TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.0115/R2

개정일: 2018년 12월 xx일

SRTP에서의 ARIA 알고리즘 운영 방법

The Use of ARIA Algorithm in SRTP

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 사이버보안 프로젝트그룹(PG503)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	박제홍	NSR	책임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.0115/R2
표준 초안 작성자	박제홍	NSR	책임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.0115/R2
	김우환	NSR	책임연구원	-	TTAK.KO-12.0115/R2
	권대성	NSR	책임연구원	-	TTAK.KO-12.0115/R1
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

서 문

1 표준의 목적

이 표준의 목적은 안전한 실시간 전송 프로토콜(SRTP, Secure Real-time Transport Protocol)에서 국내 블록 암호 알고리즘 표준인 ARIA를 사용하기 위한 방법을 정의하여, ARIA의 SRTP 적용에 대한 상호 운용성(Interoperability)을 확보하는 것이다.

2 주요 내용 요약

이 표준은 ARIA를 CTR(Counter) 모드와 GCM(Galois/Counter Mode)의 기반 블록 암호로 사용하여 실시간 전송 프로토콜에서 정의하는 RTP와 RTCP 패킷의 암호화와 인증 태그 계산, 그리고 세션키 유도에 적용하는 방법을 정의한다. 구체적으로는 미국 연방정부 표준 블록 암호 AES의 SRTP 적용 방법을 준용한다. 그리고 SRTP의 기본 키 관리 방식인 SDES(Session Description Protocol Security Descriptions)를 통해 세션 참여자들이 ARIA 적용을 위한 주요 파라미터를 협상하는 과정에서 필요한 crypto suite를 정의한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에서 제시하는 ARIA의 SRTP 적용 방법은 IETF RFC 8269에 제시된 내용과 같다. 그리고 ARIA 기반 SRTP crypto suite는 IETF RFC 8269에 정의된 DTLS-SRTP 보호 프로파일(protection profile)과 일대일로 대응한다.

3.2 인용 표준과 본 표준의 비교표

해당 사항 없음

Preface

1 Purpose

The standard defines the use of a korean standard block cipher algorithm ARIA in SRTP(Secure Real-time Transport Protocol) to facilitate the interoperability.

2 Summary

The standard describes how ARIA can be used to provide confidentiality and/or integrity to RTP/RTCP packets, and to provide session keys for the respective security primitives. Specifically, detailed descriptions of the use of ARIA for the encryption transform and the key derivation function are defined as the same with the cases of AES. Additionally, this standard defines new SRTP crypto suites of ARIA to be used to signal and negotiate them via SDES(Session Description Protocol Security Descriptions).

3 Relationship to Reference Standards

The standard provides the same mechanism for using ARIA in SRTP with IETF RFC 8269. And each SRTP crypto suite defined in this standard corresponds one-to-one to the individual DTLS-SRTP protection profile defined in IETF RFC 8269.

목 차

SRTP에서의 ARIA 알고리즘 운영 방법
(The Use of ARIA Algorithm in SRTP)

1 적용 범위

안전한 실시간 전송 프로토콜(SRTP, Secure RTP)[2]은 오디오, 비디오와 같은 멀티미디어 데이터를 전송하는 용도로 설계된 실시간 전송 프로토콜(RTP, Real-time Transport Protocol)[1]에 대한 기밀성, 무결성, 메시지 인증, 재전송 공격 방어 등의 정보보호 서비스를 제공한다.

SRTP는 정보보호 서비스 제공을 위한 기반 블록 암호로 AES를 권고하고 있으며[2,4], 다양한 보안 요구 사항을 추가로 반영하기 위해 여러 가지 확장 규격을 정의하고 있다[7,10,11].

이 표준에서는 먼저 ARIA의 SRTP 적용 방법을 정의하여, SRTP에서 국내 블록 암호 알고리즘 표준인 ARIA[13,14]를 사용할 수 있도록 한다. 그리고 SRTP의 기본 키 관리 방식인 SDES[4]를 통해 세션 참여자들이 ARIA 적용을 위한 주요 파라미터를 협상하는 과정에서 필요한 ARIA 기반의 SRTP crypto suite를 정의한다.

이 표준은 블록 암호 ARIA를 사용하여 구현된 SRTP의 직접 적용 또한 호환이 필요한 정보보호 시스템 및 암호 제품에 다양하게 활용할 수 있다.

2 인용 표준

IETF RFC 8269 (2017), The ARIA Algorithm and Its Use with Secure Real-Time Transport Protocol (SRTP) (2절과 3절, 그리고 5절을 인용함)

3 용어 정의

3.1 암호 알고리즘 용어

3.1.1 AES(Advanced Encryption Standard)

국제 공모 프로젝트를 통해 개발된 미국 연방정부 표준 블록 암호 알고리즘[12]으로 블록 크기는 128 비트이고 키 크기는 128, 192, 256 비트를 지원함. 키 크기에 따른 규격의 차이를 구분할 경우 각각 AES-128, AES-192, AES-256으로 표기

3.1.2 ARIA
국내 전자정부 안전성 강화를 목적으로 개발되어 2004년 KS 표준으로 제정된 블록 암호 알고리즘[13]. AES와 인터페이스가 같고, 키 크기에 따라 각각 ARIA-128, ARIA-192, ARIA-256으로 표기

3.1.3 CTR(CounTeR) 모드
블록 단위로 증가하는 카운터(counter)를 블록 암호 입력값으로 하여 얻어진 연속된 출력값을 평문과 XOR하는 방식으로 암호화를 수행함으로써 기밀성을 제공하는 블록 암호 운영 모드

3.1.4 GCM(Galois/Counter Mode)
CTR 모드와 유한체 곱셈으로 정의된 인증 태그(authentication tag) 계산 함수를 조합하여 설계된 인증 암호화 운영 모드

3.1.5 HMAC(Keyed-Hash Message Authentication Code)
해시 함수 기반 메시지 인증 코드 알고리즘

3.1.6 SHA(Secure Hash Algorithm)
미국 연방정부 표준 해시 함수로, 이 표준에서는 160 비트 출력값을 가지는 SHA-1만 고려

3.1.7 메시지 인증 코드(MAC, Message Authentication Code)
임의 길이 메시지와 비밀키로부터 생성되는 고정 길이의 인증 태그(authentication tag)를 검증함으로써 메시지의 위변조 여부를 판단할 수 있는 암호 알고리즘

3.1.8 블록 암호(block cipher)
비밀키를 이용하여 고정된 길이의 데이터 블록을 암호화하거나 복호화하는 알고리즘

3.1.9 인증 암호화 운영 모드(AEAD, Authenticated Encryption with Associated Data)
기밀성과 무결성을 동시에 제공하며, 특히 데이터의 일부분에 대해서는 암호화하지 않고 무결성만 보장하는 것을 허용하는 블록 암호 운영 모드

3.1.10 충돌쌍 공격(collision attack)
같은 출력값을 가지는 서로 다른 두 개의 입력 데이터를 찾는 공격

3.1.11 해시 함수(hash function)
임의 길이의 메시지를 일정 길이의 출력값으로 압축하는 알고리즘

3.2 네트워크 프로토콜 용어

3.2.1 IP 보안(IPsec, Internet Protocol Security) 프로토콜

망 계층(network layer)인 인터넷 프로토콜(IP) 계층에서 패킷 단위 암호화 및 메시지 인증을 통해 정보보호 서비스를 제공하는 프로토콜

3.2.2 S/MIME(Secure/Multipurpose Internet Mail Extensions)

전자 우편을 통해 다양한 종류의 데이터를 전송하기 위해 만들어진 멀티미디어 전자 우편 프로토콜 MIME(Multi-purpose Internet Mail Extensions)을 확장하여, 전자 우편에 기밀성과 인증, 그리고 부인 방지 등의 정보보호 서비스를 제공하는 프로토콜

3.2.3 SRTP의 키 관리를 위한 데이터그램 전송 계층 보안 확장(DTLS-SRTP, DTLS extension to establish keys for SRTP)

데이터그램 전송 계층 보안(DTLS, Datagram Transport Layer Security)의 핸드쉐이크(handshake) 프로토콜을 기반으로, SRTP의 암호키 관리와 함께 주요 암호 알고리즘과 파라미터 협상을 지원하는 키 관리 프로토콜

3.2.4 멀티미디어 인터넷 키 관리 방식(MIKEY, Multimedia Internet KEYing)

SRTP와 같은 실시간 멀티미디어 보안 프로토콜의 암호키 관리를 지원하는 일-대-다(one-to-many) 또는 작은 규모의 상호 작용형 그룹에 적합한 키 관리 프로토콜

3.2.5 실시간 전송 프로토콜(RTP, Real-time Transport Protocol)

인터넷상의 오디오와 비디오 같은 멀티미디어 데이터를 실시간으로 전송하기 위해 설계된 패킷 구조와 운영 규격을 정의한 프로토콜

3.2.6 세션(session)

망 환경에서 사용자 사이 또는 컴퓨터 사이의 대화를 위한 논리적 연결

3.2.7 세션 기술 프로토콜(SDP, Session Description Protocol)

멀티미디어 통신에 있어 세션 개시, 초대, 시작 등 세션 운영 전반에 대한 규격을 명시한 프로토콜

3.2.8 안전한 실시간 전송 프로토콜(SRTP, Secure RTP)

실시간 전송 프로토콜에서 정의한 RTP/RTCP 패킷을 대상으로 암호화, 메시지 인증, 재전송 공격 방어 등의 기법을 적용하여, 실시간 전송 멀티미디어 데이터에 대한 정보보호 서비스를 제공하는 프로토콜

3.2.9 인터넷 할당 번호 관리 기관(IANA, Internet Assigned Numbers Authority)

IETF의 RFC로 발간되는 각종 인터넷 프로토콜의 고유 매개변수들과 프로토콜 파라미터를

관리하는 기관 (http://www.iana.org)

3.2.10 전송 계층 보안(TLS, Transport Layer Security) 프로토콜

TCP/IP 계층의 서버-클라이언트 통신에 대한 정보보호 서비스를 제공하는 프로토콜로, 크게 cipher suite와 키 교환 및 사용자 인증을 수행하는 핸드쉐이크 단계(handshake layer)와 데이터 암호화 및 메시지 인증을 수행하는 레코드 단계(record layer)로 구성

4 약어

ARIA_128_CTR	ARIA-128 in Counter Mode
ARIA_256_CTR	ARIA-256 in Counter Mode
ARIA_128_GCM	ARIA-128 in Galois/Counter Mode
ARIA_256_GCM	ARIA-256 in Galois/Counter Mode
ARIA-CTR	ARIA in Counter Mode
ARIA-GCM	ARIA in Galois/Counter Mode
CCM	Counter with CBC-MAC(Cipher Block Chaining MAC)
HMAC-SHA1	HMAC based on SHA-1
IETF	Internet Engineering Task Force
PRF	Pseudo-Random Function
RTCP	RTP Control Protocol
SDES	SDP Security Descriptions
SRTCP	Secure RTCP
XOR	eXclusive OR

5 암호 알고리즘

5.1 기밀성 알고리즘(cryptographic transform)

SRTP 권고 블록 암호 알고리즘인 AES와 국내 블록 암호 표준 알고리즘인 ARIA는 키와 블록 크기, 그리고 운영 모드 사용 방법이 같고, ARIA의 SRTP 적용에 대한 특이한 제약 사항이 존재하지 않는다. 따라서 ARIA는 AES와 같은 방법[2,7,11]으로 SRTP에 적용할 수 있다. SRTP에서 ARIA는 두 가지 운영 모드(CTR, GCM)의 기반 함수로 사용되어, RTP/RTCP 패킷 암호화에 적용될 수 있다.

5.1.1 ARIA-CTR

AES-128을 CTR 모드의 기반 블록 암호로 사용하여 SRTP의 RTP/RTCP 패킷 암호화에 적용하는 방법은 [2]에 정의되어 있으며, AES-256의 경우는 [7]에 정의되어 있다.

ARIA를 CTR 모드의 기반 블록 암호로 사용(ARIA-CTR)하여 SRTP의 패킷 암호화에 적용하는 방법은 AES의 경우(AES-CTR)와 같으며, 키 크기에 따라 각각 ARIA_128_CTR과 ARIA_256_CTR로 구분한다. AES-CTR과 ARIA-CTR의 유일한 차이점은 CTR 모드의 기반 블록 암호로 각각 AES와 ARIA를 사용하는 것이다.

기밀성 운영 모드인 CTR을 사용할 경우, 패킷 무결성 보장을 위해 별도의 인증 알고리즘을 같이 사용해야 한다. SRTP는 160 비트 키를 사용하는 HMAC-SHA1을 필수 구현 인증 알고리즘으로 제시하고 있으며[2], 6절에서 제시하는 ARIA-CTR 기반 crypto suite는 HMAC-SHA1을 인증 알고리즘으로 사용한다.

RTP 패킷의 헤더 확장(header extension)에 대한 기밀성 제공을 위해, [10]에서는 AES-CTR로 암호화하는 방법을 정의하고 있다. SRTP의 RTP 패킷 페이로드 암호화에 ARIA-CTR을 적용하는 경우, 헤더 확장 보호를 위해서도 ARIA-CTR을 적용하며 그 방법은 [10]에 정의된 방법을 준용한다.

5.1.2 ARIA-GCM

AES를 GCM[5]의 기반 블록 암호로 사용하여 SRTP의 RTP/RTCP 패킷 암호화에 적용하는 방법은 [11]에 정의되어 있다. ARIA를 GCM의 기반 블록 암호로 사용(ARIA-GCM)하여 SRTP의 패킷 암호화에 적용하는 방법은 AES의 경우(AES-GCM)와 같다. AES-GCM과 ARIA-GCM의 유일한 차이점은 기반 블록 암호로 각각 AES와 ARIA를 사용하는 것이다.

SRTP의 RTP 패킷 암호화에 AES-GCM을 적용하면서 헤더 확장에 대한 기밀성 제공이 필요한 경우, 헤더 확장 암호화에는 AES-CTR을 적용한다[11]. 패킷 암호화에 ARIA-GCM을 적용하는 경우, 헤더 확장 암호화에는 ARIA-CTR을 적용하며 그 방법은 [10,11]에 정의된 방법을 준용한다.

5.2 키 유도 함수(key derivation function)

특정 세션에서 암호 알고리즘에 사용될 세션키를 마스터 비밀키와 솔트(salt)키로부터 유도하기 위해, [2]의 4.3.3절에서는 AES-128을 CTR 모드로 운용하는 키 유도 함수를 정의하고 이를 AES-CM PRF로 표기하였다. AES-256의 SRTP 적용 방법을 정의한 [7]에서는 AES-256을 CTR 모드로 운용하는 키 유도 함수를 정의하고 이를 AES_256_CM_PRF로 표기하였다.

ARIA를 사용하는 키 유도 함수(ARIA-CTR PRF)는 AES의 경우와 같게 정의하며, 키 크기에 따라 각각 ARIA_128_CTR_PRF와 ARIA_256_CTR_PRF로 표기한다. [7]과 [11]에 제시된 AES-CM PRF의 사용 요구조건은 ARIA-CTR PRF에도 같게 적용된다.

6 Crypto suites

SRTP의 기본 키 관리 방식인 SDES[4]는 암호 알고리즘 적용과 관련한 주요 파라미터 설정을 한데 묶어 SRTP crypto suite로 정의하여, 세션 참여자들이 암호 알고리즘 협상 과정에 사용할 수 있도록 하였다.

SRTP crypto suite는 기밀성 운영 모드를 사용하는 경우에는

블록 암호_키 크기_운영 모드_메시지 인증_인증 태그 길이

로 표기하고, 인증 암호화 운영 모드(AEAD)를 사용하는 경우에는

AEAD_블록 암호_키 크기_운영 모드_인증 태그 길이

로 표기한다. 예를 들어, ARIA_128_CTR_HMAC_SHA1_80은 패킷 암호화를 위해 128 비트 키의 ARIA-CTR을 적용하고, 패킷 무결성 보장을 위해 HMAC-SHA1을 적용하며 이때 인증 태그의 길이는 80 비트인 것을 의미한다.

기밀성 알고리즘으로 ARIA-CTR을 사용하는 crypto suite를 정리하면 <표 6-1>과 같다.

<표 6-1> ARIA-CTR crypto suite (단위: 바이트)

번호	Crypto suite	키 크기		인증 태그 길이
		블록 암호	HMAC	
1	ARIA_128_CTR_HMAC_SHA1_80	16	20	10
2	ARIA_128_CTR_HMAC_SHA1_32	16	20	4
3	ARIA_256_CTR_HMAC_SHA1_80	32	20	10
4	ARIA_256_CTR_HMAC_SHA1_32	32	20	4

<표 6-1>의 각 crypto suite에 대응하는 파라미터 설정은 <표 6-2><표 6-3><표 6-4><표 6-5>와 같다. 이들 파라미터 설정은 SDES의 속성값(attribute)으로 사용된다.

<표 6-2> ARIA_128_CTR_HMAC_SHA1_80 파라미터

파라미터	값
Master key length	128 비트
Master salt length	112 비트
Key Derivation Function	ARIA_128_CTR PRF
Maximum key lifetime (SRTP)	2^{48} 패킷
Maximum key lifetime (SRTCP)	2^{31} 패킷
Cipher (for SRTP and SRTCP)	ARIA_128_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 비트
SRTP authentication tag length	80 비트
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 비트
SRTCP authentication tag length	80 비트

<표 6-3> ARIA_128_CTR_HMAC_SHA1_32 파라미터

파라미터	값
Master key length	128 비트
Master salt length	112 비트
Key Derivation Function	ARIA_128_CTR_PRF
Maximum key lifetime (SRTP)	2^{48} 패킷
Maximum key lifetime (SRTCP)	2^{31} 패킷
Cipher (for SRTP and SRTCP)	ARIA_128_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 비트
SRTP authentication tag length	32 비트
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 비트
SRTCP authentication tag length	80 비트

<표 6-4> ARIA_256_CTR_HMAC_SHA1_80 파라미터

파라미터	값
Master key length	256 비트
Master salt length	112 비트
Key Derivation Function	ARIA_256_CTR_PRF
Maximum key lifetime (SRTP)	2^{48} 패킷
Maximum key lifetime (SRTCP)	2^{31} 패킷
Cipher (for SRTP and SRTCP)	ARIA_256_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 비트
SRTP authentication tag length	80 비트
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 비트
SRTCP authentication tag length	80 비트

<표 6-5> ARIA_256_CTR_HMAC_SHA1_32 파라미터

파라미터	값
Master key length	256 비트
Master salt length	112 비트
Key Derivation Function	ARIA_256_CTR_PRF
Maximum key lifetime (SRTP)	2^{48} 패킷
Maximum key lifetime (SRTCP)	2^{31} 패킷
Cipher (for SRTP and SRTCP)	ARIA_256_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 비트
SRTP authentication tag length	32 비트
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 비트
SRTCP authentication tag length	80 비트

기밀성 알고리즘으로 ARIA-GCM을 사용하는 crypto suite를 정리하면 <표 6-6>과 같다.

<표 6-6> ARIA-GCM crypto suite (단위: 바이트)

번호	Crypto suite	블록 암호 키 크기	인증 태그 길이
1	AEAD_ARIA_128_GCM	16	16
2	AEAD_ARIA_256_GCM	32	16

ARIA-GCM을 기밀성 알고리즘으로 사용하는 경우 자체적으로 인증 태그를 생성하기 때문에, 관련 crypto suite는 별도의 인증 알고리즘을 포함하지 않는다. 그리고 인증 암호화 운영 모드를 사용할 경우 인증 태그는 절삭하지 않고 128 비트로 사용한다.

<표 6-6>의 각 crypto suite에 대응하는 파라미터 설정은 <표 6-7><표 6-8>과 같다.

<표 6-7> AEAD_ARIA_128_GCM 파라미터

파라미터	값
Master key length	128 비트
Master salt length	96 비트
Key Derivation Function	ARIA_128_CTR_PRF
Maximum key lifetime (SRTP)	2^{48} 패킷
Maximum key lifetime (SRTCP)	2^{31} 패킷
Cipher (for SRTP and SRTCP)	ARIA_128_GCM
AEAD authentication tag length	128 비트

<표 6-8> AEAD_ARIA_256_GCM 파라미터

파라미터	값
Master key length	256 비트
Master salt length	96 비트
Key Derivation Function	ARIA_256_CTR_PRF
Maximum key lifetime (SRTP)	2^{48} 패킷
Maximum key lifetime (SRTCP)	2^{31} 패킷
Cipher (for SRTP and SRTCP)	ARIA_256_GCM
AEAD authentication tag length	128 비트

ARIA 기반의 SRTP crypto suite(<표 6-1>,<표 6-6>)에서 키 유도 함수는 기밀성 알고리즘과 같은 키 크기를 사용하는 ARIA-CTR PRF로 정의한다.

7 필수 crypto suite

SRTP에서는 필수 crypto suite로 AES_CM_128_HMAC_SHA1_80을 지정하여, 호환이 필요한 응용 환경에서 반드시 구현하도록 권고하고 있다. 그러나 국내의 경우 국가 표준 블록 암호 알고리즘인 ARIA의 우선 적용이 필요한 환경이 있음을 고려하여, 국내 보안 제품 사이의 기본적인 호환성을 보장하기 위한 별도의 필수 crypto suite를 다음과 같이 제시한다.

ARIA_128_CTR_HMAC_SHA1_80

8 안전성 고려 사항

이 표준은 80 비트보다 짧은 길이의 인증 태그를 사용하는 SRTP crypto suite를 포함하고 있다. 이들은 [2]에 제시된 예와 같이 인증 태그 길이의 제한이 불가피한 환경에 한정하여 사용될 수 있지만, 그 이외의 경우에는 안전성 수준을 저하시키는 요소이므로 사용을 허용하지 않는다.

SRTP는 현재 HMAC-SHA1을 필수 구현 인증 알고리즘으로 권고하고 있으며, 기밀성 운영 모드를 사용하는 SRTP crypto suite는 모두 HMAC-SHA1을 사용하고 있다. 충돌쌍 공격 관점에서 SHA-1의 취약성이 알려짐에 따라, IETF를 비롯한 국제 표준 기구나 국내 암호 모듈 검증제도 등에서는 SHA-1을 배제하고 SHA-2나 SHA-3와 같은 안전한 해시 함수의 사용을 권고하고 있다[9]. 그러나 SRTP의 경우 SHA-1이 HMAC의 기반 함수로만 사용되고 있으며, 이러한 용도에 있어 SHA-1의 취약성은 아직 알려진 바 없다.

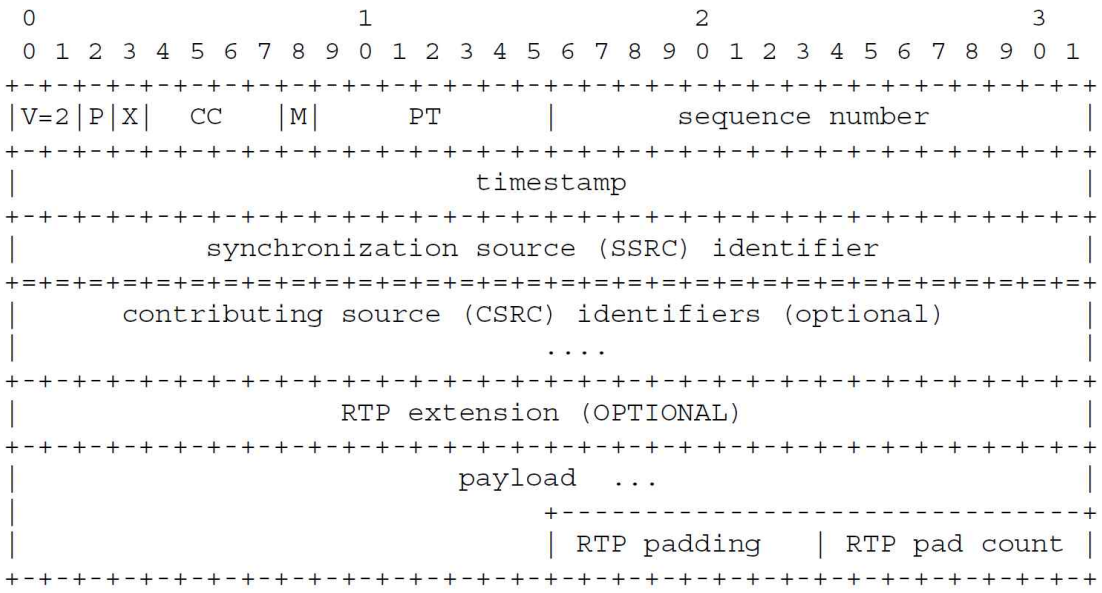
SRTP의 키 관리 방식으로 SDES를 사용할 경우, 암호 속성 보호를 위한 SDES 자체 방법이 정의되어 있지 않기 때문에 (D)TLS, IPsec, S/MIME 등 별도의 보안 프로토콜을 함께 사용해야 한다[4].

부 록 Ⅰ

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

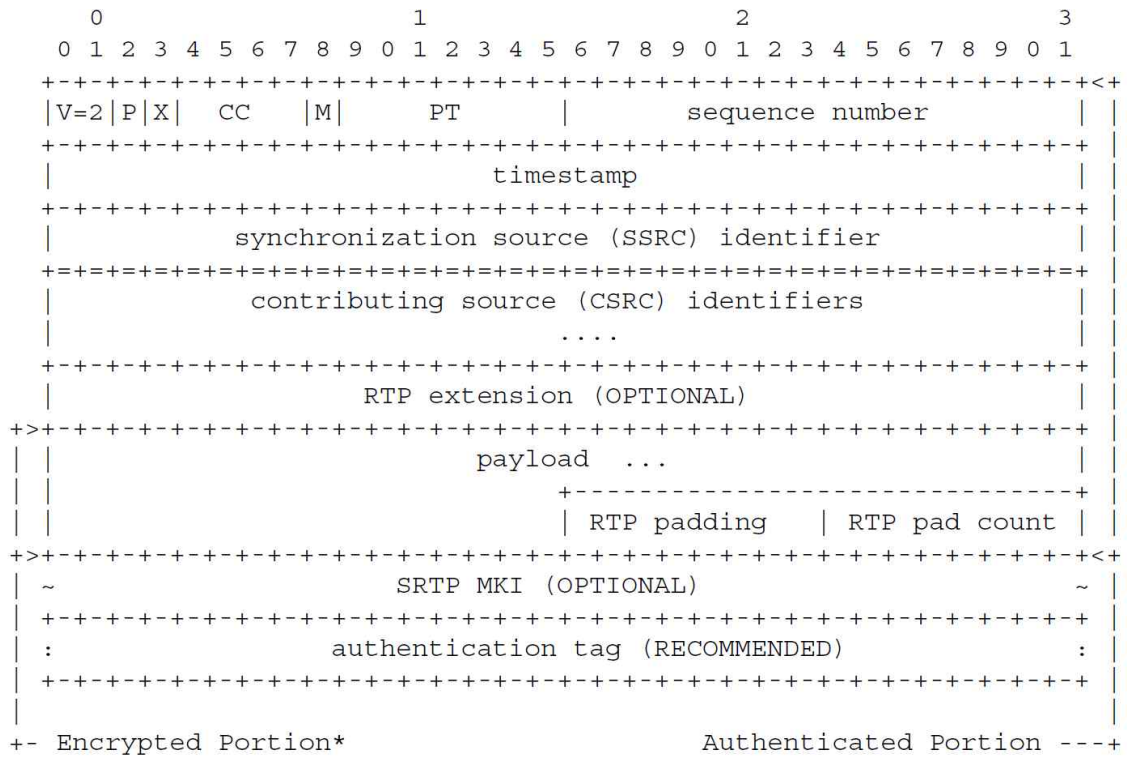
SRTP와 키 관리 방식

실시간 전송 프로토콜[1]은 VoIP(Voice over IP), 멀티미디어 원격회의(multimedia conferencing), IPTV(Internet Television)를 포함하는 다양한 멀티미디어 응용에 사용되고 있다. 실시간 전송 프로토콜에서는 두 가지 세부 프로토콜인 RTP와 RTCP를 정의하고 있다. 데이터 전송 프로토콜인 RTP는 실시간 데이터의 전송에 활용되며, 동기화를 위한 타임 스템프, 패킷 손실과 재배열 검출을 위한 순서 정보, 그리고 데이터의 인코딩 정보 등을 포함하는 패킷 구조를 정의한다. 제어 프로토콜인 RTCP는 RTP 세션의 품질 제어 정보를 세션 참여자들이 교환하기 위한 패킷 구조를 정의한다. 참고로 RTP 패킷 구조는 <그림 Ⅰ-1>과 같다.

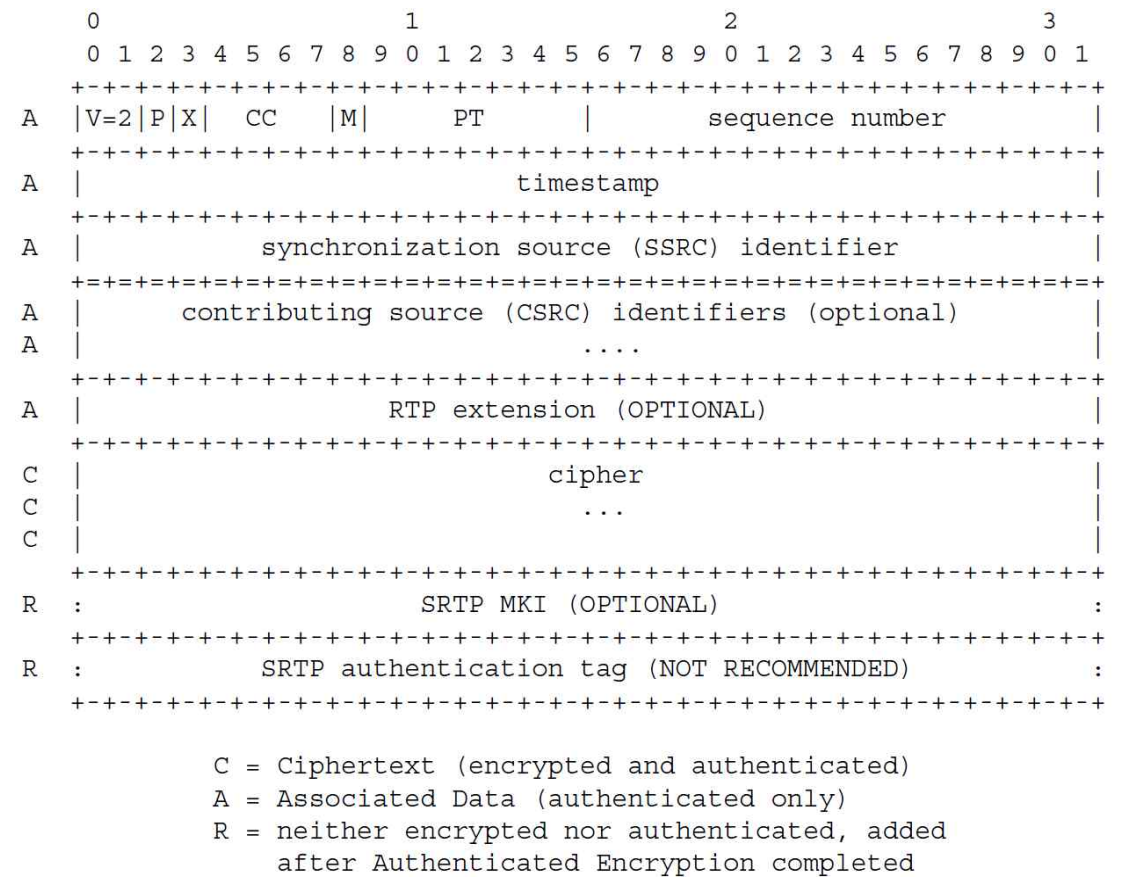


(그림 Ⅰ-1) RTP 패킷 구조(출처: [11])

SRTP[2]는 실시간 전송 프로토콜에 요구되는 다양한 보안 요구조건을 충족시킬 수 있도록 설계된 프로토콜로, 실시간 전송 프로토콜에서 정의하는 RTP와 RTCP 트래픽에 대한 기밀성(confidentiality), 무결성(integrity), 근원 인증(source authentication), 그리고 재전송 방지(replay protection) 서비스를 제공한다. 안전한 실시간 전송 프로토콜에서는 RTP/RTCP 패킷 전체에 대한 무결성을 보장하고, 특히 페이로드에 대해서는 기밀성까지 보장할 수 있도록 설계되었다[2]. 참고로 SRTP에 적용하는 기밀성 알고리즘의 특성(블록 암호 운영 모드)에 따라, (그림 Ⅰ-1)에 도시한 RTP 패킷에 대응하는 SRTP 패킷 구조는 각각 (그림 Ⅰ-2), (그림 Ⅰ-3)과 같다.



(그림 Ⅰ-2) 기밀성 운영 모드 기반 기밀성 알고리즘을 적용한 SRTP 패킷 구조(출처: [2])



(그림 Ⅰ-3) 인증 암호화 운영 모드 기반 기밀성 알고리즘을 적용한 SRTP 패킷 구조(출처: [11])

이러한 SRTP의 정보보호 서비스는 적용 가능한 여러 가지 기밀성 알고리즘, 인증 알고리즘, 그리고 키 유도 함수를 조합하여 제공한다. <표 Ⅰ-1>은 현재 SRTP에서 지원하는 기밀성 알고리즘을 정리한 것이다.

<표 Ⅰ-1> SRTP가 지원하는 기밀성 알고리즘

운영모드 / 블록암호	CTR	GCM	CCM	f8
AES	○	○	×	○
ARIA	○	○	×	×
SEED	○	○	○	×

SRTP는 블록 암호를 스트림형 운영 모드의 기반 함수로 사용하는 방식으로 기밀성 알고리즘을 정의한다. SRTP의 기밀성 알고리즘으로 현재 사용 가능한 블록 암호는 AES[12], ARIA[13], SEED[16]가 있고, 운영 모드는 CTR, GCM, CCM, f8[15,2]이 있다. 인증 암호화 운영 모드인 CCM과 GCM을 사용하여 기밀성 알고리즘을 구성하는 경우, 암호화 과정에서 인증 태그를 생성하기 때문에 별도의 인증 알고리즘을 사용할 필요가 없다. 반면 기밀성 운영 모드인 CTR과 f8을 사용하는 경우, 패킷 무결성 보장을 위해 160 비트 키를 사용하는 HMAC-SHA1을 같이 사용한다.

이러한 기밀성 알고리즘과 인증 알고리즘을 이용하여 제공 가능한 정보보호 서비스의 안전성은 유일한 비밀 요소인 암호키에 의존한다. SRTP의 기밀성 알고리즘과 인증 알고리즘에 입력 파라미터로 사용되는 암호키는 통신 개체들이 공유한 마스터 비밀키(master secret key)와 마스터 솔트(master salt)로부터 세션 단위로 키 유도 함수를 이용해 생성된다. 이때 암호키는 기밀성 알고리즘에 사용되는 암호화용 키와 솔트, 그리고 인증 알고리즘에 사용되는 인증키로 구분할 수 있으며, 인증 암호화 운영 모드 기반의 기밀성 알고리즘을 사용하는 경우에는 별도의 인증키를 생성하지 않는다. 키 유도 함수를 이용하여 세션 단위로 유도되는 암호키(세션키)의 안전성은 마스터 비밀키의 안전성에 의존한다.

SRTP는 키 유도 함수를 통해 세션키를 생성하는 방법을 정의하고 있지만, 그 입력이 되는 마스터 비밀키와 마스터 솔트의 생성과 공유에 대해서는 다루지 않는다. 그리고 마스터 비밀키와 마스터 솔트의 생성과 공유는 SRTP와는 독립적으로 정의된 키 관리 방식에 의해 SRTP의 세션 초기화 이전에 완료된 것을 가정한다. 현재 SRTP의 키 관리 방식으로 운용 가능한 프로토콜로 SDES[4], DTLS-SRTP[6], MIKEY[3], ZRTP[8] 등이 알려져 있다. 참고로 SRTP에 사용하는 암호 알고리즘은 키 관리 프로토콜 자체 보안을 위한 암호 알고리즘과는 무관하다.

SRTP의 키 관리 방식은 세션키 유도를 위한 마스터 비밀키와 마스터 솔트의 생성과 공

유를 가능하게 하는 것과 함께, SRTP에서 사용하는 암호 알고리즘을 세션 참여자들이 협상하여 결정할 수 있도록 한다. SRTP는 기밀성 알고리즘, 인증 알고리즘, 그리고 키 유도 함수를 개별적으로 정의하여 사용할 수 있도록 하여 사용자들에게 암호 알고리즘 적용에 대한 유연성과 확장성을 주는 반면, 사용자는 개별 암호 알고리즘에 대한 많은 정보가 필요하게 된다. 이러한 사용자의 부담을 줄이기 위해, SDES와 DTLS-SRTP는 사전에 개별 암호 알고리즘과 관련 주요 파라미터 설정을 한데 묶어 각각 “SRTP crypto suite”와 “SRTP 보호 프로파일”이라는 이름으로 사용한다. SRTP crypto suite와 SRTP 보호 프로파일은 암호 알고리즘의 SRTP 적용을 좀 더 쉽게 만드는 반면 SRTP가 가지는 유연성을 저하시키는 요인이 된다. SDES나 DTLS-SRTP와는 다르게, MIKEY는 개별 암호 알고리즘을 선택할 수 있도록 하여 SDES와 DTLS-SRTP에 비해 상대적으로 높은 유연성을 제공한다.

이 표준에서는 블록 암호 ARIA를 이용하여 정의된 SDES의 SRTP crypto suite를 <표 6-1>과 <표 6-6>에 제시하고 있다. SRTP crypto suite의 구성에서 알 수 있듯이, SRTP crypto suite는 주요 암호 알고리즘의 조합뿐만 아니라 마스터 비밀키와 마스터 솔트의 크기, 인증 태그의 길이, 고정된 마스터 비밀키에 대해 허용 가능한 RTP/RTCP 패킷 개수 등 다양한 파라미터를 설정하고 있다. 블록 암호 ARIA를 이용하여 정의된 SRTP crypto suite는 SRTP 보호 프로파일과 일대일로 대응하며, DTLS-SRTP의 경우 개별 SRTP 보호 프로파일을 식별하기 위한 식별값을 IANA로부터 부여받아 사용하는 특징을 가진다. MIKEY의 경우 기밀성 알고리즘과 인증 알고리즘, 그리고 키 유도 함수 각각에 대한 식별값을 IANA로부터 부여받아 협상 과정에서 사용할 수 있도록 하고 있다.

부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

※ 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

II-2.1 시험인증 대상 여부

해당 사항 없음

II-2.2 시험표준 제정 현황

해당 사항 없음

부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

II-3.1 TTAK.KO-12.0201/R1

이 표준에서 정의한 ARIA의 SRTP 적용 방법을 실제 사용자들이 공유하기 위해서는 키 관리 방식을 이용한 협상이 선행되어야 한다. TTAK.KO-12.0201/R1은 MIKEY[3]를 SRTP의 키 관리 방식으로 사용할 경우, ARIA의 SRTP 적용에 대한 협상에 필요한 보안 파라미터 설정을 제시하고 있다.

II-3.2 TTAK.KO-12.0202/R1

DTLS-SRTP[6]를 SRTP의 키 관리 방식으로 사용할 경우, ARIA의 SRTP 적용에 대한 협상에 필요한 보호 프로파일(protection profile) 정의와 식별값은 TTAK.KO-12.0202/R1에 제시되어 있다. 이 표준에서 제시하는 SRTP crypto suite와 DTLS-SRTP의 ARIA 기반 보호 프로파일은 일대일로 대응한다.

부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] IETF RFC 3550, “RTP: A Transport Protocol for Real-time Applications”, 2003.
[2] IETF RFC 3711, “The Secure Real-time Transport Protocol (SRTP)”, 2004.
[3] IETF RFC 3830, “MIKEY: Multimedia Internet KEYing”, 2004.
[4] IETF RFC 4568, “Session Description Protocol (SDP) Security Descriptions for Media Streams”, 2006.
[5] IETF RFC 5116, “An Interface and Algorithms for Authenticated Encryption”, 2008.
[6] IETF RFC 5764, “Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)”, 2010.
[7] IETF RFC 6188, “The Use of AES-192 and AES-256 in Secure RTP”, 2011.
[8] IETF RFC 6189, “ZRTP: Media Path Key Agreement for Unicast Secure RTP”, 2011.
[9] IETF RFC 6194, “Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms”, 2011.
[10] IETF RFC 6904, “Encryption of Header Extensions in the Secure Real-time Transport Protocol (SRTP)”, 2013.
[11] IETF RFC 7714, “AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)”, 2015.
[12] NIST FIPS 197, “Advanced Encryption Standard (AES)”, 2001.
[13] KS, KS X 1213-1, “128비트 블록 암호 알고리즘 ARIA - 제1부: 일반”.
[14] KS, KS X 1213-2, “128비트 블록 암호 알고리즘 ARIA - 제2부: 운용 모드”.
[15] KS, KS X 3254, “n비트 블록 암호 운영 모드 - 제1부 일반”.
[16] TTA, TTAS.KO-12.004/R1, “128비트 블록 암호 알고리즘 SEED”, 2005.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2009.12.22	제정 TTAK.KO-12.0115	-	사이버보안 PG (PG503)
제2판	2011.12.21	개정 TTAK.KO-12.0115/R1	SRTP crypto suite 목록 조정	사이버보안 PG (PG503)
제3판	2018.12.xx	개정 TTAK.KO-12.0115/R2	1. 영문 대응표준(IETF RFC 8269)을 반영하여, ①ARIA-192, CCM 모드 사용 배제 ②GCM 인증 태그 길이 128 비트 고정 ③SDES의 SRTP crypto suite 목록을 DTLS-SRTP 보호 프로파일 목록에 맞춰 조정 2. 표준명 변경	사이버보안 PG (PG503)