김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제3호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 3 JUCHE105(2016).

웨브봉사에서 자료기지암호화를 위한 한가지 방법

김일광, 박광훈, 리충명

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《과학기술을 빨리 발전시키고 전민과학기술인재화를 실현하여 지식경제시대의 요구에 맞게 인민경제의 현대화, CNC화수준을 높이고 나라의 경제구조를 완비하여야 합니다.》

웨브봉사에서 자료보안을 실현하기 위하여 일반적으로 자료기지를 암호화하거나 웨브통신자료를 암호화하는 방법을 쓰고있다. 자료기지암호화는 스키마화일의 구조를 분석한데 기초하여 화일에서 리용하지 않는 구역을 객체접근암호설정과 객체암호화에 리용하거나 대칭암호화체계와 공개열쇠암호화체계를 결합하는 방법으로 진행한다.[1, 2]

한편 봉사기측과 말단측에 암호화코드와 복호화코드를 넣어 웨브통신자료들을 암호화하는 방법으로 웨브봉사에서의 보안을 실현하고있다.[3]

그러나 이러한 방법들은 암호화코드내용을 해석하는데는 주의를 돌리지 못하였으며 해석이 쉬운 웨브프로그람인 경우에 대처하기 힘들다.

특히 Java언어로 작성된 웨브응용프로그람인 경우 그 해석이 매우 쉬우므로 자료기지가 높은 강도로 암호화되였다고 해도 그 복호화코드가 Java언어로 작성된 경우 그 암호화는 믿음성을 잃게 된다.

그러므로 우리는 역코드가 쉬운 Java프로그람을 리용한 웨브봉사에서 자료보안을 실현하기 위한 방법을 제기하고 실현하였다.

1. JNI에 의한 복호화방법

JNI(Java Native Interface)는 JDK의 일부분으로서 JVM에서 실행되는 Java코드가 C언어의 함수들을 리용하게 하는 대면부이다.

자료기지를 암호화한 조건에서 그 복호화코드를 C언어로 작성한다면 설사 Java언어로 작성된 웨브응용프로그람의 원천코드를 해석하였다고 하여도 복호화코드를 알수 없으므로 자료기지암호화의 믿음성을 담보할수 있다.

이를 위하여 우선 C언어로 복호화함수를 다음과 같이 작성한다.

```
JNIEXPORT jstring JNICALL Java_com_ujuche_form_CodeUtils_
decodeString(JNIEnv* env, jobject obj_this, jstring content)
{
…
}
```

여기서 Java_com_ujuche_form_CodeUtils_decodeString은 Java언어로 작성되고 com.ujuche.form.CodeUtils라는 패키쥐로 묶어진 Java클라스에 decodeString이라고 선언된

함수의 실현부라는것을 나타낸다.

다음 Java언어로 복호화함수호출을 위한 대면부클라스를 다음과 같이 작성한다.

```
public class CodeUtils
{
    public static native String decodeString(String content);
    static
    {
     System.loadLibrary("CodeUtils");
    }
}
```

여기서 선언된 decodeString함수를 호출하면 우에서 C언어로 작성한 함수가 호출되여 실행된다.

C언어로 작성된 프로그람은 Windows조작체계에서는 DLL로, 리눅스계렬의 조작체계에서는 SO형식의 서고로 묶어진다.

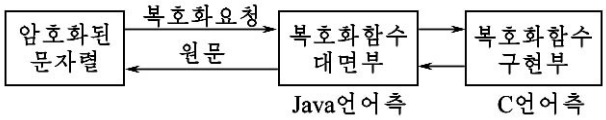

그림 1. JNI를 리용한 복호화흐름

이와 같이 원천코드가 공개되는 Java프로그람에는 복호화함수대면부만 선언하고 그 정의부는 C언어로 실현함으로써 복호화를 안전하게 실현한다.

JNI를 리용한 복호화흐름은 그림 1과 같다.

2. 웨브봉사에서 자료기지보안

우리는 Java언어로 작성된 자료기지암호화프로그람을 리용하여 자료기지를 암호화하였다.

다음 복호화를 위하여 C프로그람으로 된 복호화모듈을 작성하고 JNI를 리용하여 Java프로그람으로 되여있는 웨브봉사기측프로그람에서 이 모듈을 참조하도록 하였다.(그림 2)

이러한 자료기지암호화는 봉사기측의 코드해석여부에 의존하지 않고 암호화가 진행되는것으로 하여 안전한 암호화방식으로 된다. 우리는 이 방식을 리용하여 주체사상학습자료검색프로그람(봉사기용)에 도입하여 자료기지보안을 실현하였다.

웨브말단에서 웨브봉사기에 요청이 들어오면 요청을 접수한 봉사기는 복호화코드를 리용하여 암호화된 자료기지에 요청을 보내며 그 결과를 현시해준다.

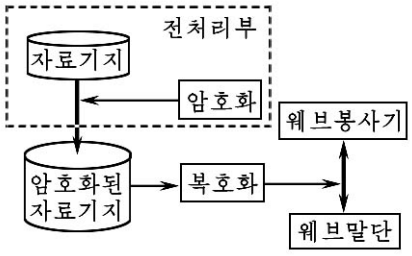

그림 2. 웨브봉사에서 자료기지 암호화체계의 구성도

이상에서 본바와 같이 우리는 암호화의 믿음성을 암호화알고리듬을 로출시키지 않는 방향에 중점을 두어 높이였다.

Java언어로 암호화모듈을 작성하여 리용하는 경우와 C언어로 작성하여 리용하는 경우

비교결과는 표와 같다.

표. 비교결과

모듈작성언어	알고리듬공개여부	복호화시간/s	
		길이가 255이하	길이가 255이상
Java언어	공개	0.01	0.02
C언어	비공개	0.01	0.023

맺 는 말

C언어로 암호화 및 복호화모듈을 작성하고 Java언어로 작성된 웨브봉사기측프로그람에서는 JNI를 경유하여 이 모듈을 리용함으로써 자료기지암호화를 실현하였다.

참 고 문 헌

[1] **김일성**종합대학학보(자연과학), 56, 8, 12, 주체99(2010).
[2] **김일성**종합대학학보(자연과학), 54, 9, 51, 주체97(2008).
[3] **김일성**종합대학학보(자연과학), 48, 6, 33, 주체91(2002).
[4] 任俊伟 等; 计算机应用研究, 7, 180, 2005.

주체104(2015)년 11월 5일 원고접수

A Method for DB Encryption in Web Service

Kim Il Gwang, *Pak Kwang Hun* and *Ri Chung Myong*

We made encryption and decryption module in C++ and then used this module in web server program in Java.

This method is useful for DB encryption in web service.

Key words: DB encryption, web service