안드로이드 기반 데이터 암호화 플랫폼 분석 및 설계

조대균*, 윤성열*, 박석천**
*가천대학교 전자계산학과
**가천대학교 컴퓨터공학과
e-mail:scpark@gachon.ac.kr

Analysis and Design of Data-Encryption Platform Based on Android

Dae-Kyun Cho*, Sung-Yeol Yun*, Seok-Cheon Park**
*Dept of Computer Science, Gachon University
**Dept of Computer Engineering, Gachon University

요 약

최근 모바일 보안에 많은 이슈가 되고 있고, 그 중 많은 사람들이 이용하는 안드로이드 어플리케이션에서도 악성 어플리케이션이 등장함에 따라 많은 개인정보 피해가 속출되고 있다. 이에 따라 안드로이드 어플리케이션의 데이터유형 별로 특징을 분석하고, 분석된 유형별로 사용할 수 있도록 암호화 알고리즘을 분석하며, 분석된 내용을 바탕으로 안드로이드에서 사용할 수 있도록 플랫폼의 형태로 설계하였다.

1. 서론

최근 무선정보통신이 발전함에 따라 그에 따른 여러 가지 형태의 무선장비가 개발되어 사용되고 있다. 무선장비의 형태는 스마트폰, 태블릿 PC 등등 여러 가지 형태로 개발되고 있으며, 특히 스마트폰 시장의 규모는 IT 업계에 새로운 트렌드를 이끌고 있다. 이러한 대표적인 스마트폰 장비 중 안드로이드가 있다. 그리고 안드로이드 기기에 사용할 수 있는 어플리케이션도 많이 개발되어 사용되고, 안드로이드 어플리케이션을 이용하여 많은 정보가 이동되고 있다.[1]

하지만 이렇게 이동되는 정보에 대한 보안 인식은 많이 부족한 실정이라 이용자의 중요한 정보를 강제로 유출 시키는 악성 어플리케이션도 생겨나고 있다. 이와같은 정보 유출 문제는 개발자들의 데이터 암호화에 대한 지식이 부족하고, 데이터를 암호화를 사용해야 한다는 인식도 많이 부족함에 따라 문제가 더욱 심각해지고 있다. 또한 일반적으로 안드로이드 어플리케이션을 개발하는 것보다 보안을 추가하여 개발하는 것이 훨씬 많은 시간과 비용이 소모된다. 그리고 일반적인 데이터 암호화 기술은 암호화 알고리즘별로 장, 단점이 극명하게 다르기 때문에, 잘못 사용할 경우에는 충분한 암호화 강도를 기대할 수 없고, 연산속도·효율성 등이 현저하게 떨어진다[2][3].

따라서 본 논문에서는 안드로이드 환경에서 사용될 수 있는 어플리케이션을 이용되는 데이터 시나리오별로 분석하고, 분석된 시나리오를 암호 알고리즘과 비교 분석한다. 분석된 내용을 이용하여 안드로이드기반 데이터 암호화 플랫폼 설계한다. 이를 통해 안전한 어플리케이션 개발을 하고자 하는데 목적이 있다.

본 논문은 2장에서는 관련연구를 작성하고, 3장에서는 안드로이드 데이터와 암호 알고리즘에 대해서 분석하고, 4장에서는 분석한 내용을 바탕으로 안드로이드 기반 데이터 암호화 플랫폼 설계한다.

2. 관련 연구

2.1 안드로이드

휴대폰용 운영체제·미들웨어·응용프로그램을 한데 묶은 소프트웨어 플랫폼으로써, 현재 애플의 iOS와 함께 휴대폰 업계를 이끌고 있다. 11년도 1월에 안드로이드 사용자는 미국 내에서는 전체 스마트폰 이용고객중 26%를 차지하여 두 번째로 많이 사용되는 스마트폰이며(첫 번째 많이 사용되는 스마트폰은 블랙베리 33.5%), 국내에서는 11년도 4월 기준으로 안드로이드 스마트폰이 국내 출시된지 1년만에 500만대 이상이 팔렸으며 국내 스마트폰 시장에서 차지하는 비율은 60%가 넘는다. 또한 10년 12월 기준으로 안드로이드 마켓의 어플리케이션의 숫자는 20만이 돌파하였으며, 다운로드 횟수는 25억 회가 넘는다. 안드로이드는 많은 사람들이 사용하고 있으며, 많은 어플리케이션이 개발되고 사용되어지고 있다.[4]

2.2 암호 알고리즘

DES 암호화 알고리즘은 Data Encryption Standard의 약어로써, 미국의 국가 표준국이 국가 표준으로 채택하였

* 가천대학교 일반대학원 전자계산학과
** 가천대학교 IT대학 컴퓨터공학과 정교수(교신저자)

으며, 암호 알고리즘이 공개되어 있다. 대칭형 암호 방식으로 정보를 보내는 사람과 받는 사람이 동일한 비밀키를 가져야 하며, 암·복호화 속도가 다른 암호화 알고리즘의 비해 빠른 장점을 가지고 있다.

RSA(Rivest Shamir Adleman) 암호화 알고리즘은 소인수분해의 어려움을 가지고 데이터를 암호화 하는 방식으로, 앞에서 언급한 DES 알고리즘과는 다르게 송신자와 수신자의 개인키가 상이해도 사용할 수 있는 암호화 알고리즘이다. RSA 암호화 알고리을 사용하려면 굉장히 큰 숫자(1024bit)이상의 수를 사용하게 되면 암호화된 데이터를 해독하는데 굉장히 오랜 시간이 소요되는 만큼 암호화 강도가 굉장히 높다. 하지만 반대로 굉장히 큰 수 자리를 사용하기 때문에 DES 암호화 알고리즘과 비교했을 경우 자원소모량이 많고, 암·복호화에 걸리는 시간도 길다.

ECC(Elliptic Curve Cryptosystem) 암호화 알고리즘은 약 10년 전부터 비트당 안전도가 타 공개키 암호 알고리즘보다 효율적이라는 것이 알려졌다[5][6].

3. 안드로이드 기반 데이터 암호화 플랫폼 분석

3.1 데이터 암호화 시나리오 분석

안드로이드 어플리케이션은 이동하는 데이터의 형태에 따라 단말저장형 데이터, 일반 전송형 데이터, 실시간 전송형 데이터로 구분된다. 단말 저장형 데이터의 경우에는 스케줄러, 주소록 등과 같이 데이터 이동이 안드로이드 기기 단말에서만 주로 사용되는 데이터이며, 일반 전송형 데이터는 메일 및 카드 결제와 같이 1회성으로 전송을 하는 데이터를 말하며, 실시간 전송형 데이터는 전화와 문자, 채팅과 같이 실시간으로 주고 받는 데이터이다. 시나리오별 암호화 알고리즘을 비교하면 표 1과 같다[7].

<표 1> 시나리오별 암호화 알고리즘 비교

	단말저장형 데이터	일반전송형 데이터	실시간 전송형 데이터
특성	개인정보 보호	매우 높은 암호 강도	빠른 암·복호화 속도/강한 암호 알고리즘
어플리케이션 유형	스케줄러, 메모, 전화번호부	그림 첨부, 메일, 모바일 뱅킹	음성통화, 채팅
위험요소	도난, 분실, 해킹 노출	해킹	해킹
암·복호화 속도	빠름	느림	중간
키 분배	어려움	용이함	용이함
필요 암호 강도	낮음	높음	높음
알고리즘	DES	RSA	ECC

상기 표 1과 같이 데이터의 타입을 분류한 것은 암호화 알고리즘의 특징을 극대화 하려고 하는 것이다. DES 암호화 알고리즘의 장점은 빠른 암·복호화 속도와 다른 알고리즘에 비해 메모리 및 자원 소모량이 낮다. 하지만 송·수신자가 동일한 개인키를 가지고 있어야 하며, 개인키를 가지고 있지 않은 경우 키 전송을 해야 하는 큰 어려움이 있다. RSA 암호화 알고리즘의 장점은 다른 알고리즘에 비해 한번에 많은 양의 데이터를 할 수 있다. 단점은 다른 알고리즘에 비해 자원 소모량 및 암·복호화에 걸리는 시간이 많이 소모된다는 점이다. ECC 암호화 알고리즘은 DES 알고리즘과 RSA 알고리즘의 특징을 둘 다 가지고 있는데, ECC 알고리즘은 공개키 알고리즘으로써 개인키 전송의 유리한 장점을 가지고 있다. 또한 RSA 알고리즘에 비해 적은 키 길이로도 높은 암호화 강도를 가지기 때문에 RSA에 비해 보다 암·복호화 속도 및 자원 효율성은 높다.

3.2 시나리오에 따른 암호 알고리즘 비교 분석

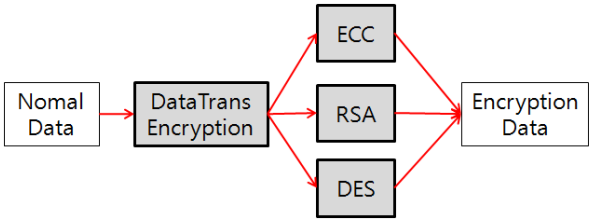
데이터 암호화 시나리오에 따른 암호화 알고리즘별 특징별로 어플리케이션을 분류한 후에는 각 필요한 암호화 알고리즘을 선택하여야 한다. 그러나 일반적인 안드로이드 어플리케이션 개발자의 경우에는 암호화 알고리즘의 특징을 잘 모를 경우가 많다. 따라서 일반적인 암호화 알고리즘의 특징을 표 2에 나타내었다. 분석표의 기준은 암호화의 쓰이는 키의 크기가 DES는 8bit, ECC는 160bit, RSA는 1000bit의 기준일 때를 나타낸 것이다. 이 기준은 각 알고리즘이 충분히 높은 암호화 강도를 기대할 수 있는 최소치이다.

<표 2> 안드로이드 기반 데이터 유형 분석 표

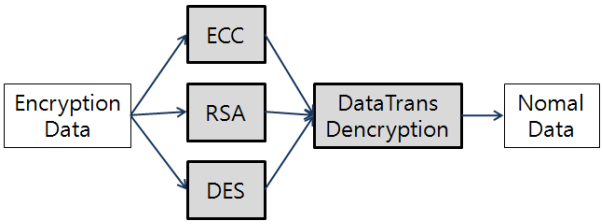
사항	요약	DES	ECC	RSA	단위
메모리 사용량	암·복호화 모듈의 데이터 처리 시 메모리 사용량	500 ~ 800	1200 ~ 1800	1700 ~ 2300	Kb
보안성 (암호화 강도)	위의 키 크기일 때 보안 수준	낮음	높음	높음	
암·복호화 속도	데이터 암·복호화 처리 속도 (※ 초기화 시간)	0.009 ~ 0.012	0.001 ~ 0.1 (1.126 ±0.3)	180 ~ 210 (904 ±80)	ms
암·복호화 키 노출위험성	키 교환 시 위험	높음	낮음	낮음	
데이터 크기(String의 길이)	모듈 1회당 처리하는 데이터(String)의 길이	8	100 ~ 160	1000 ~ 1600	bit

4. 안드로이드 기반 데이터 암호화 플랫폼 설계

그림 1, 2는 안드로이드 기반 데이터 암호화 플랫폼 구성도이다. 그림 1은 데이터를 암호화하는 과정을 나타낸 것이며, 그림 2는 복호화 과정을 나타낸 것이다.

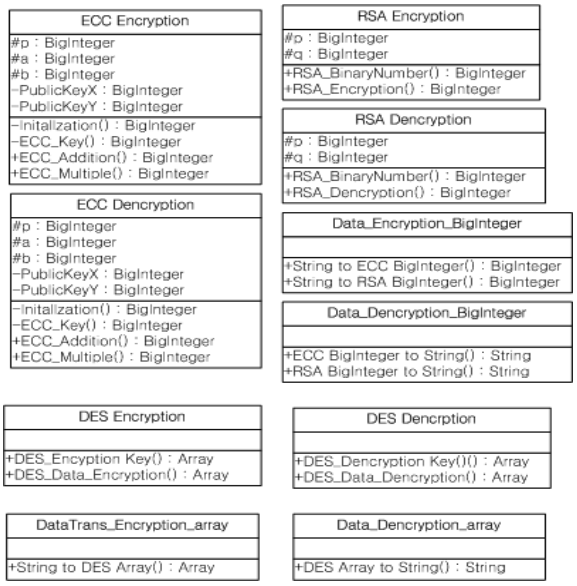


(그림 1) 안드로이드 기반 데이터 암호화 플랫폼 설계 구성도-암호화



(그림 2) 안드로이드 기반 데이터 암호화 플랫폼 설계 구성도-복호화

암호화 과정은 평문 데이터가 데이터형 변환 모듈에서 각 암호화에 필요한 데이터 형태로 변환되며, 각 암호화 모듈에서 암호화가 되어 암호화된 데이터로 변환된다. 복호화 과정에서는 암호화된 데이터가 암호화 모듈에 들어가서 복호화 과정을 통해 데이터가 복호화되며 데이터 형변환 모듈을 통해 원래의 데이터로 나타내는 과정을 나타내고 있다.



(그림 3) 안드로이드 기반 데이터 암호화 플랫폼 상세 클래스 다이어그램

그림 3은 안드로이드 기반 데이터 암호화 플랫폼 상세 클래스 다이어그램이다. 클래스는 10개로 구성되어 있으며, 각 암호화 알고리즘 별 Encryption과 Dencryption 클래스 다이어그램으로 구성되어 있으며, 암호화 및 복호화를 위한 데이터형 변환 클래스도 2개씩로 구성되어 있다.

기본적으로 암호화를 하기 위해서는 String형 및 파일로 데이터가 구성되어 있고, 기본 데이터 형태를 Array 및 BigInteger형으로 변환해야 한다. Array는 DES 암호화 알고리즘에서 사용되며, BigInteger형은 ECC와 RSA 암호화 알고리즘의 사용한다.

5. 결론

본 논문에서 안드로이드 어플리케이션을 사용되는 데이터 시나리오에 따라 어플리케이션을 분석하였고, 시나리오에 맞는 각 암호화 알고리즘의 특징을 분석하였다. 그리고 각각 분석한 내용을 활용하여 데이터 특징에 맞는 암호화 알고리즘을 이용할 수 있도록 안드로이드 플랫폼의 형태로 설계하였다.

제안하는 안드로이드 기반 데이터 암호화 플랫폼을 이용하여 안드로이드 어플리케이션을 제작하면 암호 알고리즘을 보다 쉽게 사용할 수 있으며, 보다 안전한 어플리케이션을 만들 수 있다. 향후연구로도 안드로이드 기반을 벗어나 iOS 및 기타 다른 분야에서 활용할 수 있도록 개선할 예정이다.

ACKNOWLEDGMENT

본 연구는 가천대학교의 지원으로 수행되었음

참고문헌

[1] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안 기술”, 정보보호학회지, 2009.10

[2] 박지연, 민홍, 장준혁, 조유근, 홍지만, "안드로이드 플랫폼을 위한 보안 기법 연구", 2011 한국컴퓨터종합학술대회 논문집 Vol. 38, No.1(B), 2011. 6

[3] 장선진, “Android Security”, 제 6회 공개 SW 역량프라자 정기기술 세미나, 2010.12

[4] 고석훈, “안드로이드 플랫폼 동향”, 한국콘텐츠학회 논문지, 2010. 6

[5] 염헌영, 강수용, 김현주, 최순호, “대칭키/공개키 암호 알고리즘의 키 길이 따른 안전도 비교 분석 및 관련 S/W 개발”, 정보통신연구진흥원 학술기사, 2001.11

[6] 강주성, 박춘식, “공개키 암호 방식의 안전성 개념에 관한 연구 ”, 정보보호학회지, 1998.12

[7] 윤성열, 조대균, 박석천, “모바일 환경에서 시나리오에 따른 암호 알고리즘 비교 분석 연구”, 한국정보처리학회 춘계학술대회, 2011. 5