3GPP2의 브로드캐스트-멀티캐스트 서비스 보안 프레임워크

홍도원 | ETRI 정보보호연구본부 정보보호기반연구팀 선임연구원
TTA 암호기술연구반 참관자
강주성 | ETRI 정보보호연구본부 정보보호기반연구팀 선임연구원
신상욱 | 부경대학교 전자컴퓨터정보통신공학부

1. 서론

3세대 이동통신 네트워크상에서 하나의 링크를 통해 동일한 정보를 다수의 사용자에게 제공하는 point-to-multipoint 서비스, 즉 브로드캐스트와 멀티캐스트 서비스의 사용 빈도가 높아질 것으로 기대되기 때문에 이 서비스들을 효율적으로 지원하기 위한 기술이 필요하다. 이를 위해 3GPP(3rd Generation Project Partnership)와 3GPP2(3rd Generation Project Partnership 2)는 각각 MBMS(Multimedia Broadcast/Multicast Service)와 BCMCS (Broadcast/Multicast Service)에 대한 표준화를 추진 중에 있다.

브로드캐스트와 멀티캐스트 서비스의 핵심 요구사항은 효율적인 방법으로 네트워크 자원을 사용하여 다수의 사용자들에게 동시에 콘텐츠를 제공할 수 있어야 한다는 것이다. 콘텐츠가 무료로 제공되면 임의의 사용자들이 콘텐츠가 제공되는 채널에 액세스할 수 있다. 그러나 채널 액세스가 가입(subscription) 기반이면, 가입하지 않은 사용자들은 컨테츠를 이용할 수 없어야 한다. 이를 위해 사용자를 인증하고 안전한 방법으로 콘텐츠를 전달할 수 있는 보안 서비스가 필요하다. 3G 네트워크에서 point-to-point 서비스는 사용자를 인증하고 사용자와 네트워크 사이에 사용될 키들을 일치시키는 메커니즘을 사용한다. 이 키들은 시그널링 데이터에 대한 무결성을 보호하고 선택적으로 시그널링 데이터와 사용자 데이터 모두의 기밀성 보호를 위해 사용된다. 3G 브로드캐스트-멀티캐스트 서비스는 사용자를 인증하기 위해 point-to-point 서비스에서 사용한 것과 동일한 절차를 이용하는 것이 가능하다. 사용자 그룹에게 키를 전달하기 위해서는 독자적인 키 관리와 분배 메커니즘이 요구된다. 키 분배 기법은 브로드캐스트-멀티캐스트 키 전송을 보호하기 위해 point-to-point 기밀성에 의존할 수 있으며, 데이터 보호는 별도의 메커니즘을 요구한다.

본 고에서는 3GPP2에서 브로드캐스트-멀티캐스트 서비스 보안 프레임워크를 분석한다. 먼저 BCMCS 보안을 위한 표준화 동향을 살펴본 후, 현재 TSG (Technical Specification Group)의 최종 검토과정에 있는 S.P0083 v0.7 문서를 중심으로 BCMCS 보안 프레임워크를 상세히 분석한다.

2. 3GPP2 BCMCS 보안 표준화 동향

3GPP2에서 BCMCS에 관한 표준화는 2001년부터 시작되었으며, 단계 1 문서(S.R0030)는 2001년 8월부터, 그리고 단계 2의 초안 문서는 2002년 8월부터

작성하여 계속 수정 중에 있다. BCMCS의 보안에 관해서는 현재 "브로드캐스트-멀티캐스트 서비스 보안 프레임워크"(S.P0083)를 작성하여 계속 논의 중에 있다. 3GPP2는 가입되지 않은 사용자가 브로드캐스트 서비스에 액세스하는 것을 방지하기 위해 보안 메커니즘을 적용한다.

2002년 9월 회의에서 Qualcomm은 단계 2 BCMCS 보안 아키텍처의 첫번째 초안(v0.1)을 제안하였다. Qualcomm에 의해 제안된 "Broadcast Security Framework"는 BCMCS의 브로드캐스트 서비스 단계를 위한 보안 프레임워크를 정의한 것으로, 비용을 지불하지 않고 콘텐츠에 접근하려는 사용자들을 방지하기 위해 콘텐츠를 암호화하고, 복호화 키를 가입한 사용자들에게만 제공하는 것을 목적으로 한다. 2002년 10월 회의에서 Lucent는 ESP/IPsec을 적용한 보안 프레임워크를 제안하고 평가하였으며, Qualcomm은 9월 회의에서 제안한 프레임워크를 수정한 기법을 제안하였다. 2002년 11월 회의에서는 Lucent와 Qualcomm에 의해 제안된 두 기법을 통합한 v0.2 문서를 작성하였으며, 2002년 12월 회의에서는 신뢰 모델과 필요한 새로운 정의를 추가하고 몇가지 개념을 명확히 기술하여 v0.4 문서를 작성하였다.

2003년 1월 회의에서는 S.P0083의 문서 제목을 "Broadcast Security Framework"에서 "Broadcast-Multicast Service Security Framework"로 수정하고, TSG 검토를 위한 v0.5 문서를 완성하여 배포하였다. 2003년 5월 회의에서는 키 생성방법 개발을 결정하였으며, 가능한 한 3GPP2 표준 암호 함수를 사용하기로 하였다. 2003년 6월 회의에서 WG4는 TSG-X BCMCS Ad hoc 그룹과의 회의를 통해 현재의 S.P0083 문서를 TSG-X BCMCS 문서와 일관성이 있도록 수정하였다. 또한 2003년 7월 회의에서 Lucent는 BCMCS를 위한 보안 함수를 제안하였으며, WG4는 이를 채택하여 S.P0083 문서에 포함시켜 v0.7 문서로 수정하였다. WG4는 S.P0083 v0.7 문서를 TSG에 제출하여 검토를 요청하였다.

3. 3GPP2 BCMCS 보안 프레임워크

이 절에서는 현재 TSG 검토를 위해 제출된 S.P0083 문서를 중심으로 3GPP2에서 개발중인 BCMCS 보안 프레임워크를 분석한다. 3GPP2 BCMCS의 목적은 허가된(가입된) 사용자에게 브로드캐스트/멀티캐스트 서비스를 제공하는 것이다. CS(Content Source)는 셀룰라 시스템을 통해 BCMCS 가입자에게 콘텐츠를 제공한다. 콘텐츠는 오디오/비디오 데이터와 같은 IP 멀티미디어 메시지이거나 또는 브로드캐스트 멀티미디어 메시지일 수 있다. CS는 방문 네트워크(serving network)의 일부일 수도 있고 또는 독립적인 개체일 수 있다. 콘텐츠가 무료로 제공되면 임의의 사용자들이 콘텐츠에 접근할 수 있다. 브로드캐스트 서비스로의 접근이 가입 기반이면 콘텐츠는 허가된 사용자들만이 접근할 수 있도록 암호화되어질 수 있다. 3GPP2 S.P0083 문서는 브로드캐스트 서비스를 위한 보안의 필요성을 다룬다.

하나의 CS가 하나 이상의 캐리어(carrier)에 하나 이상의 BCMCS를 제공할 수 있다. 사용자들은 그들의 캐리어를 통해 또는 직접 CS로부터 서비스에 가입할 수 있다. 사용자 가입 프로파일을 지원하는 개체는 SM(Subscription Manager)이다. 사용자는 하나 이상의 SM을 통해 하나 이상의 서비스에 가입할 수 있다. SM은 서비스 권한부여를 제공하고 BCMCS 키 관리에서 핵심적인 부분이다.

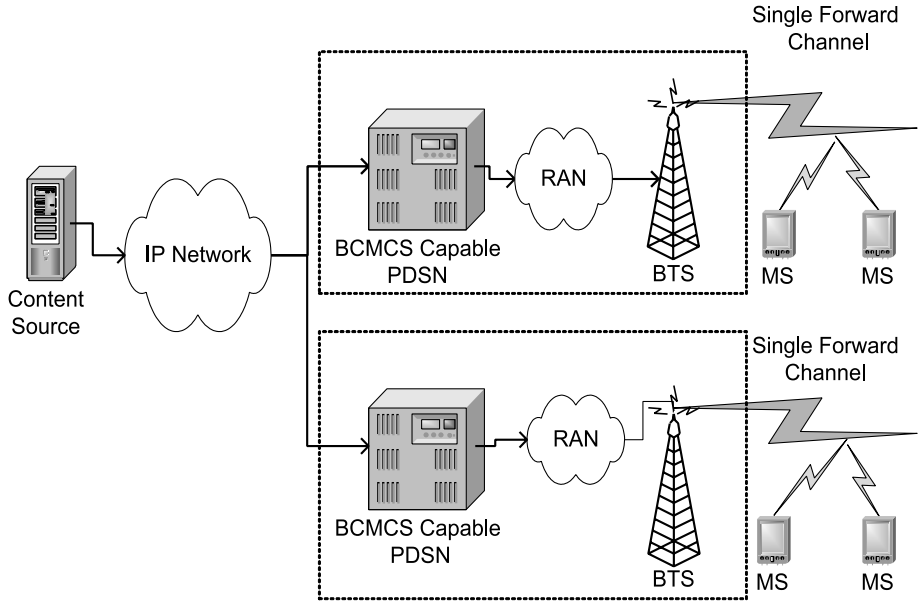

그림 1. 브로드캐스트-멀티캐스트 서비스 개요

3.1 BCMCS 키 관리 개요

MS(Mobile Station)는 두 개의 분리된 개체, UIM(User Identity Module)과 ME(Mobile Equipment)로 고려된다. UIM은 안전한 메모리를 가진 저전력 프로세서이다. ME는 고전력 프로세서이지만 안전한 메모리를 가지지 않는다. ME와 UIM은 하나의 물리 유닛으로 통합될 수도 있다. 사실 MS는 내부의 안전한 메모리를 가진 신뢰되는 ME로 간주될 수 있다.

셀룰러 서비스를 위한 사용자 인증과 권한부여뿐만 아니라 네트워크 보안은 BCMCS 보안 표준 문서에서 정의하지 않는다. BCMCS 보안에서는 다음의 신뢰 모델을 가정한다. 모든 네트워크 개체들은 그들이 통신하는 다른 네트워크 개체를 신뢰한다고 가정한다. 그리고 네트워크 개체들간의 통신은 안전하고 모든 네트워크 개체들은 자신의 작업을 정확히 수행한다고 가정한다. UIM은 SM에 의해 신뢰되고 그 역도 성립한다. 모든 네트워크 개체는 UIM이 비밀 값을 유지하고 정확하게 동작한다는 것을 신뢰한다. 그렇지만 UIM은 SM만을 신뢰한다.

3GPP2의 BCMCS에서 다루는 주요 위협은 사용자가 특정 콘텐츠 스트림에 대해 허가되지 않고 그 스트림의 내용에 접근하는 것이다. 이 위협을 방지하기 위해 콘텐츠는 ME에게 암호화되어 전달되고 복호화 키는 BCMCS를 수신하는 것이 허가된(가입된) 사용자들에게만 제공된다. 여기서의 주요 초점은 권한부여를 요구하는 콘텐츠 스트림에 대한 키 관리 기법이다.

콘텐츠는 유일하고 빈번하게 변경되는 SK(Short-term Key)를 사용하여 암호화된다. ME는 동일한 SK를 사용하여 콘텐츠를 복호화한다. SK는 허가되지 않은 사용자와 자신의 SK를 공유하는 "rogue shell"의 영향을 최소화하기 위해 빈번하게 변경되어야 한다. SK는 무선상으로 전달되지 않으며, BAK(Broadcast Access Key)와 암호화된 콘텐츠와 함께 브로드캐스

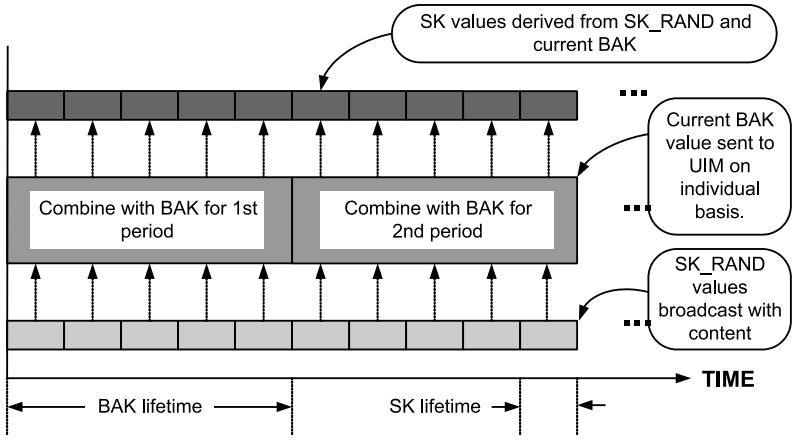

그림 2. BCMCS 키 관리 개요

트되는 난수로부터 UIM에 의해 유도된다.

사용자가 필요한 BAK 값을 복호화하기 위해 사용자의 UIM은 SM과 RK(Registration Key)를 공유해야 한다. RK의 제공은 이 문서의 범위밖이다. TK(Temporary Key)는 SM에 의해 RK로부터 유도되어 BAKD(BAK Distributor)에게 전달되고 BAK를 암/복호화하기 위해 BAKD에 의해 사용된다.

BAK는 BAKD에 의해 암호화되어진다. BAKD는 CS 또는 SM 또는 visiting 셀룰러 시스템에 관련되어진다. 동일한 BAK가 특정 콘텐츠 스트림에 가입한 모든 사용자에게 제공되고 미리 정의된 시간동안 유효하다. UIM이 암호화된 BAK를 획득하면, BAK를 복구하여 브로드캐스트를 복호화하기 위해 필요한 SK를 계산한다. SK는 콘텐츠 복호화를 위해 ME에게 전달된다. BAK는 ME에게 누설되지 않는다. 미리 제공된 정확한 RK를 가진 UIM만이 BAK를 복구할 수 있다.

3.2 보안 기능적 아키텍처

그림 3은 BCMCS에 관련된 기능 개체들을 보여준

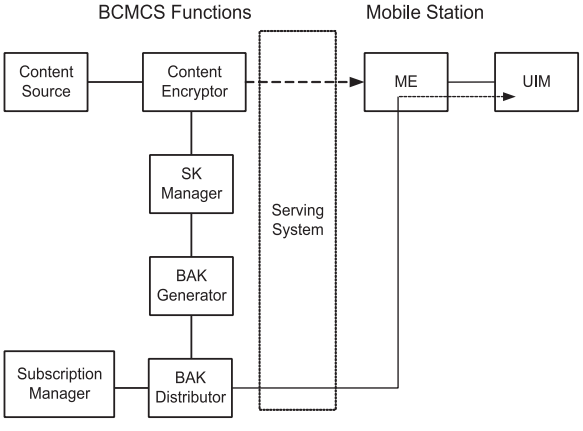

그림 3. 기능적 아키텍처

다. 이 개체들은 안전한 BCMCS를 지원하기 위해 필수적인 기능들을 나타낸다. 네트워크에서 하나 또는 여러 개의 물리적 개체로 통합될 수 있다. 이들 기능 개체들이 분리된 구조 개체들에 해당한다고 가정하지 말아야 한다. 따라서 모든 인터페이스들이 표준화를 요구하지는 않는다.

먼저 콘텐츠가 전달되는 경로에서 CS(Content Source)와 CE(Content Encryptor)가 관련된다. CS는 암호화되지 않은 콘텐츠를 생성하며, CE는 SKM(SK Manager)에 의해 제공되는 SK를 사용하여 콘텐츠를 암호화한다. 키와 권한부여 경로에는 SM(Subscription Manager), BAKG(BAK Generator), BAKD(BAK Distributor), SKM(SK Manager)이 관련된다. SM은 AAA의 기능을 제공하며, UIM과 등록키 RK(Registration Key)를 공유한다. 이 키는 A-Key 또는 AAA를 위해 사용되는 키 K 또는 브로드캐스트 서비스를 위해 제공된 또다른 키일 수 있다. SM은 사용자 고유의 RK에 기반하여 TK를 계산한다. BAKG는 BAK를 생성하여 BAKD와 SKM에게 분배한다. BAKD는 BAK의 분배를 제어한다. SKM은 SK의 갱신과 분배를 제어한다.

그리고 MS(Mobile Station)는 UIM(User Identity Module)과 ME(Mobile Equipment)로 구성된다고 가정한다. UIM은 SM과 RK를 공유하고, BCMCS에 관련된 모든 키 관리를 수행한다. ME는 브로드캐스트를 수신하기 위한 장비를 포함하며, UIM으로부터 획득한 SK를 사용하여 암호화된 콘텐츠의 복호화를 수행한다.

3.3 키 분배 메커니즘

그림 4는 BCMCS 암호화를 위한 키 분배에 관련된 기본적인 통신을 보여준다.

3.3.1 BAK 생성

다음의 단계 ①~②는 MS에게 암호화된 콘텐츠를 전달하기 이전에 수행된다.

① UIM과 SM는 BCMCS에 관한 인증과 키 교환의

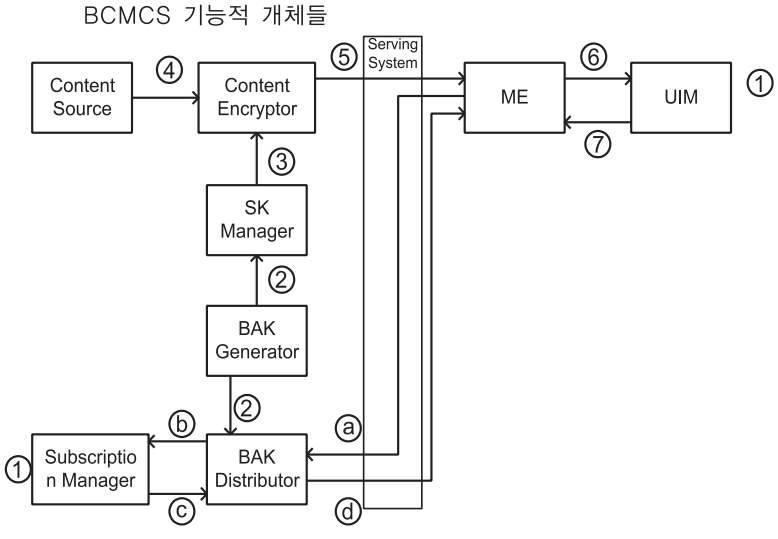

그림 4. BCMCS 보안에 관련된 기능적 개체들 사이의 통신흐름

기본이 되는 RK를 가지고 있다.

② BAKG는 BAK를 생성하고 식별자 BAK_ID와 만료 시간 BAK_Expire에 관련시킨다. BAK, BAK_ID, BAK_Expire는 SKM과 BAKD에게 전달된다.

3.3.2 변경되지 않은 BAK를 가진 멀티캐스트 IP 콘텐츠 암호화를 위한 정상적인 절차

다음의 단계 ③~⑦은 MS에서 BAK가 이전의 복호화 동작으로부터 변경되지 않았을 때 발생하는 정상적인 상황이다.

③ SKM은 현재의 BAK와 SK_RAND로부터 SK를 생성한다. SKM은 SK, SK_RAND, BAK_ID, BAK_Expire를 CE에게 전달한다.

④ CS는 CE에게 암호화되지 않은 콘텐츠를 전달한다.

⑤ CE는 SK를 사용하여 콘텐츠를 암호화하여 serving system을 통해 MS에게 전달한다. CE는 또한 암호화된 콘텐츠 스트림과 함께 SK_RAND와 BAK_ID를 전달한다.

⑥ ME는 암호화된 콘텐츠를 수신하면 다음과 같이 동작한다.

a. BAK_ID와 SK_RAND가 마지막 수신된 콘텐츠로부터 변경되지 않았다면 ME는 그 콘텐츠에 현재 할당된 SK를 사용하여 콘텐츠를 복호화하여 사용자 애플리케이션에게 전달한다.

b. BAK_ID 또는 SK_RAND가 변경되었다면, ME는 UIM에게 새로운 SK를 요구한다. 이 request에는 BCMCS_FLOW_ID, BAK_ID, SK_RAND가 포함된다.

⑦ UIM은 BAK와 SK_RAND로부터 SK를 생성하여 ME에게 SK를 반환한다. ME는 콘텐츠를 복호화하여 사용자 애플리케이션에게 전달한다.

3.3.3 변경된 또는 활용 가능하지 않은 BAK를 가진 절차

그림 4에서 단계 ⓐ~ⓓ는 MS에서 새로운 BAK를 요구할 때 수행된다.

ⓐ ME는 BAKD에게 요구되는 BAK의 BAK_ID를 포함한 BAK request를 전송한다. SM에 의해 request가 정당한 가입자로부터 왔다는 것을 결정할 수 있도록 BAK request는 RK에 기반한 인증정보를 포함할 수도 있다.

ⓑ UIM에게 BAK를 전송하기 위해 BAK는 의도된 수신자 외의 다른 개체에 의해 수신되는 것을 방지하기 위해 암호화되어야 한다. BAKD는 SM에 의해 생성된 temporary key TK를 요구한다.

ⓒ SM은 TK_RAND와 RK로부터 TK를 생성한다. TK_RAND는 BAKD 또는 SM에 의해 생성될 수도 있다. TK_RAND는 단계 a에 기술된 인증과정에서 challenge로 사용될 수도 있다. SM은 TK와 TK_RAND를 BAKD에게 전송한다.

ⓓ BAKD는 TK로 BAK를 암호화하여 TK_RAND, BAK_Expire와 함께 ME를 통해 UIM에게 전송한다. UIM은 TK_RAND와 RK로부터 TK를 계산한 후 암호화된 BAK를 복호화하여 BAK를 얻는다. BAK와 BAK_Expire는 UIM에 저장된다. UIM은 BAK lifetime의 만료를 예상하여 새로운 BAK를 획득하여 저장할 수 있도록 적어도 두 개의 BAK 값을 저장할 수 있어야 한다.

3.4 BAK 관리

사용자는 다수의 콘텐츠 스트림에 대해 BAK 갱신 과정을 반복할 수 있다. 그 이후에 MS는 동시에 다수의 콘텐츠 스트림을 위한 복호화 키를 관리하는 능력을 가진다. 어느 BAK가 어느 콘텐츠 스트림에 해당하

는지를 결정하기 위해 BCMCS 식별자인 BCMCS_FLOW_ID가 BAK와 함께 저장되어야 한다. 표준 문서에서는 MS가 BAK 갱신을 어떻게 결정하는지는 명시하지 않는다. 자신의 BAK가 만료되는지 또는 만료되었는지를 결정하기 위해 MS에게 어떤 수단이 제공된다고 가정한다.

- BAK_ID : UIM은 해당하는 BCMCS_FLOW_ID를 참조하여 BAK가 특정 콘텐츠 스트림에 관련되었는지를 결정할 수 있다. 그렇지만 특정 BCMCS_FLOW_ID에 관련된 두 개의 BAK 값을 저장할 필요가 있을 때가 있다. 이것은 BAK가 실제 SK를 암/복호화하기 위해 사용되기 이전에 UIM에서 BAK가 갱신되어야 하기 때문이다. 결국 이전 BAK와 새로운 BAK가 동시에 UIM에 존재한다. UIM은 어느 BAK가 유효한지를 결정하기 위한 수단을 가져야 한다. 권고되는 방법은 BCMCS_FLOW_ID에 추가로 BAK 식별자 BAK_ID를 각 BAK에 할당하는 것이다. BAK는 BCMCS_FLOW_ID와 BAK_ID에 의해 식별된다. CE는 브로드캐스트 데이터에 암호화된 콘텐츠와 함께 BAK_ID를 포함시킨다. UIM은 이것을 이용하여 이전의 BAK가 사용되는지 새로운 BAK가 사용되는지를 구별할 수 있다.

BAK_Expire 값은 BAK와 함께 제공된다. 따라서 MS는 만료된 키를 갱신할 수 있다.

- BAK_Expire : BAKG는 BAK가 얼마나 빈번하게 변경될 것인지를 결정한다. 다음의 이슈들이 BAK 변경주기를 결정하는데 고려되어야 한다.
  - 빈번한 BAK 변경은 더 강한 안전성을 제공할 것이다.
  - 빈번한 BAK 변경은 가입자 제어에서 더 큰 유연성을 제공할 것이다.
  - BAK 변경 빈도 증가는 MS가 새로운 BAK 값을 갱신해야 하는 회수의 증가에 대해 평가되어져야 한다.

3.5 BCMCS 보안 알고리즘

3.5.1 콘텐츠 암호화

링크계층 암호화를 사용하는 방법과 상위계층 프로토콜을 사용한 콘텐츠 암호화의 두 가지 방법이 존재하지만 현재 S.P0083 v0.7 문서에서는 후자만을 정의하고 있다. 이 경우 BCMCS 콘텐츠는 BCMCS 콘텐츠를 전달할 수 있는 IETF 프로토콜에 의해 정의된 상위계층 프로토콜에 의해 암호화되어야 한다. 한가지 예는 SRTP(Secure Real-time Transport Protocol) 프로토콜이다. 스트림 암호화 키는 SK이다.

3.5.2 BAK 암호화

BAK 암호화는 S.S0055에 정의된 ESP_AES 알고리즘을 사용하여 수행되어야 한다. 이 경우 ESP_AES의 입력 파라미터는 다음과 같이 설정되어야 한다.

- 암호화 키 파라미터는 TK로 설정된다.
- fresh 파라미터는 TK_RAND로 설정된다.
- freshsize 파라미터는 8로 설정된다.
- buf 파라미터는 암호화되거나 복호화될 데이터를 유지하는 버퍼의 첫 번째 비트를 포함한 바이트의 주소로 설정된다.
- bit_offset은 0으로 설정된다.
- bit_count는 128로 설정된다.

3.5.3 TK 관리

(1) TK_RAND

TK_RAND는 64비트 길이를 가져야 하며, S.S0055에 명시된 f0 알고리즘에 의해 생성되어야 한다. f0 함수의 입력 파라미터는 다음과 같이 설정되어야 한다.

- K 파라미터는 RK로 설정된다.
- fi 파라미터는 0x41로 설정된다.
- Fmk 파라미터는 0x41484147로 설정된다.

(2) TK 생성

TK는 S.S0055에 명시된 f3 알고리즘에 의해 생성되어야 하며, 128비트 길이를 가진다. f3 함수의 입력 파라미터는 다음과 같이 설정되어야 한다.

- K 파라미터는 RK로 설정된다.
- fi 파라미터는 0x45로 설정된다.
- RAND 파라미터는 TK_RAND|TK_RAND로 설정된다.
- Fmk 파라미터는 0x41484147로 설정된다.

3.5.4 SK

(1) SK_RAND

SK_RAND는 S.S0055에 명시된 f0 알고리즘에 의해 생성되며 f0의 64비트 출력에서 최하위 32비트로 설정되어야 한다. f0 함수의 입력 파라미터는 다음과 같이 설정되어야 한다.

- K 파라미터는 랜덤하게 선택된 값으로 설정된다.
- fi 파라미터는 0x41로 설정된다.
- Fmk 파라미터는 0x41484147로 설정된다.

(2) SK 생성

SK는 S.S0055에 명시된 f3 알고리즘에 의해 생성되어야 하며, 128비트 길이를 가진다. f3 함수의 입력 파라미터는 다음과 같이 설정되어야 한다.

- K 파라미터는 BAK로 설정된다.
- fi 파라미터는 0x45로 설정된다.
- RAND 파라미터는 SK_RAND|SK_RAND|SK_RAND|SK_RAND로 설정된다.
- Fmk 파라미터는 0x41484147로 설정된다.

4. 결론

BCMCS는 하나의 링크를 통해 동일한 정보를 다수의 사용자에게 제공하는 point-to-multipoint 서비스로, 네트워크 자원을 효율적으로 사용하여 다수의 사용자들에게 동시에 콘텐츠를 제공할 수 있어야 한다는 것을 목적으로 한다. BCMCS는 서비스 사용 권한이 없는 사용자들이 콘텐츠를 이용할 수 없도록 사용자를 인증하고 안전한 방법으로 콘텐츠를 전달할 수 있는 보안 서비스를 필요로 한다. 3GPP2 S.P0083은 브로드캐스트-멀티캐스트 서비스 보안 프레임워크를 정의하고 있으며, 본 고에서 이를 자세히 소개하였다. 현재 S.P00873 문서는 버전 0.7 문서가 작성되어 현재 TSG에서 최종 검토과정에 있으며, 큰 변화없이 아직 정의되지 않은 보안 알고리즘 등이 추가된 후 승인될 것으로 예상된다.

향후 BCMCS 보안에서 고려해야 할 사항은 키 분배 기법과 멀티캐스트 콘텐츠의 무결성에 관한 것이다. 현재의 문서에서 키 분배과정은 point-to-point 형태로 수행되며, BCMCS가 네트워크 자원을 효율적으로 사용하는 것을 목적으로 하기 때문에, BCMCS 보안을 위한 키 분배 역시 네트워크 자원을 효율적으로 사용하는 것이 요구된다. 이를 위해 현재 IETF에서 개발되고 있는 LKH 등의 기법을 BCMCS 키 분배에 적용하는 방안에 관해 계속적으로 연구되어야 한다. 또

한 현재의 문서에서는 콘텐츠의 기밀성만을 제공하고 있는데, 콘텐츠의 무결성과 출처 인증도 중요한 요소이므로 이들 보안 서비스를 효율적으로 제공할 수 있는 기법에 관한 연구가 수행되어야 할 것으로 사료된다.

참고문헌

[1] 3GPP2 S.R0030 Version 1.0, "Broadcast/Multicast Services Stage 1", August 2001

[2] 3GPP2 S.P0083 Version 0.7, "Broadcast-Multicast Service Security Framework", 15 July, 2003

[3] 3GPP2 S.S0055 Version 1.0, "Enhanced Cryptographic Algorithms", 21 January 2002

[4] M. Baugher, E. Carrara, D.A. McGrew, M. Naslund, K. Norrman, "The Secure Real-time Transport Protocol", IETF draft-ietf-avt-srtp-09.txt, July 2003

[5] D. Wallner, E. Harder, R. Agee, "Key management for multicast: Issues and architectures", IETF, RFC 2627, June 1999