



안드로이드 기반 데이터 암호화 플랫폼 개발

2011. 05. 26

박석천



경원대학교
KYUNGWON UNIVERSITY

목 차



개발 목표 및 내용

추진체계

커뮤니티 운영체계

개발일정

목 차



개발 목표 및 내용

추진체계

커뮤니티 운영체계

개발일정

과제 개요

- 과제명 : 안드로이드 기반 데이터 암호화 플랫폼 개발
- 과제 수행기간 : 2011.04.25 ~ 2011.11.24
- 과제 유형 : 자유과제
- 개발 책임자
 - 성명 : 박석천
 - 직위 : 정교수
 - 소속 : 경원대학교 컴퓨터공학과

과제 목표 및 내용

● 과제의 필요성

모바일 기기에서의
개인정보 유출 문제

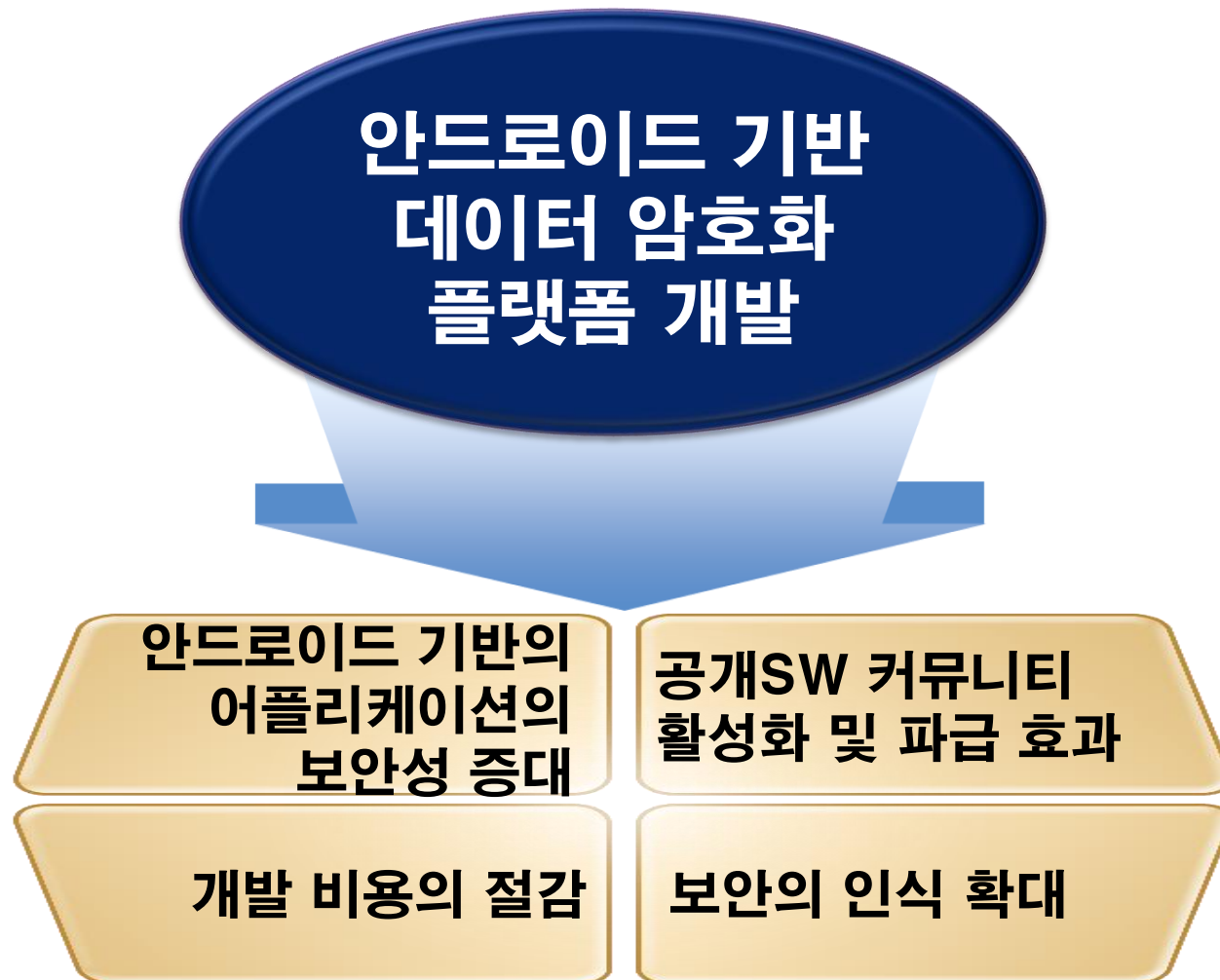
안드로이드 환경의
보안 개발 툴의 부재

공개 SW의 활성화

안드로이드 기반
데이터 암호화
플랫폼 개발

과제 목표 및 내용

● 과제 수행 기대 효과



과제 목표 및 내용

●기 수행 실적

모바일 RFID
서비스를 위한
경량화 보안
모듈 개발

- 시스템별로 보안 알고리즘의 동향 분석
- Mobile RFID에 적용할 수 있는 경량화된 보안 모듈 개발

모바일 RFID
시스템을 위한
암호 알고리즘
최적화 적용 연구
방안

- ECC 암호 알고리즘의 기술적 분석
- RFED 응용 시스템에 적용할 수 있도록 경량화 연구
- 모바일 RFED 네트워크 적용하여 효율성 연구

Embedded SIP
UA System 개발

- 임베디드 환경에서 SIP 기술을 활용한 VoIP 분석

안드로이드 기반
도청장치 모바일
인터넷 전화
개발 SW

- 인터넷 전화 VoIP 분석
- 안드로이드 기반 인터넷 전화 개발
- 경량화된 ECC 알고리즘을 이용한 암호화 기술 개발

과제 목표 및 내용

● 데이터 암호화 플랫폼 개발

안드로이드 기반의 데이터 암호화 플랫폼 요구분석

- 모바일 보안 실태 분석
- 안드로이드 기반 보안 개발 유형 조사 및 분석
- 암호화 알고리즘 분석
- 모바일 환경의 데이터 사용 유형 분석

안드로이드 기반의 데이터 암호화 플랫폼 설계

- 안드로이드 환경의 데이터 암호화 시나리오 설계
- 안드로이드 환경에 적합한 경량화된 암호화 알고리즘 설계
- 안드로이드 기반 데이터 암호화 플랫폼 설계

안드로이드 기반의 데이터 암호화 플랫폼 구현

- 안드로이드 환경의 시나리오별 데이터 암호화 구현
- 안드로이드 기반 데이터 암호화 플랫폼 구현

안드로이드 기반의 데이터 암호화 플랫폼 테스트 및 평가

- 구현된 데이터 암호화 플랫폼 모듈별 단위 테스트
- 구현된 데이터 암호화 통합 테스트
- 구현된 데이터 암호화 플랫폼 평가 및 보완

과제 목표 및 내용

● 과제 개발 내용



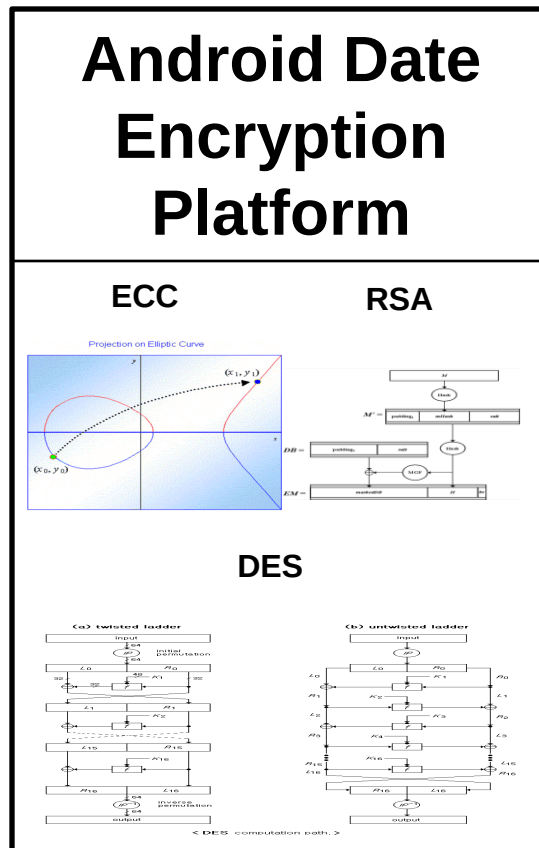
단말저장형 데이터



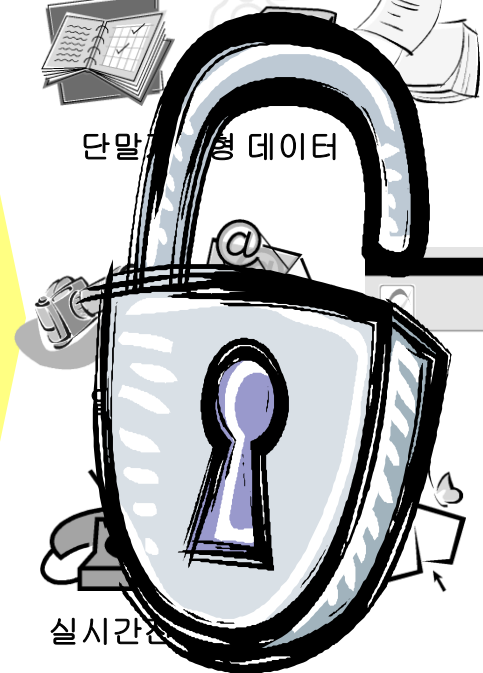
일반전송형 데이터



실시간전송형 데이터



단말저장형 데이터



실시간전

과제 목표 및 내용

● 공개 SW 커뮤니티

공개 SW 커뮤니티 프로젝트 구성

- 초기 커뮤니티 멤버구성
- Sourceforge 커뮤니티 구성
- nForge 커뮤니티 구성
- 전문가 그룹 및 관련 소모임을 통한 멤버 구성

공개 SW 커뮤니티 프로젝트 운영

- 커뮤니티 멤버구성
- 공개 SW 커뮤니티 홍보
- 커뮤니티를 통한 요구사항 및 기능 Feedback
- 커뮤니티를 통한 세미나 및 소모임
- 공개 SW 커뮤니티를 활성화를 위해 국내 · 외 안드로이드 개발 자 모임을 통한 커뮤니티 연계

과제목표 및 내용

● 핵심기술표

순위	핵심기술요소	중요성	난이도	확보여부	
				확보여부 (O,X)	확보방법
1	모바일에 적합한 암호 알고리즘 기술	30	상	O	기존 개발된 암호 알고리즘을 포팅
2	안드로이드 플랫폼 기술	20	중	O	공개 SDK
3	데이터 유형 분석 알고리즘 기술	25	상	X	개발예정
4	암호 알고리즘의 안드로이드 개발 기술	15	중	X	기존 개발된 암호 알고리즘을 포팅
5	시스템 통합	10	중	O	기존 개발된 시스템 통합을 포팅
합계		100			

과제목표 및 내용

● 혁신성과 독창성

모바일 환경의 최적화

- 기존 개발된 암호 관련 API의 단점 보완
- 새로운 암호 알고리즘
(키 생성방식, 키 전달방식, 암호 · 복호화 처리 알고리즘을 연구)
- 모바일에 적합한 경량화된 암호화 플랫폼 개발

최적의 알고리즘 선택을 통한 어플리케이션 개발의 용이함

- 데이터 암호화 개발에 대한 비용과 시간 소모
- 보안 전문가의 필요 최소화
- 보안이 강화된 어플리케이션 개발 용이

목 차



개발 목표 및 내용

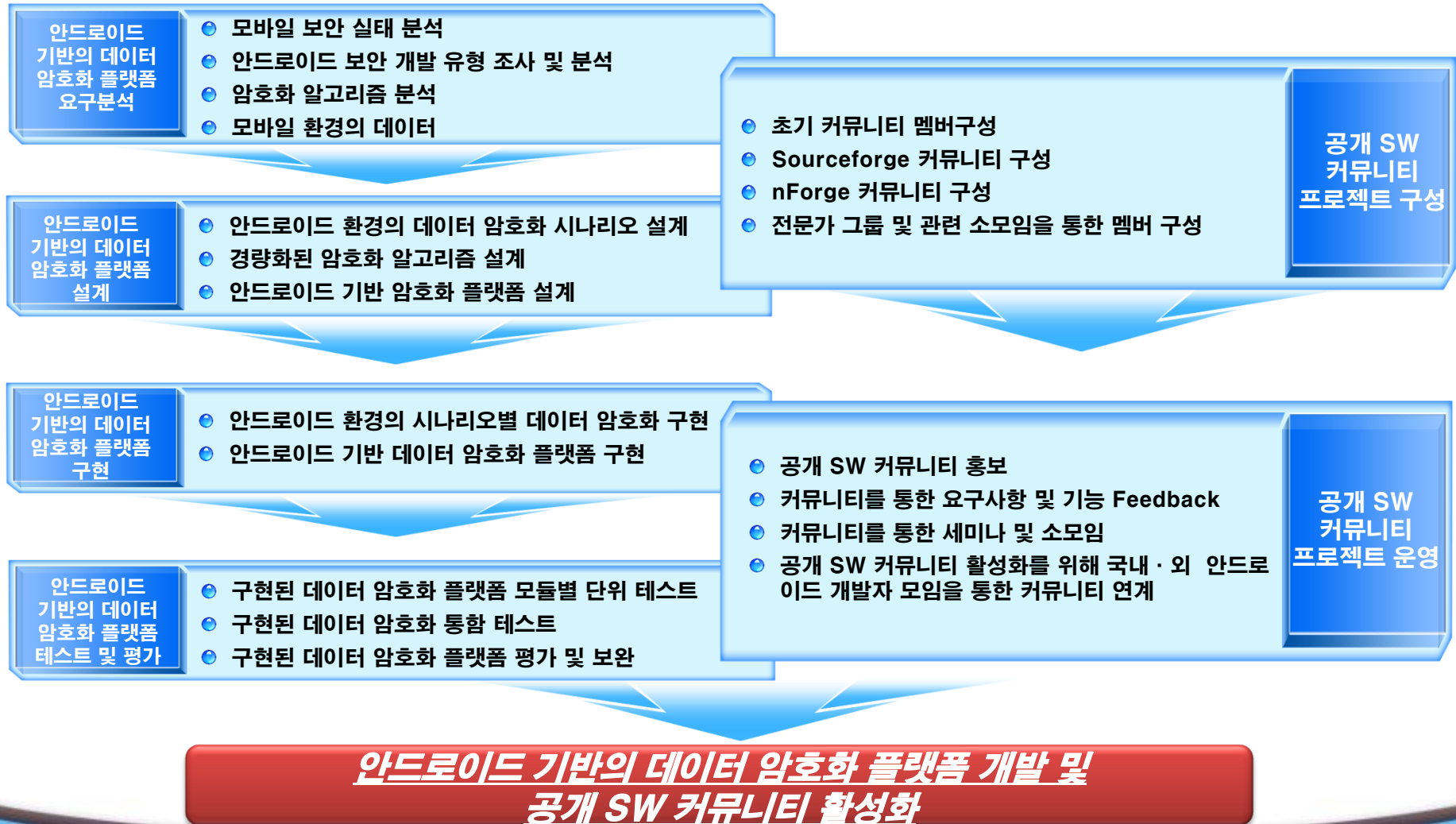
추진체계

커뮤니티 운영체계

개발일정

추진체계

● 과제추진체계



추진체계

● 수행 방법

경원대학교(주관연구기관)

- 실제 과제 수행
- 관련 문헌과 인터넷을 통한 관련자료 수집 및 분석
- 안드로이드 기반의 보안 관련 세미나, 워크샵, 학술대회를 통한 관련 자료 수집/분석
- 보안 기술 관련 전문가들과 회의를 통한 과제 진행
- 지속적인 커뮤니티 활동을 통한 과제 업데이트

전문가 그룹

- 과제 진행 검토 및 방향 협의
- 안드로이드 기반의 인터넷전화 기술동향 관련 전문가의 자문 협조
- 관련 업체 전문가에 의한 도청방지 기술협조

- 월 1회 기술세미나 발표
- 커뮤니티를 통한 지속적인 자료 공유

공개 SW 커뮤니티

- 커뮤니티 멤버구성
- Sourceforge.net 커뮤니티 구성
- nForge 커뮤니티 구성
- 학교 개발 동아리와의 교류
- 주관연구기관과의 기술 교류
- 안드로이드 개발자 모임을 통한 커뮤니티 연계

추진체계

● 과제 개발 방법

전문가그룹 활용방안

- 과제 진행 및 협조
- 월 1회 기술 세미나
- 월 1회 기술 이전 교육

주관기관(대학) 활용방안

- 월 1회 기술 세미나 발표
- 월 1회 이전 발표 시행
- 시스템 요구 사항 분석
- 모바일 환경에 적합한 경량화 암호 알고리즘 설계
- 시나리오별 데이터 암호화 설계 및 구현
- 데이터 암호화 플랫폼 설계 및 구현
- 시스템 테스트 및 평가
- Test Bed 구축
- Test Bed 가동 및 최종 평가

커뮤니티 활용방안

- 전문가 자문을 통한 과제 개발 질 향상
- 소모임을 통한 필드테스트 및 의견 검토
- 일반 사용자들의 요구사항 분석
- 과제 진행 관련 피드백
- 개발동아리와의 교류

목 차



개발 목표 및 내용

추진체계

커뮤니티 운영체계

개발일정

커뮤니티 운영체제

● 커뮤니티 구성

- 안드로이드 어플리케이션을 개발할 시 데이터 암호화 기술을 적용하기 위하여 본 커뮤니티 프로젝트 구성
- 주관기관의 개발자 중심으로 초기개발자 멤버 구성
- 지속적인 자문을 위한 전문가 그룹 형성
- 본교 개발동아리의 교류를 통한 초기 커뮤니티 멤버 구성

전문가 그룹 참여 인원

구분	소속	직위	성명
전문가	한양대	교수	오희국
전문가	순천향대	교수	이임영
전문가	성균관대	교수	엄영익
전문가	한양대	교수	김동규
전문가	KISA	단장	원유재
전문가	ETRI	부문장	장종수
합계	총 : 6명		

커뮤니티 운영체제

● 커뮤니티 운영계획

홍보를 통한
커뮤니티
사용자
참여 유도

보안뉴스, 안드로이드
개발 커뮤니티 등의
홍보를 통한 참여 유도

타 커뮤니티
연계를 통한
유대 관계
도모

타 커뮤니티에서
주최하는 세미나 및 모임
적극적인 참여하여 다른
커뮤니티와의 관계 발전

개발자센터에
개발 프로젝트
커뮤니티 신설
및 관리

SourceForge.net,
nForge, Google
개발자 센터에 개발
프로젝트 커뮤니티
신설/관리

개발자 그룹
정기 세미나
개회

초기 개발자 그룹은
월 1회 정기적인 세미나 통해
과제 진행

경원대학교
개발동아리
연계를 통한
프로젝트
활성화

본교에 존재하는 개발동아리
(하늘신폭, 앱동아리) 연계
프로젝트 활성화

커뮤니티 운영체계

● 커뮤니티 발전방안

공개 SW 커뮤니티 발전

안드로이드 사용자의
테스트를 통한
문제점 도출 및
지속적인 업데이트

안드로이드 관련
커뮤니티 등
본 프로젝트의
활용사례를 통한
사용자의 개선사항 반영

보안뉴스,
자유 게시판 등
대내외 홍보를 통한
커뮤니티 활성화

목 차



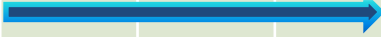
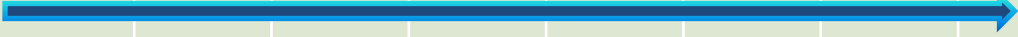
개발 목표 및 내용

추진체계

커뮤니티 운영체계

개발일정

개발일정

과제 내용	추진일정									진도율(%)
	4	5	6	7	8	9	10	11	12	
요구분석	 									50%
설계										0%
구현										0%
테스트 및 평가										0%
커뮤니티구 성	 									75%
커뮤니티 운 영		 								3%

중간보고서 : 8월, 최종보고서 12월



감사합니다