모바일 환경에서 시나리오에 따른 암호 알고리즘 비교 분석 연구

윤성열*, 조대균**, 박석천***
*, **경원대학교 전자계산학과
***경원대학교 IT대학
e-mail:scpark@kyungwon.ac.kr

Comparative Analysis of Cryptographic Algorithms by Scenario in Mobile Environment

Sung-Yeol Yun*, Dae-Kyun Cho**, Seok-Cheon Park***
*, ** ,***Division of Computer Science, Kyungwon University

요 약

모바일 환경의 발전 따라 어플리케이션의 수요 증가로 데이터 보안의 관심도가 높아지고 있다. 본 논문에서는 모바일 환경에서 시나리오에 따른 암호 알고리즘을 비교·분석하였다. 시나리오는 단말저장형 데이터, 단방향전송형 데이터, 실시간전송형 데이터로 정의하고 각각의 시나리오에 적합한 암호알고리즘을 분석하였다.

1. 서론

최근에는 통신속도의 발전과 각종 전자기기들간에 융합이 원활해지면서 현대 사회는 모바일단말 하나로 많은 업무가 가능하게 되었다. 이제 모바일단말은 단순히 무선 통신수단에서 PC의 기능까지 할 수 있는 단계로 발전하게 되어 핸드폰의 활용도가 증가되고 특히 핸드폰을 편리하게 사용하는 어플리케이션도 개발되고 있다[1].

이렇게 개발되는 어플리케이션은 긍정적인 기능을 제공하는 것 이외에, 개인 정보를 몰래 가져가거나, 핸드폰의 작동을 멈추게 하여 하드웨어까지 손상을 시킬 수 있는 어플리케이션도 있다. 이와같은 대표적인 개인정보유출 악성 앱으로 '재키 월페이퍼(Jackeey Wallpaper)가 있다. 이 악성 앱은 전화번호, IMEI, SIM 국가정보, SIM 시리얼 넘버, 보이스 메일 번호, 이메일 문자정보 등 대부분의 개인정보를 수집하여 사용자에게 피해를 주고 있고, 이와 같은 개인정보 피해는 점점 발전되어가고 있다[2].

개인정보 유출이 발생하는 것은 모바일 프로그램을 개발하는 사람들이 프로그램의 기능만을 고려하고 개인 정보보호 및 보안을 고려하지 않기 때문이다. 또한 단순히 보안의 필요성만 인식하고 암호화의 종류나 암호화를 하는데 필요한 속도나 암호화 강도 등에 대해서 잘 알고 있는 경우도 극히 드물다.

따라서 본 논문은 모바일에서 사용가능한 여러 암호알고리즘의 장·단점을 분석하고, 모바일 환경에서 발생할 수 있는 시나리오에 따라 사용하기 적합한 암호화 알고리즘을 비교 분석하고자 한다.

2. 관련 연구

일반적으로 암호알고리즘의 종류는 대칭키 알고리즘과 공개키 알고리즘이 있다. 대칭키 알고리즘과 공개키 알고리즘의 큰 차이는 복호화할 때의 복호화 키와 암호화 키의 동일함의 유무에 따라 나누어진다.

대칭키 알고리즘의 경우에는 암호화와 복호화가 동일한 키로 사용되고 동일한 방법으로 사용되는데, 간단한 수식(MOD, XOR, SHIFT)을 이용한다. 그렇기 때문에 암·복호화 속도가 매우 빠르다는 장점이 있다. 하지만 암·복호화 키가 동일해야한다. 이때 상대방에게 키를 전달하기가 매우 까다롭다. 그리고 암·복호화 키를 누군가가 알게 되면 다시 사용하기가 어렵다[3].

공개키 알고리즘의 경우에는 암호화 키와 복호화 키가 다르다. 복호화 키의 경우는 본인(A)만 비밀키를 가지고, 암호키를 공개키로써 다른 사용자(B)에게 공개한다. 다른 사용자인 B는 공개키로 A에게 전달할 데이터를 암호화하여 A에게 전달해준다. 최종적으로 비밀키를 가지고 있는 A만이 그 데이터를 알 수 있게 된다. 또한 공개키로 암호화를 한 B도 그 암호에 대해서 알 수가 없다. 이 공개키 알고리즘의 특징은 A+A를 구할 수는 있으나 A-A를 구할 수 없는 계산의 단방향성 특징이 가지고 있기 때문에 알고리즘을 사용하려면 기본적으로 복잡한 수학식(소인수분해, 타원곡선 등)을 사용한다. 따라서 복잡한 수식을 알고 공개키를 안다고 해도 암호화된 데이터를 해석하려면 굉장히 큰 시간이 소모된다. 즉, 보안강도에 있어서 굉장

* 경원대학교 일반대학원 전자계산학과 박사과정
** 경원대학교 일반대학원 전자계산학과 석사과정
*** 경원대학교 IT대학 정교수(교신저자)

히 높은 수준을 가지고 있는 것을 의미한다. 하지만 반대로 복잡한 식을 사용하기 때문에 계산하는 시간이 길고 자원의 소모가 크다는 단점을 가지고 있다[4].

표 1은 대칭키 알고리즘과 공개키 알고리즘을 비교한 표이다.

<표 1> 대칭키 알고리즘과 공개키 알고리즘 비교

	대칭키 알고리즘	공개키 알고리즘
기본 특징	XOR, MOD 등 간단한 연산	소인수분해, 타원곡선 등 복잡한 수학식
암호키 관계	암호키 = 복호키	암호키 ≠ 복호키
암호화 키	비밀	공개
복호화 키	비밀	비밀
암·복호화 속도	빠름	느림
키 분배	어려움	용이함
주요 알고리즘	DES, AES, SEED 등	RSA, ECC 등

3. 모바일 환경 시나리오 별 암호화 분석

모바일 환경은 사용자의 어플리케이션 실행 환경에 따라 3가지 시나리오를 가지고 있다.

첫 번째 시나리오는 스케줄러, 메모, 전화번호부, 시간표 등 사용자가 주로 모바일단말기에 데이터를 저장하는 경우이다. 이 경우에는 분실, 도난, 방치, 노출, 해킹 등의 위험을 받는다. 특히 개인정보가 많은 데이터이기 때문에, 암호화를 통하여 개인정보유출에 대한 예방을 할 수 있다. 단말저장형 데이터의 경우에는 대칭키 알고리즘의 약점인 인터넷을 통한 키 분배가 진행되지 않기 때문에, 단말저장형 데이터의 암호화 알고리즘으로는 대칭키 알고리즘이 적합하다. 또한 데이터의 크기의 상관없이 암·복호화가 진행되고, 공개키 알고리즘의 암·복호화의 속도보다 빠른 속도를 가진다. 대칭키 암호화 알고리즘은 기밀성, 무결성, 인증의 특징을 가지고 있다. 대칭키 알고리즘의 종류로는 DES (Data Encryption Standard), 3DES (Triple-DES), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm) 등이 있다[5].

두 번째 시나리오는 메일, 그림, 사진 첨부, 모바일뱅킹 등 단방향전송형 데이터의 경우이다. 이 경우는 무선통신, 인터넷 등과 같이 노출되기 쉬운 곳을 지나서 데이터가 전송되기 때문에 데이터가 해커 공격에 쉽게 노출될 수 있는 환경이다. 이 경우에는 암호 강도가 높은 암호화 알고리즘으로, 공개키 암호화 알고리즘인 RSA 알고리즘이 적합하다. RSA 알고리즘은 소인수분해의 어려움을 암호 알고리즘으로 만든 것으로, 1970년 후반에 만들어지고부터 전 세계적으로 지금도 많이 사용하고 있는 알고리즘이다. 현재는 RSA는 국제표준화기구를 비롯하여, ITU, ANSI, IEEE 등의 국제기구에 표준으로 제안되어지고 있는 안정화된 암호 알고리즘이고 1024bit의 암·복호화 키를 사용하고 있다. 이 암호 해독에 걸리는 시간은 슈퍼컴퓨터로 10년 이상의 시간이 소요된다. 또한 공개키 알고리즘은 키 분배에 있어서 용이하다는 장점을 가진다. 따라서 단방향 전송형 데이터 시나리오의 경우에는 RSA 알고리즘이 적합하다[6].

세 번째 시나리오는 단말대 단말이 실시간으로 데이터를 전송하는 경우이다. 음성통화, 채팅 등이 이에 속하는데, 이 경우에도 단말간 통신 환경이 외부에 노출이 되어 있어 도청에 의한 정보유출, 변조 등의 위험요소가 높다. 또한 실시간으로 진행이 되기 때문에 강력한 알고리즘과 빠른 암·복호화의 속도가 함께 요구된다. 이 시나리오에 적합한 암호화 알고리즘은 공개키 알고리즘인 ECC 알고리즘이다. ECC 알고리즘을 대칭키 암호알고리즘과는 다르게 키 분배가 용이하고 적은 키의 길이(160bit)를 가지고도 RSA(1024bit)와 동일한 암호화 강도를 나타낸다. 표 2는 각각의 시나리오에 따른 암호화 알고리즘의 비교표이다[7].

<표 2> 시나리오별 암호화 알고리즘 비교

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

4. 결론 및 향후 연구 과제

본 논문에서는 모발일 환경에서 시나리오에 따른 암호 알고리즘에 대해서 비교·분석하였다. 단말저장형 데이터, 단방향전송형 데이터, 실시간전송형 데이터일 때로 정의하고 적합한 암호화 알고리즘을 분석하였다. 또한 대칭키 알고리즘과 공개키 알고리즘의 장·단점을 비교하였고, 공개키 알고리즘 중 RSA 알고리즘과 ECC 알고리즘의 차이를 분석하였다. 단말저장형 데이터인 경우에는 대칭키 알고리즘이, 실시간 전송형 데이터에서는 ECC 알고리즘이, 단방향전송형 데이터는 RSA 알고리즘이 잘 어울리는 것을 확

인할 수 있었다.

향후 본 논문을 통해 모바일 소프트웨어를 개발 시, 소프트웨어의 시나리오별로 적합한 알고리즘을 적용하여 개발한다면 이용자들은 보다 편리하고 안심할 수 있는 소프트웨어 사용이 가능할 수 있다.

참고문헌

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

[2] 장선진, “Android Security″, 제 6회 공개 SW 역량프라자 정기기술세미나, 2010.12

[3] 정기훈, 노삼혁, “암호화 알고리즘이 웹 서버에 미치는 영향에 대한 연구”, 한국정보과학회 학술발표논문집, 2004.4

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

[5] 엄헌영, 강수용, 김현주, “대칭키/공개키 암호알고리즘의 키 길이 따른 안전도 비교 분석 및 관련 S/W 개발”, 정보통신연구진흥원 학술기사, 2001.1

[6] 조동욱, 김영수, 정권성, “RSA 암호방식의 안전성에 관한 연구”, 정보보호학회지, 1998.12

[7] 박석천, 김갑열, “모바일 RFID 서비스를 위한 ECC 기반 경량화 암호 알고리즘 구현”, 추계종합학술대회, 2008.11