을 위해 서버와 각 단말은 이진트리를 관리한다. 이진트리의 각 노드는 RGK 의 갱신에 사용되는 비밀값을 의미하며, 각 노드에 대해 해쉬함수 HL(·)과 HR(·)을 수행하면 각각 좌측 자식노드 (left child node)와 우측 자식노드 (right child node)가 생성된다. Sun 등이 제안한 시스템에서 단말 m_i 는 이진트리의 임의의 리프노드 (leaf node)에 위치하며, 단말 m_i 는 해당 리프노드와 루트노드 사이에 존재하는 모든 노드들의 이웃노드 (sibling node)에 해당하는 비밀값들을 보유한다.

(그림 1)은 Sun 등의 시스템에서 RGK 의 갱신을 위해 사용하는 키 구조의 예시를 나타낸다. (그림 1)의 Rv_i 는 노드 v_i 에 해당하는 비밀값을 나타낸다. (그림 1)에서 볼 수 있듯이, 단말 m_3 은 비밀값 Rv_1, Rv_4, Rv_9 의 이웃노드에 해당하는 비밀값의 집합인 $Im_3 = \{Rv_2, Rv_3, Rv_{10}\}$을 보유하고 있다. 그리고 단말 m_3 은 Rv_2, Rv_3 에 대해 해쉬함수 HL(·), HR(·)을 수행하여 자식노드 Rv_5, Rv_6, Rv_7, Rv_8을 생성하고, Rv_5, Rv_6에 대해 해쉬함수를 수행함으로써 궁극적으로는 Rv_9 를 제외한 모든 리프노드 Rv_7, Rv_8, Rv_{10}, Rv_{11}, Rv_{12}, Rv_{13}, Rv_{14}를 생성할 수 있다. 즉, 모든 단말은 자신과 관련된 리프노드를 제외한 나머지 리프노드에 해당하는 비밀값들을 획득할 수 있다.

만약 단말 m_k 가 그룹 G_j 로부터 탈퇴할 경우, 서버를 비롯한 모든 단말은 그룹 G_j 의 그룹키인 RGK_j 를 식 (1)과 같이 새롭게 갱신한다.

$$RGK_j' = RGK_j \oplus R_{G_j,u_k} \quad (1)$$

여기서 ⊕은 XOR 연산을 나타내며, R_{G_j,u_k} 는 탈퇴한 단말 m_k 와 관련된 리프노드에 해당하는 비밀값을 의미한다. 예를 들어, (그림 1)의 경우 R_{G_j,u_5}는 Rv_{11}을 나타낸다. 단말 m_k 가 탈퇴할 때, 서버는 탈퇴한 단말 m_k 의 ID 를 모든 단말에게 브로드캐스트 함으로써, 탈퇴한 단말의 트리에서의 위치를 알린다. 그리고 탈퇴한 단말 m_k 를 제외한 모든 단말은 단말 m_k 와 관련된 비밀값인 R_{G_j,u_k} 를 알고 있기 때문에, 식 (1)을 통해 새로운 RGK_j'을 획득할 수 있다. 탈퇴한 단말의 ID 만으로 각 단말이 RGK_j 를 갱신하기 위해서는, 위에서도 설명했듯이 가입자의 정보를 담고 있는 이진트리를 각 단말이 관리하고 있어야 한다.

새로운 단말 m_{n+1} 이 그룹 G_j 에 가입할 경우, 서버는 MPK_{n+1} 를 이용하여 RGK_j 및 Im_{n+1} 를 암호화 하여 m_{n+1} 에게 전달한다. 그리고 서버는 새로운 단말 m_{n+1} 이 트리 상에서 존재하는 위치를 모든 단말에게 브로드캐스트 한다. 이를 수신한 모든 단말은 새로운 단말 m_{n+1} 의 트리에서의 위치를 기억함으로써, 추후에 단말 m_{n+1} 이 탈퇴하였을 때 식 (1)과 같은 키 갱신을 수행할 수 있다. 한편, 새로운 단말이 그룹 G_j 에 가입한 경우에는 RGK_j 를 갱신하지 않는다.

만약 단말 m_k 가 그룹 G_j 에 포함된 채널 ch_c 로부터 탈퇴할 경우, 서버를 비롯한 모든 단말은 채널 ch_c 의 인증키 (채널 별 암호화 키)인 AK_c 를 갱신한다. AK 갱신에 사용되는 트리의 리프노드는 단말이 아니라 그룹이라는 점을 제외하면, AK 를 갱신하는 과정은 RGK 를 갱신하는 과정과 동일하다.

3. Sun 등이 제안한 접근제어 시스템의 보안 취약점

본 논문에서는 Sun 등의 시스템이 후방향 안전성, 전방향 안전성, 그리고 공모 공격에 취약하다는 것을 공격 시나리오를 통해 제시하고, 복원 능력이 낮다는 사실을 설명한다.

3.1. 후방향 안전성 (Backward Secrecy)

저자들의 주장과 달리, Sun 등이 제안한 시스템은 후방향 안전성 (backward secrecy) [5]을 보장하지 못한다. 후방향 안전성을 무너뜨리기 위한 공격 시나리오는 다음과 같다.

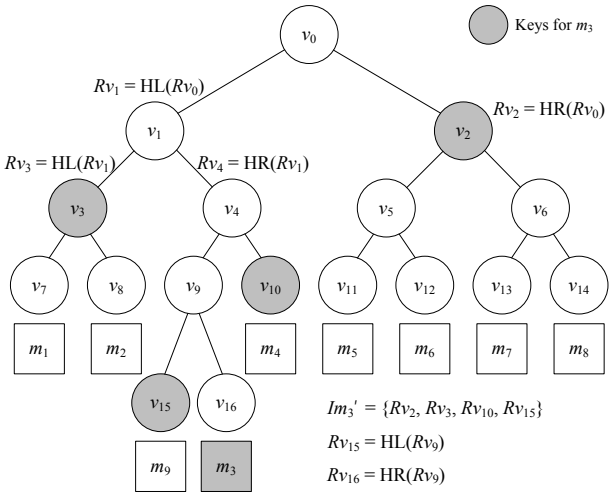
(그림 1)에서 단말 m_3 이 그룹 G_j 로부터 탈퇴하면, RGK_j 는 식 (2)와 같이 갱신된다.

$$RGK_j' = RGK_j \oplus R_{G_j,u_3} = RGK_j \oplus Rv_9 \quad (2)$$

이후에 단말 m_3 이 그룹 G_j 에 다시 가입하면, 서버는 기본적으로 단말 m_3 을 트리 상에서 과거에 위치했던 노드, 즉 v_9 에 다시 위치시킨다. 그리고 단말 m_3 은 서버로부터 MPK_3 으로 암호화 된 RGK_j'을 수신하게 된다. RGK_j'은 그룹 G_j 의 현재 RGK 를 의미한다.

이제 단말 m_3 은, 과거에 알고 있던 RGK_j, 그리고 그룹에 다시 가입하여 수신한 RGK_j'을 모두 알고 있기 때문에, 식 (3)과 같이 비밀값 R_{G_j,u_3} 를 획득할 수 있다.

$$R_{G_j,u_3} = RGK_j' \oplus RGK_j \quad (3)$$



(그림 2) Sun 등이 제안한 시스템 [2]에서 단말 m_3이 그룹에 다시 가입한 경우 키 구조의 예시

만약 단말 m_3이 그룹 G_j에 다시 가입하기 전에 단말 m_6이 해당 그룹으로부터 탈퇴하면, 그룹키 RGK_j'은 식 (4)와 같이 갱신된다.

$$RGK_j'' = RGK_j' \oplus R_{G_j,u_6} = RGK_j' \oplus Rv_{12} \quad (4)$$

단말 m_6이 탈퇴할 때, 서버는 m_6의 ID 를 그룹에 가입되어 있는 모든 단말에게 평문으로 브로드캐스트하기 때문에[2], 단말 m_3은 탈퇴한 단말 m_6의 ID 와 자신이 관리하는 이진트리를 이용하여 그룹키 갱신에 사용된 비밀값이 R_{G_j,u_6}이라는 것을 알 수 있다. 따라서, 단말 m_3은 그룹 G_j에 다시 가입하여 서버로부터 갱신된 그룹키 RGK_j''를 수신한 후, 식 (5)와 같이 RGK_j''로부터 과거의 그룹키 RGK_j'을 획득할 수 있다.

$$RGK_j' = RGK_j'' \oplus R_{G_j,u_6} = RGK_j'' \oplus Rv_{12} \quad (5)$$

RGK_j'을 획득한 단말 m_3은 식 (3)을 통해 비밀값 R_{G_j,u_3}을 획득할 수 있다. 이후에는 단말 m_3이 그룹 G_j로부터 탈퇴하더라도, 획득한 비밀값 R_{G_j,u_3}을 통해 갱신되는 모든 RGK_j들을 획득할 수 있다.

만약 단말 m_3이 그룹에 다시 가입하기 전에 다른 단말 m_9가 그룹에 가입하여 노드 v_9에 위치하게 되었을 때, 단말 m_3이 다시 가입하면 서버는 (그림 2)와 같이 v_9의 자식노드를 생성하여 좌측 자식노드에는 단말 m_9를 위치시키고 우측 자식노드에는 단말 m_3을 위치시킨다. 그리고 서버는 MPK_3으로 암호화된 RGK_j'와 $Im_3' = \{Rv_2, Rv_3, Rv_{10}, Rv_{15}\}$ (단, Rv_{15}는 Rv_9의 좌측 자식노드로서, 단말 m_9와 관련된 비밀값)을 단말 m_3에게 전송한다. 이를 수신한 단말 m_3은 식 (6)과 같이 새로운 R_{G_j,u_3}인 Rv_{16}을 획득할 수 있다.

$$R_{G_j,u_3}' = Rv_{16} = HR(Rv_9) = HR(RGK_j' \oplus RGK_j) \quad (6)$$

이후에는 단말 m_3이 그룹 G_j에서 탈퇴하더라도, 획득한 비밀값 R_{G_j,u_3}'을 통해 갱신되는 모든 RGK_j들을 획득할 수 있다. 따라서 Sun 등의 시스템은 어떠한 경우에도 후방향 안전성을 제공하지 못한다.

3.2. 전방향 안전성 (Forward Secrecy)

PPC 서비스에서 전방향 안전성 (forward secrecy) [5]은 중요한 보안 요구사항이다. 그룹에 가입하지 않은 단말 m_4가 암호화 된 비디오/오디오 스트림을 저장하고 있었다고 가정한다. 만약 해당 단말이 그룹 G_j에 가입하게 되면, 서버는 MPK_4로 현재의 그룹키인 RGK_j'를 암호화 하여 단말 m_4에게 전달한다. Sun 등이 제안한 시스템에서는 단말이 그룹에 가입할 때 그룹키가 갱신되지 않기 때문에, 단말 m_4는 RGK_j'를 통해 과거에 저장해두었던 암호화 된 스트림들을 복호화 할 수 있다.

또한, 단말 m_4는 RGK_j'으로부터 과거의 모든 그룹키를 획득할 수 있다. RGK_j'으로 갱신되기 이전의 그룹키를 RGK_j라고 가정한다. RGK_j가 그룹키로 사용될 때, (그림 1)과 같은 경우 단말 m_8이 그룹에서 탈퇴하면 그룹키 RGK_j는 식 (7)과 같이 RGK_j'으로 갱신된다.

$$RGK_j' = RGK_j \oplus R_{G_j,u_8} = RGK_j \oplus Rv_{14} \quad (7)$$

단말 m_8이 그룹에서 탈퇴할 때, 서버는 단말 m_8의 ID 를 그룹에 가입되어 있는 모든 단말에게 평문으로 전달하기 때문에, 단말 m_4는 그룹키의 갱신에 사용되었던 비밀값이 R_{G_j,u_8}이라는 것을 알 수 있다. 이후에 단말 m_4가 그룹 G_j에 가입하면, 서버는 단말 m_4에게 MPK_4로 암호화 된 RGK_j'와 Im_4를 전달한다. 현재의 그룹키인 RGK_j'과 Rv_{14}를 획득한 단말 m_4는, 식 (8)과 같이 과거의 그룹키 RGK_j를 획득할 수 있다.

$$RGK_j = RGK_j' \oplus R_{G_j,u_8} = RGK_j' \oplus Rv_{14} \quad (8)$$

한편, 단말 m_4가 그룹 G_j에 가입하기 이전에, 단말 m_9가 해당 그룹에 가입하여 노드 v_{10}에 위치하였다고 가정한다. 이후 단말 m_9가 해당 그룹에서 탈퇴하면, 그룹키 RGK_j는 식 (9)와 같이 RGK_j''으로 갱신된다.

$$RGK_j'' = RGK_j \oplus R_{G_j,u_9} = RGK_j \oplus Rv_{10} \quad (9)$$

이후에는 단말 m_4가 그룹 G_j에 가입하더라도, Rv_{10}을 모르기 때문에 과거의 그룹키인 RGK_j를 획득할 수 없다. 그러나 이러한 경우에도, 단말 m_4는 앞에서 설명한 후방향 안전성 (backward secrecy)에 대한 공격을 통해 Rv_{10}을 획득하여, 식 (9)으로부터 과거의 그룹키인 RGK_j를 획득할 수 있다. 따라서 Sun 등이 제안한 시스템은 전방향 안전성을 제공하지 못하며, 새롭게 가입한 단말은 과거에 송신되었던 모든 스트림을 과금 없이 시청할 수 있다.

[2] 서버는 탈퇴한 단말 m_6가 가입한 모든 그룹과 모든 채널의 가입자들이 RGK 와 AK 를 갱신할 수 있도록 m_6의 탈퇴 사실을 알려야 한다. 만약 m_6의 탈퇴 사실을 평문이 아닌 암호문으로 알린다면, m_6가 가입한 그룹 및 채널의 개수에 따라 서버가 수행해야 하는 암호화 연산 및 브로드캐스트 메시지의 크기는 선형적으로 증가한다. 수천만명의 가입자들이 빈번하게 가입/탈퇴를 반복하는 pay-TV 시스템에서 이러한 연산복잡도를 갖는 시스템은 성능 측면에서 적합하지 않다. 더불어, [2]의 TABLE IV 에 보면 브로드캐스트 메시지의 크기는 상수 (constant)로 표기되어 있다. 즉, [2]의 저자들도 브로드캐스트 메시지가 평문으로 전송된다는 것을 가정하고 있다.

3.3. 공모 공격 (Collusion Attack)

공모 공격 (collusion attack)은, 하나의 그룹 내에서 단말들이 단합함으로써 어떠한 단말도 과금 없이 서비스를 지속적으로 제공받는 것을 의미한다. Sun 등이 제안한 시스템은 이러한 공모 공격에 취약하다.

예를 들어, (그림 1)의 단말 m_1 과 m_7 이 각각 Rv_2 와 Rv_1 을 서로에게 전달하면, 두 단말 모두 그룹에서 탈퇴한 이후에도 과금 없이 서비스를 수신할 수 있게 된다. 반면, 기존 접근제어 시스템, [3], [4]의 경우 단말들이 서로에게 비밀값을 전달하더라도, 하나 이상의 단말이 그룹에 가입하고 있어야 공모 공격자들이 서비스를 지속적으로 수신할 수 있다. 따라서, [2]는 기존 접근제어 시스템, [3], [4]등의 다른 pay-TV 보안 프로토콜들에 비해 공모 공격의 위협에 더욱 심각하게 노출되어 있다. 한편, 단말 m_1 과 m_7 이 비밀값 Rv_2 와 Rv_1 을 공유하기 위해서는, 단말에 존재하는 스마트카드 혹은 저장장치로부터 비밀값을 추출해야 한다. 스마트카드 혹은 저장장치로부터 비밀값을 추출하는 기법들은 이미 제시되어 있기 때문에 [6], [7], 이러한 공격은 유효 (practical)하다고 주장할 수 있다.

3.4. 낮은 복원 능력 (Poor Reparability)

낮은 복원 능력 (poor reparability)은, 공격자에 의해 하나의 스마트카드 내에 저장되어 있는 임의의 비밀정보가 노출되었을 때, 해당 스마트카드뿐 아니라 공격을 받지 않은 모든 스마트카드에 저장되어 있는 정보도 갱신해야 하는 문제를 의미한다. 즉, 하나의 단말에 대해 공격이 발생했을 때, 이를 복원하기 위해 비현실적인 비용이 소모되는 시스템은 복원이 사실상 불가능 하다 (poor reparable). Sun 등의 시스템에서 공격을 통해 단말 m_1 이 비밀값 Rv_1 을 획득하게 될 경우, Rv_1 을 갱신하기 위해서는 시스템에 존재하는 모든 단말에 저장되어 있는 Rv_1 을 갱신해야 한다. 따라서 Sun 등의 시스템은 하나의 단말에 대한 공격이 발생했을 때 시스템의 복원이 사실상 불가능 하다.

4. 개선 방법 및 대안에 관한 논의

Sun 등이 제안한 시스템이 공모 공격에 취약한 이유는, 특정 단말이 모르는 장기 (long-term) 비밀값을 다른 모든 단말들은 알고 있기 때문이다. 즉, 특정 단말은 자신이 모르는 장기 비밀값을 다른 단말로부터 제공받는 대신, 해당 단말이 모르는 장기 비밀값을 해당 단말에게 제공함으로써 결과적으로 두 단말이 시스템으로부터 부당한 이득을 취할 수 있게 된다. 시스템이 이 공모를 탐지하기 어렵다는 것도 취약성의 또 다른 원인이 된다.

Sun 등의 시스템이 낮은 복원 능력을 갖는 이유는, 대부분의 단말이 서로 공통된 장기 (long-term) 비밀값을 갖고 있기 때문이다. 하나의 단말이 공격 당했을 때 시스템을 복원하기 위해서는 해당 단말에 저장되어 있는 모든 장기 비밀값을 갱신해야 하는데, 이 비밀값이 다른 단말에도 저장되어 있다면 해당 단말들도 그 비밀값을 갱신된 값으로 교체해야 한다. Sun 등의 시스템에서 특정 그룹의 전체 가입자 수가 n 명이라고 가정할 때, 모든 단말은 (n – 1)개의 장기 비밀값을 각각의 단말들과 공유하고 있으므로, 그 복잡도는 $O(n^2)$이라고 볼 수 있다. 결과적으로 하나의 단말이 공격 당했을 때 해당 단말이 가입한 그룹 중 하나의 그룹의 안전성을 복원하기 위한 복잡도는 $O(n^2)$이다. 즉, 복원에 필요한 복잡도가 지수적으로 (exponentially) 증가하기 때문에, Sun 등의 시스템은 공격에 대한 복원이 사실상 불가능하다고 할 수 있다.

결론적으로, 공모 공격으로부터 안전하고, 우수한 복원 능력을 갖기 위해서는, 단말들이 서로 모르는 장기 비밀값을 분배하여 보유하고 있어서는 안되며, 다수의 단말이 동일한 장기 비밀값을 공유해서도 안된다. Sun 등의 시스템을 일부 수정하는 것으로는 이 문제를 해결할 수 없으며, 단말들이 장기 비밀값을 공유하지 않도록 프로토콜을 새롭게 설계해야 한다.

5. 결론

기존 접근제어 모델인 PPC 와 PPV 의 단점을 극복하기 위해, Sun 등은 새로운 접근제어 모델인 F-PPC 를 제안하고, F-PPC 를 지원하는 새로운 접근제어 시스템을 제안하였다 [2]. 그러나 Sun 등이 제안한 시스템은 pay-TV 의 핵심 보안 요구사항인 후방향 안전성 및 전방향 안전성 (backward/forward secrecy)을 만족시키지 못할 뿐 아니라, 공모 공격 (collusion attack)에 대한 취약점이 존재하였다. 뿐만 아니라, Sun 등이 제안한 시스템은 하나의 단말에 대한 공격에 의한 피해를 복원하는데 소요되는 비용이 비현실적이기 때문에 (poor reparable), Sun 등이 제안한 시스템은 pay-TV 의 보안 시스템으로 사용하기에는 적합하지 못하다.

참고문헌

[1] B. M. Macq and J. J. Quisquater, “Cryptology for Digital TV Broadcasting,” *Proc. IEEE*, vol. 83. no. 6, pp.944-957, June 1995.

[2] H. M. Sun, C. M. Chen, and C. Z. Shieh, “Flexible-Pay-Per-Channel: A New Model for Content Access Control in Pay-TV Broadcasting Systems,” *IEEE Trans. Multimedia*, vol. 10, no. 6, pp. 1109-1120, Oct. 2008.

[3] Y. L. Huang, S. Shieh, F. S. Ho, and J. C. Wang, “Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems,” *IEEE Trans. Multimedia*, vol. 6, no. 5, pp. 760-769, Oct. 2004.

[4] B. Liu, W. Zhang, and T. Jiang, “A Scalable Key Distribution Scheme for Conditional Access System in Digital Pay-TV System,” *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 632-637, May 2004.

[5] P. Sakarindr and N. Ansari, “Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks,” *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 8-20, Oct. 2007.

[6] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Proc. 19th Advances in Cryptology*, Santa Barbara, 1999, pp. 388-397.

[7] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining smartcard security under the threat of power analysis attacks,” *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541-552, May 2002.