모바일 환경의 어플리케이션 유형별 데이터 암호화 플랫폼 설계

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

Design of Data Encryption Platform by Types of Application in Mobile Environment

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

요 약

모바일 보안에 대해 개인정보유출 피해방지를 위하여 모바일 기반 어플리케이션에 사용되는 데이터 유형을 단말저장형, 일반전송형, 실시간전송형 데이터로 정의하고, 데이터 유형에 맞는 암호화 알고리즘의 특징을 비교·분석하였다. 그리고 개발자가 개발하는 어플리케이션에 맞는 암호화 알고리즘을 사용하기 위하여 암호화 알고리즘 특성에 맞는 항목으로 객관적인 비교·분석을 하였다. 또한 객관적인 분석을 통하여 데이터형태를 정할 수 있는 데이터 유형분석 알고리즘을 설계하였다.

1. 서론

최근에 전자기기장비와 통신환경의 진화에 따라 모바일 환경이 급속히 발전하였다. 특히 스마트폰은 대중적으로 보급되어 현재에는 일상에 꼭 필요한 수단이 되었다. 그리고 스마트폰을 보다 효율적으로 사용하기 위한 어플리케이션은 빠르게 발전하여 많은 이용자를 확보하고 있다.

그러나 이런 어플리케이션 중 개인정보를 유출시키는 악성 어플리케이션이 발생하여 이용자들에게 개인정보 유출피해를 주고 있다. 이런 문제를 방지하기 위해서는 어플리케이션을 개발할 때, 데이터를 암호화하여 관리하는 방법으로 해결할 수가 있다[1][2].

따라서 본 논문에서는 모바일 환경의 어플리케이션 유형별 데이터 암호화 플랫폼을 설계하기 위해 모바일 환경의 어플리케이션 유형별 데이터를 정의하고, 암호화 알고리즘의 특징 및 장·단점을 비교·분석한다. 분석된 어플리케이션의 데이터 특징에 따라 맞는 암호화 알고리즘을 선택하는 알고리즘을 설계한다.

2. 관련연구

2.1 DES 암호화 알고리즘

DES(Data Encryption Algorithm) 암호화 알고리즘은 미국 IBM에서 개발한 대표적인 대칭키 암호화 알고리즘이다. 1977년부터 미국 표준국에서 채택되어 지금까지도 사용하고 있다. DES 암호화 알고리즘은 64bit의 블록을 단위로 암호화하고, 암호화 시 사용되는 키는 56bit의 키를 사용한다. 특징으로는 암·복호화 속도가 다른 암호화 알고리즘보다 빠르며, 현재에는 보안강도의 향상을 위해 3-DES 및 AES 암호화 알고리즘을 많이 사용된다[3].

2.2 RSA 암호화 알고리즘

RSA 암호화 알고리즘은 미국 MIT의 Rivest, Shamir, Adlemen가 발표한 대표적인 공개키 암호화 방식으로, 암호화 강도 및 키 분배에 용이하여 현재에도 많이 사용하는 암호화 알고리즘 방식이다. 암호화 알고리즘의 방식은 큰 두 개 소수의 소인수분해의 어려움을 이용하여 암호화 알고리즘으로 사용하고 있으며, 1024bit에 암·복호화 키를 사용하기 때문에 암·복호화 속도가 느린 단점을 가지고 있다[4].

2.3 ECC 암호화 알고리즘

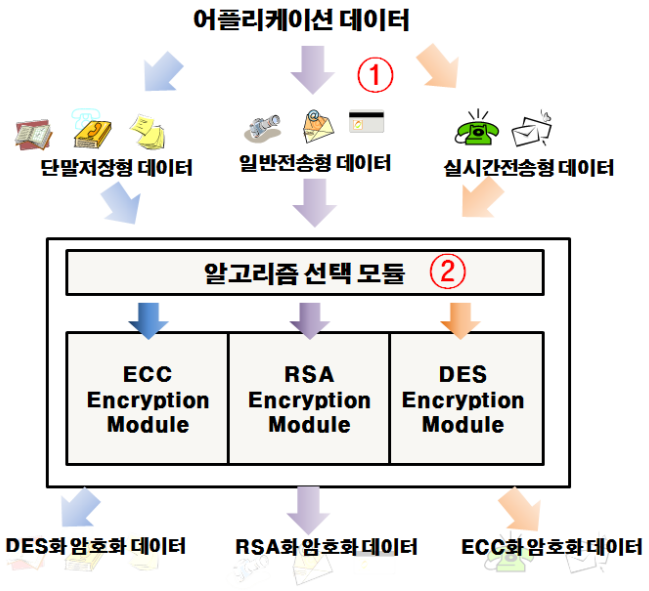
ECC(Elliptic Curve Cryptosystem) 암호화 알고리즘은 타원곡선 암호체계를 이용한 공개키 암호화 방식의 하나로, 1985년 N. Koblitz와 V.S. Miller의해 발표되었다. 타원곡선과 법의 개념을 사용하며, RSA 알고리즘 1024bit와 ECC 암호화 알고리즘의 160bit가 비슷한 암호화 강도를 가지고 있어 모바일 데이터 암호에서 많이 사용되고 있는 암호화 알고리즘이다[5].

---

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

3. 모바일 환경의 어플리케이션 유형별 암호화 플랫폼 설계

그림 1은 어플리케이션 유형별 암호화 플랫폼 설계를 위해 도출한 암호화 플랫폼 설계 개요도이다. ①에서는 어플리케이션 데이터를 유형별로 정의하고, ②에서는 개발하는 어플리케이션의 특징을 제시된 질문을 통해 정의된 데이터형태로 선택하는 알고리즘을 설계한다.



(그림 1) 암호화 플랫폼 설계 개요도

3.1 데이터 암호화 시나리오 분석

현재 이용하는 모바일 어플리케이션의 데이터를 이동형태에 따라 단말저장형 데이터, 일반전송형 데이터, 실시간전송형 데이터 형태로 구분하였다. 단말저장형 데이터는 전화번호부, 주소록과 같이 다른 단말로 이동되지 않고 단말내에서만 사용되는 데이터이며, 일반전송형 데이터는 메일, 결제 등과 같이 일회성의 큰 자료를 다른 단말로 보내는 데이터이며, 실시간전송형 데이터는 통화, 채팅과 같은 단말간 지속적인 통신이 필요한 데이터이다[6].

표 1은 데이터 시나리오별 특징을 비교연구한 표이다. 표와 같이 데이터 형태를 구분한 것은 각각의 암호화 알고리즘의 특징을 활용하기 위함이다. 단말저장형 데이터는 DES 암호화 알고리즘의 빠른 암·복호화와 데이터가 통신환경을 이용하지 않아 키 전송이 사용할 필요가 없는 특징을 이용한 것이다. 일반전송형 데이터는 중요한 데이터를 이용하기 위해서는 높은 암호화 강도와 통신환경에서 사용하기 적합한 공개키 암호화 알고리즘, 일회성으로 사용하기에 적합한 RSA 암호화 알고리즘의 특징을 이용하였다. 실시간 전송형 데이터는 지속적으로 통신환경에서 사용하고, 통신환경에서 비교적 빠른 암·복호화 속도를 사용하는 ECC 암호화 알고리즘의 특징을 이용한 내용이다.

<표 1> 데이터 시나리오별 특징 비교

	단말저장형 데이터	일반 전송형 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

3.2 암호화 알고리즘 비교 분석

모바일에서 이용가능한 암호화 알고리즘의 일반적인 특징으로는 이용하는 개발자가 주관적인 판단으로 어플리케이션의 특징과 맞지 않은 암호화 알고리즘을 사용할 수 있다. 따라서 객관적인 판단을 할 수 있도록 항목을 정하고 이를 구체적인 수치로 표현하였다. 표 2는 모바일 환경에서 암호화 알고리즘 유형분석한 표이다[7].

<표 2> 모바일 기반 암호화 알고리즘 특징 분석

사항	요약	DES	ECC	RSA	단위
메모리 사용량	암·복호화 모듈의 데이터 처리 시 메모리 사용량	788	1583	1836	Kb
키의 크기	속도와 암호 강도를 고려한 평균(표준) 데이터의 길이	8	160	1000	bit
보안성 (암호화 강도)	위의 키 크기일 때 보안 수준	낮음	높음	높음	
암·복호화 속도	데이터 암·복호화 처리 속도 (※ 초기화 시간)	0.009	0.001 (1.126)	205 (904)	ms
암·복호화 시 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

항목은 모바일 메모리 사용량, 키의 크기, 보안성, 암·복호화 속도, 암·복호화 시 키 노출위험성, 일반 데이터의 크기로 구분하였다. 또한 항목에 대해서 각 암호화 알고리즘을 이용할 경우에 나타나는 평균적인 수치를 표 2에 나타내었다.

4. 모바일 어플리케이션 데이터 유형 분석 알고리즘 설계

암호화 알고리즘 비교 분석을 통해 도출된 표는 보안 알고리즘에 사전지식이 없는 개발자가 이용하기 어렵기 때문에 표 2를 바탕으로 표 3과 같은 질문을 통해 개발자가 어플리케이션 개발에 데이터유형을 선택할 수 있는 알고리즘을 설계하였다.

<표 3> 모바일 데이터 유형 분석 알고리즘

	질문	보기		
1	단말에서 사용 가능한 자원 메모리의 양은 얼마입니까?	적음	보통	여유로움
2	어플리케이션 사용에서 보안과 처리시간에 대해서 어느 것에 중점을 두십니까?	처리시간	중간	보안
3	통신을 사용합니까?	한다		안한다
4	평균처리하는 데이터의 크기(bit)	TEXT로 입력받음		

표 3은 모바일 데이터 유형 분석 알고리즘으로 각 질문마다 해당되는 보기를 선택하여 각각 데이터형태에 점수를 부가하여 최고로 나온 점수를 채택하는 방식이다.

질문 1은 '단말에서 사용 가능한 자원 메모리의 양은 얼마입니까?'에 대한 질문은 표 2의 항목중 메모리 사용량에 해당되는 내용으로 적음은 단말저장형 데이터, 보통은 단말저장형, 실시간전송형 데이터, 여유로움은 단말저장형, 실시간전송형 일반전송형 데이터에게 1점씩를 부여한다.

질문 2는 '어플리케이션 사용에서 보안과 처리시간에 대해서 어느 것에 중점을 두십니까?'에 대한 질문은 표 2의 키의 크기, 보안성, 암·복호화 속도에 대한 내용으로 처리시간은 단말저장형 데이터, 중간은 실시간 전송형 데이터, 보안은 일반전송형 데이터 항목에 2점씩 부여한다.

질문 3은 '통신을 사용합니까'에 대한 질문은 표 2의 항목 중 암·복호화 시 키 노출 위험성에 해당되는 내용으로 한다는 일반전송형, 실시간전송형 데이터, 안한다는 단말저장형 데이터에 점수를 1점씩 부여한다.

질문 4는 '평균처리하는 데이터의 크기'에 대한 질문은 표 2의 데이터 크기에 해당되는 내용으로 입력받은 데이터의 크기가 1~100bit일 경우에는 3가지 단말저장형, 실시간전송형 일반전송형 데이터, 100~1000bit일 경우에는 일반전송형과 실시간전송형 데이터에, 1000bit이상을 경우에는 일반전송형 데이터에게 점수를 1점씩 부여한다.

표 3의 질문을 통해 부여하는 점수 중 가장 높은 항목이 개발하려는 어플리케이션 데이터형태의 가장 근접한 데이터형태이며, 개발자는 각각의 필요한 데이터형태로 단말저장형 데이터는 DES 암호화 알고리즘, 일반전송형 데이터는 RSA 암호화 알고리즘, 실시간전송형 데이터는 ECC 암호화 알고리즘 사용하여 개발에 이용한다.

5. 결론

본 논문에서는 모바일 환경의 어플리케이션 유형별 암호화 플랫폼을 설계하였다. 이를 위해 모바일에서 이용되는 데이터의 형태를 단말저장형 데이터, 일반전송형 데이터, 실시간전송형 데이터로 정의하였고, 데이터의 형태에 맞는 암호화 알고리즘의 특징을 분석하였다. 또한 각각의 암호화 알고리즘을 모바일 메모리 사용량, 키의 크기, 보안성, 암·복호화 속도, 암·복호화 시 키 노출위험성, 일반 데이터의 크기에 대한 항목에 따라 객관적으로 비교·분석하였으며, 개발자가 자신이 개발하는 어플리케이션의 형태에 맞는 데이터 유형을 선택할 수 있는 알고리즘을 설계하였다.

제안하는 모바일 환경의 어플리케이션 유형별 암호화 알고리즘 선택 비교연구를 통해 개발하는 어플리케이션의 보안를 추가한다면 개인정보 유출 및 기타 보안관련 피해를 예방할 수 있을 것이다.

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] 장선진, "Android Security", 제 6회 공개 SW 역량프라자 정기기술 세미나, 2010.12
[3] 임웅택, 남길현, "DES 암호알고리즘의 안전성분석과 확장된 DES-like 암호알고리즘의 설계에 관한 연구", 정보보호학회 논문지, 1993.12
[4] 조동욱, 김영수, 정권성, "RSA 암호방식의 안전성에 대한 연구", 정보보호학회지, 1998.12
[5] 박석천, 김갑열, "모바일 RFID 서비스를 위한 ECC기반 경량화 암호 알고리즘 구현", 추계종합학술대회, 2008.11
[6] 윤성열, 조대균, 박석천, "모바일 환경에서 시나리오에 따른 암호 알고리즘 비교 분석 연구", 한국정보처리학회 춘계학술대회, 2011. 5
[7] 윤성열, 조대균, 박석천, "안드로이드 기반 데이터 암호화 플랫폼 설계 및 구현", 한국정보처리학회 춘계학술대회, 2012. 4