TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.0201/R1

개정일: 2018년 12월 xx일

SRTP에서 ARIA 알고리즘 사용을 위한 MIKEY 파라미터 정의

MIKEY Parameters for 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-12.0201/R1
표준 초안 작성자	박제홍	NSR	책임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.0201/R1
	김우환	NSR	책임연구원	-	TTAK.KO-12.0201/R1
	권대성	NSR	책임연구원	-	TTAK.KO-12.0201
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.xx

서 문

1 표준의 목적

이 표준의 목적은 안전한 실시간 전송 프로토콜(SRTP, Secure RTP)의 키 관리 방식으로 MIKEY(Multimedia Internet KEYing) 프로토콜을 사용할 때, 블록 암호 ARIA의 SRTP 적용을 세션 참여자들이 협상하는 과정에서 필요한 주요 파라미터와 식별값(identifier)을 제시하여 SRTP에서 ARIA 사용에 대해 상호 운용성(interoperability)을 확보하는 것이다.

2 주요 내용 요약

이 표준은 MIKEY 프로토콜을 통해 블록 암호 ARIA의 SRTP 적용을 세션 참여자들이 협상하는 과정에서 필요한 MIKEY 보안 정책 페이로드(Security policy payload)의 SRTP 정책(SRTP policy) 파라미터와 식별값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에서 제시하는 SRTP 정책(SRTP policy) 파라미터는 기밀성 알고리즘과 키 유도 함수이며, 이는 ARIA를 SRTP에서 사용하기 위한 규격(TTAK.KO-12.0115/R2)을 기반으로 설정된 것이다. 그리고 SRTP 정책 파라미터 식별값은 상호 운용성을 보장하기 위해 IETF RFC 8269에 제시된 IANA의 할당값을 준용한다.

3.2 인용 표준과 본 표준의 비교표

해당 사항 없음

Preface

1 Purpose

The standard provides interoperability with the use of ARIA in SRTP by presenting the security parameters and corresponding identifiers necessary for negotiating ARIA use in SRTP when applying MIKEY as a SRTP's key management mechanism.

2 Summary

The standard defines SRTP policy parameters of MIKEY security policy payload that set the security parameters and options for using ARIA in SRTP, and provides corresponding identifiers to be used for negotiating the use of ARIA in SRTP via MIKEY.

3 Relationship to Reference Standards

The main SRTP policy parameters defined in this standard are encryption algorithm and key derivation function, and both are based on the specification of the use of ARIA in SRTP defined in TTAK.KO-12.0115/R2. And the identifiers of the corresponding SRTP policy parameters conform to the IANA's assigned values set forth in IETF RFC 8269 to ensure interoperability.

목 차

SRTP에서 ARIA 알고리즘 사용을 위한 MIKEY 파라미터 정의 (MIKEY Parameters for 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 세션 참여자들이 마스터 비밀키와 솔트(salt)키를 공유하고 있다고 가정한 상태에서 키 유도 함수를 이용하여 특정 세션에서 암호 알고리즘 동작에 직접 사용되는 암호키(세션키)를 유도하는 방식만 정의하고 있다. 이때 SRTP에서 사용되는 암호 알고리즘이나 암호키 크기 등은, 운용 환경에서의 다양한 보안 요구 사항에 대응하기 위해 사용자가 변경할 수 있는 선택 요소이다. 이러한 선택 요소들은 키 관리 방식을 통해 세션을 맺는 과정에서 세션 참여자들이 협상을 통해 합의하고 공유하게 된다.

그러나 SRTP는 자체적인 키 관리 방식을 가지고 있지 않기 때문에, SRTP가 보장하는 정보보호 서비스를 제공하기 위해서는 마스터 비밀키 공유와 함께 암호 알고리즘과 관련 파라미터(이하 보안 파라미터) 설정을 세션 참여자들이 협상하는데 사용할 수 있는 별도의 키 관리 프로토콜이 요구된다.

SRTP를 위한 키 관리 방식으로는 SDES[4], DTLS-SRTP[5], 또는 MIKEY[3]가 주로 고려된다. 이들은 SRTP 보안 파라미터 협상 과정을 단순화하기 위해, 주요 SRTP 보안 파라미터의 조합을 사전에 설정하고 이에 대한 식별값(identifier)을 부여하여 관리하고 있다.

MIKEY는 단대단(peer-to-peer), 단순 일대다(simple one-to-many), 그리고 작은 규모의 그룹 통신 환경에서 사용자들이 실시간으로 멀티미디어 데이터를 안전하게 주고받을 수 있도록 암호키 관리 기능을 제공하는 보안 프로토콜이다. MIKEY는 SRTP와 같이 실제 데이터 암호화를 위해 사용되는 보안 프로토콜의 암호키 공유를 가능하게 할 뿐만 아니라, 암호 알고리즘의 선택이나 암호키 크기 등의 협상을 위해 관련 보안 정책 파라미터를 상대방에게 전달할 수 있는 페이로드(Security policy payload)를 별도로 정의하고 있다. 특히 SRTP 사용에 특정한 보안 정책 페이로드 파라미터를 SRTP 정책(SRTP policy) 파라미터로 정의하였다.

따라서 MIKEY를 키 관리 방식으로 사용하는 SRTP에 국내 블록 암호 알고리즘 표준인 ARIA[7,8]를 적용하기 위해서는, SRTP 적용 방법을 정의하는 것과 함께 MIKEY 프로토

콜이 지원하는 SRTP 정책 파라미터를 정의해야 한다.

이 표준에서는 SRTP의 키 관리 방식으로 MIKEY 프로토콜을 사용하는 경우, ARIA의 SRTP 적용에 대한 설정을 세션 참여자들이 공유하기 위해 필요한 SRTP 정책 파라미터를 정의한다. 참고로 이러한 SRTP 정책 파라미터에 기반하여 ARIA를 SRTP에서 사용하는 상세 규격은 [9]에서 별도로 다룬다.

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

2 인용 표준

IETF RFC 8269 (2017), The ARIA Algorithm and Its Use with Secure Real-Time Transport Protocol (SRTP) (5절과 6.1절을 인용함)

3 용어 정의

3.1 암호 알고리즘 용어

3.1.1 ARIA
국내 전자정부 안전성 강화를 목적으로 개발되어 2004년 KS 표준으로 제정된 블록 암호 알고리즘. 미국 연방정부 표준 블록 암호 AES와 인터페이스가 같으며, 키 크기에 따라 각각 ARIA-128, ARIA-192, ARIA-256으로 구분하여 표기

3.1.2 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

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

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

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

3.1.6 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

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

3.1.8 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

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

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

3.2 네트워크 프로토콜 용어

3.2.1 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

3.2.2 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

3.2.3 실시간 전송 프로토콜(RTP, Real-time Transport Protocol)
인터넷상의 오디오와 비디오 같은 멀티미디어 데이터를 실시간으로 전송하기 위해 설계된 패킷 구조와 운영 규격을 정의한 프로토콜

3.2.4 세션(session)
망 환경에서 사용자 사이 또는 컴퓨터 사이의 대화를 위한 논리적 연결

3.2.5 세션 기술 프로토콜(SDP, Session Description Protocol)

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

3.2.6 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

3.2.7 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)

4 약어

ARIA-CTR	ARIA in Counter Mode
ARIA-GCM	ARIA in Galois/Counter Mode
HMAC-SHA-1	HMAC based on SHA-1
IETF	Internet Engineering Task Force
PRF	Pseudo-Random Function
RTCP	RTP Control Protocol
SDES	SDP Security Descriptions

5 SRTP 정책

MIEKY의 보안 정책(security policy)은 키 관리 기능의 제공 대상이 되는 특정 보안 프로토콜의 정책 집합을 규정한다. 특히 SRTP에 대한 MIKEY의 보안 정책을 특정하여 SRTP 정책(SRTP policy)이라 하며, 여기에는 SRTP의 운용과 관련한 각종 파라미터를 포함하고 있다. ARIA 사용과 관련된 파라미터로는 암호화 알고리즘(Encryption algorithm, Type 0)과 키 유도 함수(SRTP pseudo random function, Type 5)가 있으며, 이들은 [2]에서 정의한 ARIA의 SRTP 적용 방법에 대응한다. 참고로 [2]에서는 암호화 알고리즘과 동일한 의미를 가지는 용어로 “기밀성 알고리즘”을 사용한다.

SRTP에 사용되는 암호 알고리즘과 관련 파라미터를 MIKEY를 통해 협상하기 위해서는 SRTP 정책의 암호화 알고리즘(Encryption algorithm, Type 0) 파라미터가 정의되어 있어야 한다. <표 5-1>에서는 암호화 알고리즘 파라미터에 추가된 ARIA 기반의 기밀성 알고리즘과 그에 대한 식별값 및 기본 키 크기를 명시한다. 기본 키 크기는 SRTP 정책의 세

션 암호화 키 크기(Session encr. key length, Type 1) 파라미터를 설정하지 않았을 때 사용하는 값으로 128 비트이며, 높은 안전성 수준이 요구되는 경우 256 비트를 사용할 수 있다.

<표 5-1> SRTP 암호화 알고리즘 파라미터

SRTP 암호화 알고리즘	식별값	기본 키 크기 (단위: 비트)
ARIA-CTR	7	128
ARIA-GCM	8	128

SRTP의 암호화 알고리즘으로 ARIA-CTR을 선택할 경우, SRTP 정책의 인증 알고리즘(Authentication algorithm, Type 2) 파라미터에서 HMAC-SHA-1(식별값 1)을 선택하고 SRTP 정책의 인증 태그 길이(Authentication tag length, Type 11) 파라미터에 설정된 값을 인증 알고리즘 계산값(인증 태그)의 길이로 사용한다. 반면 암호화 알고리즘으로 ARIA-GCM을 선택할 경우, 인증 알고리즘 파라미터는 NULL(식별값 0)을 선택하고 인증 태그의 길이는 SRTP 정책의 AEAD 인증 태그 길이(AEAD authentication tag length, Type 20) 파라미터에 설정된 값을 사용한다.

SRTP의 키 유도 함수를 MIKEY를 통해 협상하기 위해서는 SRTP 정책의 키 유도 함수(SRTP pseudo random function) 파라미터가 정의되어 있어야 한다. <표 5-2>에서는 키 유도 함수 파라미터로 ARIA 기반의 PRF와 그에 대한 식별값을 명시한다.

<표 5-2> SRTP 키 유도 함수 파라미터

SRTP 키 유도 함수	식별값
ARIA-CTR	2

SRTP 암호화 알고리즘의 기반 블록 암호로 ARIA를 사용할 경우 키 유도 함수는 ARIA-CTR을 사용한다. 이때 키 유도 함수에 사용되는 키의 크기는 세션 암호화 키 크기(Session encr. key length) 파라미터(Type 1)에 설정된 값을 사용한다.

6 안전성 고려 사항

SRTP는 인증 태그 길이의 제한이 불가피한 환경을 고려하여 32 비트 인증 태그의 사용을 허용하고 있다. 그러나 80 비트 이하 길이의 인증 태그는 안전성 수준을 저하시키는 요인이므로, [2]에 제시된 예와 같이 불가피한 상황이 아닌 경우에는 사용을 허용하지 않는다.

SRTP는 현재 HMAC-SHA-1을 필수 구현 인증 알고리즘으로 권고하고 있으며, 기밀성 운영 모드를 사용할 경우 HMAC-SHA-1을 같이 사용하고 있다. 충돌쌍 공격 관점에서 SHA-1의 취약성이 알려짐에 따라, IETF를 비롯한 국제 표준 기구나 국내 암호모듈 검증 제도 등에서는 SHA-1을 배제하고 SHA-2나 SHA-3와 같은 안전한 해시 함수의 사용을 권고하고 있다[6]. 그러나 SRTP의 경우 SHA-1이 HMAC의 기반 함수로만 사용되고 있으며, 이러한 용도에 있어 SHA-1의 취약성은 아직 알려진 바 없다.

부 록 Ⅰ-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 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 TTAK.KO-12.0115/R2

이 표준은 ARIA의 SRTP 적용에 대한 협상을 키 관리 방식인 MIKEY를 이용하여 수행할 경우 필요한 보안 파라미터 설정을 정의하고 있다. 이 표준에서 정의한 보안 파라미터 설정에 대응한 ARIA의 SRTP 적용 방법은 TTAK.KO-12.0115/R2에 정의되어 있다.

MIKEY를 비롯하여, SRTP의 키 관리 방식으로 주로 고려되는 프로토콜로는 SDES[4]와 DTLS-SRTP[5]가 있다. SDES를 통한 ARIA의 SRTP 적용에 대한 협상은 SRTP crypto suite를 이용하여 이루어지며, TTAK.KO-12.0115/R2는 이러한 ARIA 기반의 SRTP crypto suite를 제시하고 있다.

Ⅰ-3.2 TTAK.KO-12.0202/R1

DTLS-SRTP[5]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.

부 록 Ⅰ-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 5764, “Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)”, 2010.
[6] IETF RFC 6194, “Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms”, 2011.
[7] KS X 1213-1, “128비트 블록 암호 알고리즘 ARIA - 제1부: 일반”.
[8] KS X 1213-2, “128비트 블록 암호 알고리즘 ARIA - 제2부: 운용 모드”.
[9] TTA TTAK.KO-12.0115/R2, “SRTP에서의 ARIA 알고리즘 운영 방법”, 2018.

※ 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 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2012.12.21	제정 TTAK.KO-12.0201	-	사이버보안 PG (PG503)
제2판	2018.12.xx	개정 TTAK.KO-12.0201/R1	1. 영문 대응표준(IETF RFC 8269)을 반영하여, MIKEY 보안 파라미터 정의 수정 (ARIA-CCM 삭제) 2. 표준명 변경	사이버보안 PG (PG503)