

ARIA SRTP 프로토콜 스택 개발

2010. 09. 15

오픈스택(주)

남재권

WE WISH YOU SUCCESS

사업명	ARIA SRTF 프로토크 스택 개발		
과제유형	일반과제, 자유과제		
사업기간	2010.4.20 ~ 2010.11.19 (7개월)		
과제수행기관	오픈스택(주)		
총괄책임자	성 명	남 재 권	
	소속/직위	오픈스택(주)/대표이사	
사업 비	총사업비	정부지원금	수행기관부담금
	60,000천원	50,000천원	현물 10,000천원

■ 과제의 필요성[1/2]

구 분			구현방법
멀티미디어 트래픽보호	IP 폰 ~ IP 폰	보안프로토콜	SRTP (RFC3711)
		암호화 알고리즘	ARIA(Default) : ARIA_192_HMAC_SHA1_80 AES : AES_CM_128_HMAC_SHA1_80
		키관리 방법	SDES (RFC4568)
		참조 : SRTP Crypto Suite	ARIA_CM_192_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_80

행안부 인터넷 전화 인증 요건

구분	표준화 기구명	분과명	표준내용(표준규격명)	제.개정 년도
국제표준	IETF	Network Working Group	“A Description of the ARIA Encryption Algorithm” (RFC 5794)	2010
국제표준	IETF	AVT	“The ARIA Algorithm and Its Use with the Secure Real-time Transport Protocol(SRTP)” draft-nsri-avt-aria-srtp-00.txt	2010
국제표준	IETF	AVT	“The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP)” (RFC 5669)	2010
국제표준	IETF	AVT	“The Camellia Algorithm and Its Use wiht the Secure Real-time Transport Protocol(SRTP)” draft-avt-kanno-srtp-camellia-01	2010
국제표준	IETF	AVT	“The use of AES-192 and AES-256 in Secure RTP” draft-ietf-avt-srtp-big-aes-03.txt	2010

▣ 과제의 목표

항목	내 용
SRTP	RFC 3711 - The Secure Real-time Transport Protocol (SRTP) 구현
ARIA	SRTP 에서 ARIA Cipher Suite (ARIA_CTR_128_HMAC_SHA1_80) 지원
AES	SRTP 에서 AES Cipher Suite (AES_CM_128_HMAC_SHA1_80) 지원
SEED	SRTP 에서 SEED Cipher Suite (SEED_CTR_128_HMAC_SHA1_80) 지원
Camellia	SRTP 에서 Camellia Cipher Suite (CAMELLIA_CTR_128_HMAC_SHA1_80) 지원
과제 홍보	http://www.openariasrtp.org 통하여 이 프로젝트의 결과물을 전 세계에 홍보
세미나	이 프로젝트를 소개하고 설명하는 세미나를 1회 실시

■ 과제 수행 방법

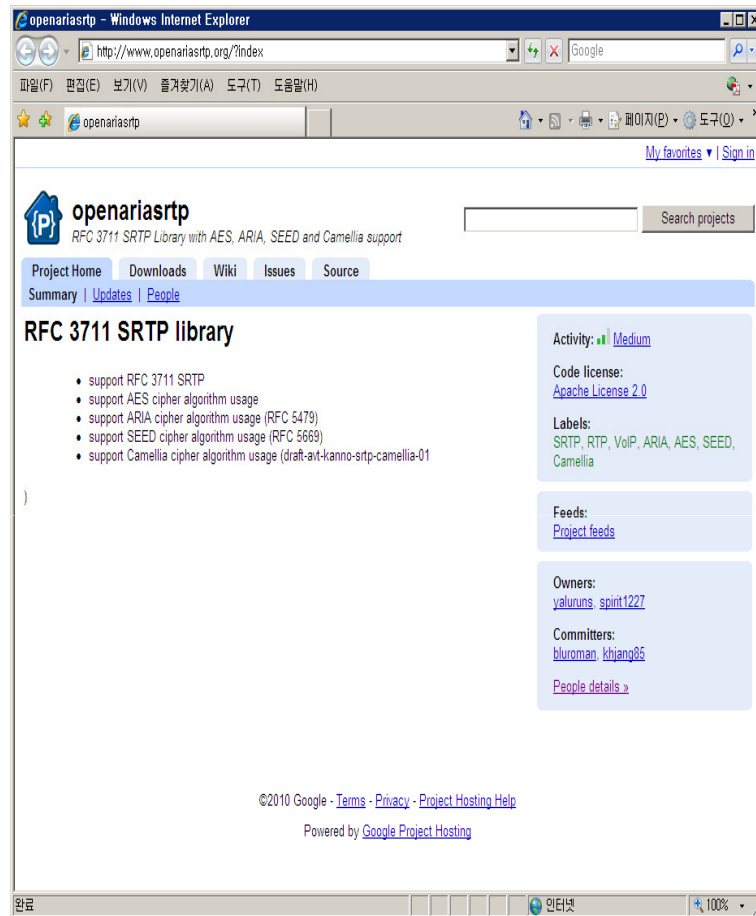
- 오픈스택(주)의 연구원들이 주가 되어서 ARIA, AES, SEED, Camellia SRTP를 ANSI C 기반의 언어로 개발한다.
- <http://www.openariasrtp.org> 홈페이지를 개설하여 ARIA 를 이용한 SRTP에 대한 홍보 및 설명문서 등을 게재
- <http://sourceforge.net> 에 "Open Aria SRTP" 프로젝트를 개설
- sf.net의 SVN을 사용하여 OSS 진영의 개발자들이 누구나 참여할 수 있도록 source code 를 관리
- sf.net 의 mailing list 를 사용하여 개발의 issue 들을 OSS 개발 참여자들 사이에 공유
- ARIA 지원 SRTP 의 검증은 오픈스택(주)의 시제품 VoIP 영상전화기 상에 직접 개발된 과제 결과물을 적용 하여 이를 갖고 KISA, TTA 등을 통하여 공인된 인증을 받도록 한다.
- “Open Aria SRTP”를 사용하여 개발한 VoIP 제조사들이 자신의 단말에 이를 바르게 적용했는지 검증을 돕기 위하여 단말 호환성 검증 서비스를 오픈스택(주)이 실시하거나 혹은 오픈스택(주)의 시제품 VoIP 영상단말기를 단말 제조사들에게 대여하는 서비스를 제공한다.

사업계획	추진실적	달성도(%)
ARIA SRTP 구현	개발 완료 후 단말에 적용 (5월30일)	85
AES SRTP 구현	개발 완료 후 단말에 적용 (6월30일)	85
SEED SRTP 구현	개발 완료 후 단말에 적용 (7월30일)	85
Camellia SRTP 구현	개발 완료 후 단말에 적용 (8월30일)	85
과제홍보	www.openariasrtp.org openariasrtp.sourceforge.net code.google.com/p/openariasrtp	운용중
세미나 개최	2010년 8월20일 코엑스에서 개최	100 %

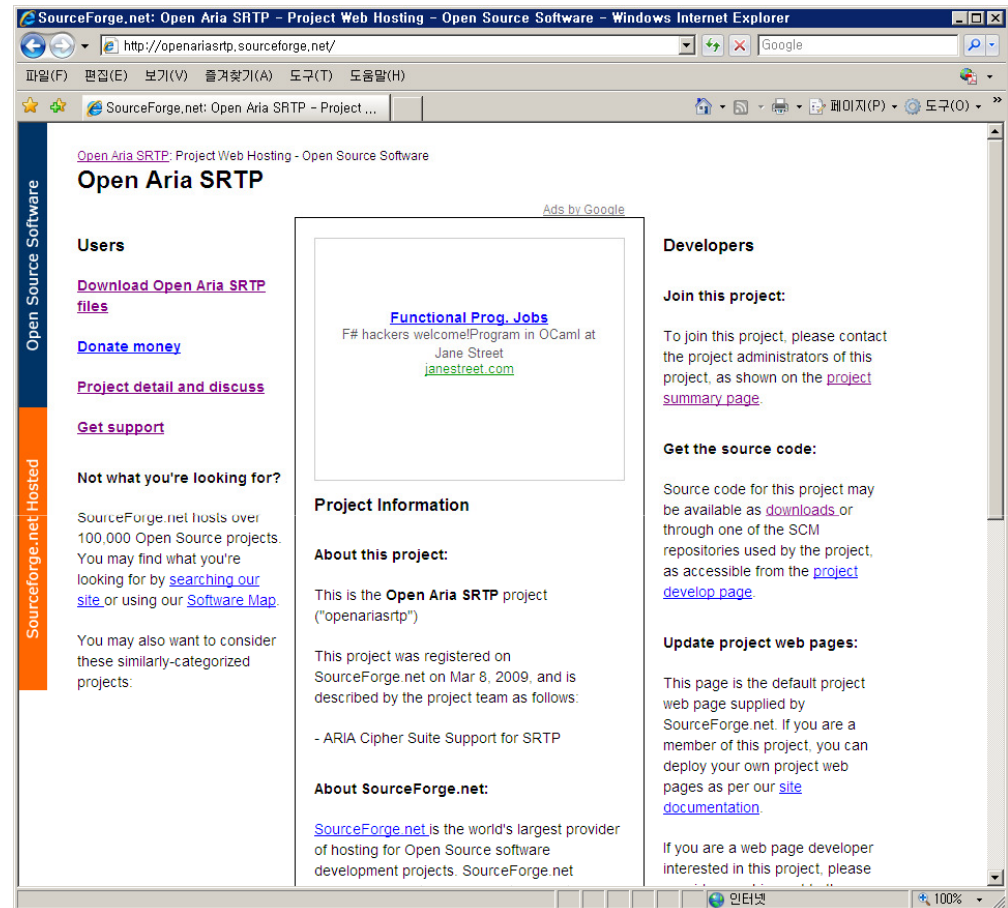
▣ 세부추진내용(1/3) SRTP 구현

- David McGrew 의 libsrtp 1.4.4 에서 시작.
<http://sourceforge.net/projects/srtp> 에서 download 받을 수 있음
- ARIA Source Code:
http://service2.nis.go.kr/pw_certified/aria_open.jsp에서 download 받을 수 있음
- AES ICM 을 참고하여 ARIA ICM 을 추가 구현
- srtp_create(), srtp_dealloc(), srtp_protect(), srtp_unprotect() 를 이용하여 RTP stack 과 붙임
- Open ARIA SRTP 가 <http://sourceforge.net/projects/openariasrtp> 혹은 <http://www.openariasrtp.org> 올려져 있음
- SEED 와 Camellia 에 대해서도 유사한 방식으로 구현

세부추진내용(2/3) 결과물 홍보 확산



www.openariasrtp.org



openariasrtp.sourceforge.net

▣ 세부추진내용(3/3) 세미나 개최

- 2020년 8월20일 10:00 ~ 15:00 코엑스 컨퍼런스룸 308호 B-C
- 국내 VoIP 전문가 40 여명 참석

▪ 세션 내용

Session	강연주제	강사	시간
1	공개SW활성화를 위한 NIPA 역할	NIPA 박성호 책임	10:00~10:50
2	RFC 3711 과 Open ARIA SRTP	오픈스택㈜ 남재권 이사	11:00~11:50
3	VoIP 보안위협 및 보안정책	KISA 윤석웅 선임	13:00~13:50
4	행정기관 인터넷전화 적용 표준 및 인증	TTA 이문길 선임	14:00~14:50

■ 세부추진내용(3/3) 세미나개최 사진(1/3)



▣ 세부추진내용(3/3) 세미나개최 사진(2/3)

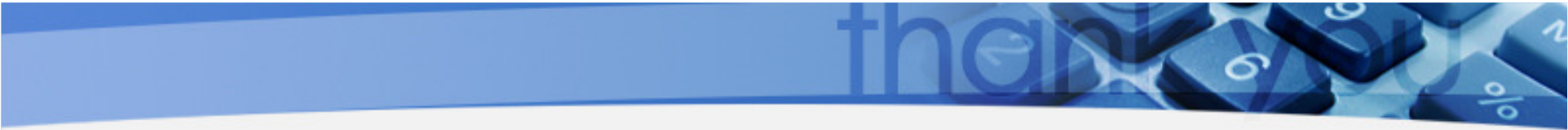


■ 세부추진내용(3/3) 세미나개최 사진(3/3)



□ 향후계획

- www.openariasrtp.org, openariasrtp.sourceforge.net 을 통해서 과제 결과물 홍보에 주력
- Open ARIA SRTP 를 산업계에 컨설팅 추진
(현재 여러 곳의 업체에서 컨설팅 문의, 제휴 문의가 들어오고 있음)



Thank you

We create !

WE WISH YOU SUCCESS

오픈스택 주식회사
경기도 성남시 분당구 야탑동 68번지 첨단기술연구센터 411, 412호
Tel. 031-789-7926 / Fax. 031-789-7925
<http://www.openstack.co.kr>