안드로이드 기반 데이터 암호화 플랫폼 설계 및 구현

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

Design and implementaion 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

안드로이드 어플리케이션 개인 정보 유출의 문제가 이슈화 되고 있다. 이 문제는 개발자가 어플리케이션을 개발하는데 있어 데이터 암호화 전혀 고려하지 않으며, 데이터 암호화에 대한 지식도 많이 부족하다. 따라서 본 논문에서는 안드로이드 어플리케이션에서 사용되는 데이터 유형을 분석하여 시나리오를 작성하여 암호화 알고리즘과 설계한다. 설계한 내용을 바탕으로 안드로이드 기반 데이터 암호화 플랫폼을 구현하였다.

1. 서론

최근 국내 스마트폰의 보급이 2,500만대를 넘어서면서 이에 따른 모바일 콘텐츠 또한 급격하게 발전하고 있다. 특히 안드로이드의 경우 애플의 iOS와 함께 스마트폰 시장에서 높은 점유율을 차지하고 있으며, 안드로이드 기반 어플리케이션 시장도 급격히 성장하고 있다.

그러나 악성 어플리케이션의 경우 안드로이드 이용자의 개인 정보를 유출시키고, 유출되는 데이터는 암호화가 되지 않은 상태로 유출되기 때문에, 이 피해는 안드로이드 이용자에게 고스란히 전달되어 큰 문제를 발생되고 있다.[1][2].

따라서 본 논문에서는 이런 문제를 해결하기 위해 안드로이드 어플리케이션의 유형을 시나리오를 작성하고, 작성된 시나리오를 바탕으로 암호알고리즘과 분석하며, 분석된 내용을 바탕으로 안드로이드 기반 데이터 암호화 플랫폼 설계를 작성한다. 그리고 안드로이드 기반 데이터 암호화 플랫폼을 구현한다.

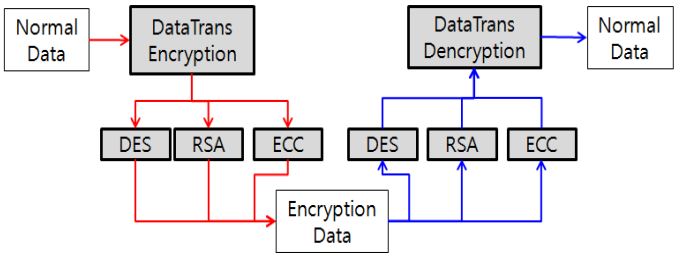
2. 안드로이드 기반 데이터 암호화 분석

안드로이드 어플리케이션에서 사용되는 데이터의 유형에 따라 단말저장형 데이터, 일반전송형 데이터, 실시간 전송형 데이터로 시나리오를 작성하였다. 단말저장형 데이터의 경우에는 단말내에서만 이동되는 데이터, 일반전송형 데이터의 경우에는 일반적으로 한번만 전송하는 데이터, 실시간 전송형 데이터는 쌍방간의 지속적인 교류하는 데이터로 구분하였다.

그리고 어플리케이션 특징 및 키분배, 암·복호화 속도 등을 비교하였을 때 단말저장형 데이터는 DES 암호화 알고리즘, 일반전송형 데이터는 RSA 암호화 알고리즘, 실시간 전송형 데이터는 ECC 암호화 알고리즘을 사용하는 것이 적합하다[3].

3. 안드로이드 기반 데이터 암호화 플랫폼 설계

안드로이드 기반 데이터 암호화 플랫폼 구성은 그림 1과 같이 설계하였다.



(그림 1) 안드로이드 기반 데이터 암호화 플랫폼 구성도

그림 1의 빨간색 화살표는 암호화 절차이며, 파란색 화살표는 복호화 절차이다. 암호화 절차에서는 평문 데이터가 데이터형 변환 모듈 통해 int배열 및 BigInteger 데이터로 변환되어 암호화과정을 통해 데이터 암호화를 한다. 복호화 절차는 암호화된 데이터인 Int배열 및 BigInteger 데이터가 복호화 모듈에 들어가서 복호화 과정을 통해 데이터가 복호화되며 데이터 형변환 모듈을 통해 원래의 평문 데이터로 나타낸다[4].

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

4. 안드로이드 기반 데이터 암호화 플랫폼 구현

4.1 구현환경

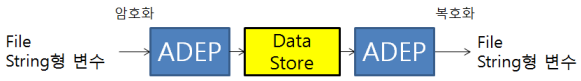
안드로이드 기반 데이터 암호화 플랫폼을 구현하기 위한 개발환경은 표 1과 같다.

<표 1> 제안하는 플랫폼의 구현환경

	구성요소	사양
H/W	CPU	Intel i5 650 3.2Ghz
	RAM	2GB
S/W	운영체제	Windows 7
	개발 플랫폼	JDK 1.7.0 eclipse Android Platform

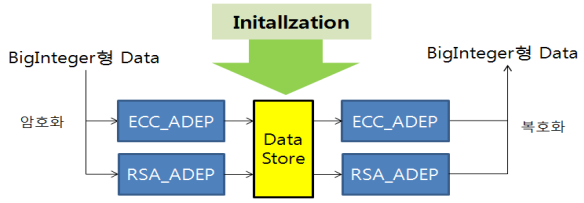
4.2 시스템 구성

제안하는 안드로이드 기반 데이터 암호화 플랫폼(ADEP:Android Data Encryption Platform)은 ECC, RSA, DES 암호화 알고리즘을 이용하여 각 데이터를 File이나 String형으로 입력하게 되면 ADEP를 통해 암호화된 데이터가 저장되고, ADEP를 통해 복호화가 되어 원래 데이터 형태로 된다. 그림 2는 ADEP 전체 시스템 구성도이다.



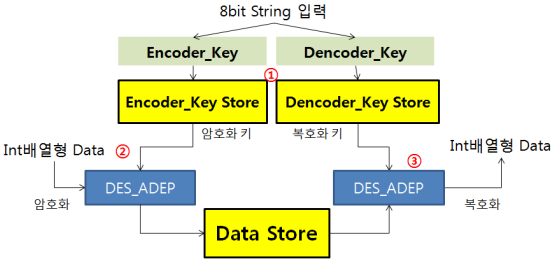
(그림 2) 전체 시스템 구성도

그림 3은 일반 및 실시간 전송형 모듈 구성도이다. Initallzation에서는 ECC 및 RSA암호화 알고리즘을 사용하는 초기화 상수값을 설정한다. 그리고 BigInteger형 Data를 입력 받아서 암·복호화를 한다.



(그림 3) 일반 및 실시간 전송형 모듈 구성도

그림 4는 단말 저장형 모듈 구성도이다. 모듈 절차는 다음과 같다.



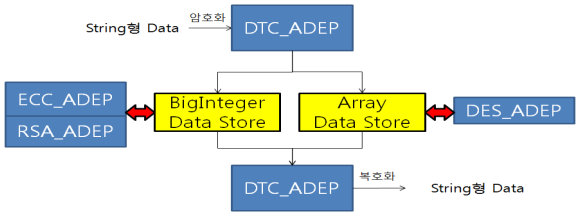
(그림 4) 단말저장형 모듈 구성도

① 8bit String을 이용하여 Encoder_Key와 Dencoder_Key에서 암·복호화 키를 생성한다.

② 입력받은 데이터와 Encoder_Key를 이용하여, 데이터를 암호화 한다.

③ 암호화된 데이터와 Decoder_Key를 이용하여 암호화된 데이터를 복호화 한다.

그림 5는 안드로이드 기반 데이터 형 변환 플랫폼 구성도이다. 일반 String형 Data나 File 데이터를 데이터형 변환 모듈 (DTC_ADEP)을 통해 Int배열 Data나 BigInteger형 Data로 변환된다. 변환된 데이터를 이용하여 ECC, RSA, DES 모듈에 암·복호화 과정으로 처리를 하고, 다시 원래의 String형 Data 및 File Data로 형변환을 한다.



(그림 5) 안드로이드 기반 데이터 형 변환 플랫폼 구성도

5. 결론

본 논문에서는 안드로이드 데이터 암호화 플랫폼 설계 및 구현을 하기 위해 안드로이드 어플리케이션을 데이터 사용 유형에 따라 분석하고, 시나리오를 작성하였다. 시나리오에 맞는 암호화 알고리즘을 플랫폼 설계하였으며, 플랫폼 설계를 바탕으로 데이터 암호화 플랫폼을 구현하였다.

제안하는 안드로이드 안드로이드 기반 데이터 암호화 플랫폼을 이용하면 보다 안전한 안드로이드 어플리케이션을 개발할 수 있다. 향후연구로는 운영체제의 범위를 안드로이드에서 보다 확장할 수 있도록 개선할 예정이다.

ACKNOWLEDGMENT

"본 연구는 지식경제부 및 정보통신산업진흥원의 'IT융합 고급인력 지원사업'의 연구결과로 수행되었음"
(NIPA-2012-H0401-12-1001)

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] 윤성열, 조대균, 박석천, "모바일 환경에서 시나리오에 따른 암호 알고리즘 비교 분석 연구", 한국정보처리학회 춘계학술대회, 2011. 5

[4] 윤성열, 조대균, 박석천, "안드로이드 기반 데이터 암호화 플랫폼 분석 및 설계", 한국정보처리학회 춘계학술대회, 2012. 4