S/W 개발 분석 단계에서 암호화

신성윤* · 진동수*** · 신광성* · 이현창**

*군산대학교 컴퓨터정보공학과

**원광대학교 정보전자상거래학부(융복합창의연구소)

***경인여자대학교 경영과

Legal System and Regulation Analysis by S/W Development Security

Seong-Yoon Shin* · Dong-Soo Jin*** · Kwong-Seong Shin* · Hyun-Chang Lee**

*Dept. of Computer Information Engineering, Kunsan National University

**Div. Of Information and Electronic Commerce(Institute of Convergence and Creativity)
Wonkwang University

***Dept. of Business Administration, Kyung-In Woman's University

E-mail : {s397220, waver}@kunsan.ac.kr, hclglory@wku.ac.kr, dsjin777@kiwu.ac.kr

Acknowledgement : "This research is partially supported by Institute of Information and Telecommunication Technology of KNU"

요 약

본 논문에서는 암호화에서는 중요 정보의 전송 또는 저장 시 정보의 기밀성과 무결성을 보장하여야 한다는 것을 제시한다. 암호화는 단방향 및 양방향 암호화를 적용하며 암호화 키는 안전성이 보장되어야 한다는 것도 제시한다.

ABSTRACT

This paper suggests that confidentiality and integrity of information should be guaranteed when transmitting and storing important information in encryption. Encryption should consider both one-way encryption and two-way one and that encryption key should assure security.

키워드

암호화(Encryption), 무결성(Integrity), 기밀성(Confidentiality)

Ⅰ. 서 론

암호화란 데이터 전송 시 타인의 불법적인 방법에 의해 데이터가 손실되거나 변경되는 것을 방지하기 위해 데이터를 변환하여 전송하는 방법이다[1]. 또한 암호화는 암호키를 이용해서 정보를 바로 해독할 수 없도록 변환하는 것으로 특정인만 해독할 수 있게 하는 것[2]이란 정의도 있다.

암호화에 관련된 연구로는 맵리듀스 기반의 분산 암호화 처리 방법[3], Java API에 포함되어 암호화 기능을 제공하는 JCA(Java Cryptography Architecture)를 이용하여 HDFS 암호화를 구현하고 성능 실험을 수행한 방법[4], 깊이정보 영상 콘텐츠를 숨기기 위한 암호화 방식[5]과 그 밖의 방법과 같이 다양한 분야에 걸쳐서 암호화를 수행하고 실험하였다.

Ⅱ. 암호화

1. 암호화를 위한 원칙

암호화를 적용하기 위한 대상 데이터는 사잔에 합의된 기준에 따라 식별되어야 하며, 암호화의

실행을 위한 알고리즘과 키의 강도 및 암호화 키 관리 요건은 명확하게 정의되어야 한다..

2. 암호화 대상 선정

암호화의 대상 선정은 그림 1과 같이 데이터의 등급 및 해당 데이터의 존재 양태에 따라서 정의한다.

데이터등급 / 암호화	DB 내 저장	어플리케이션 사용 시	네트워크 전송
1 등급	암호화	암호화	암호화
2 등급	일부 데이터 암호화	불필요	외부망:암호화 내부망:평문(전용선 사용)
3 등급	불필요	불필요	외부망:암호화 내부망:평문(전용선 사용)

그림 1. 데이터 암호화 기준 정의(예시)

3. 암호화 알고리즘 및 키 선정 기준

암호화의 유형별로 그림 2와 같이 사용 가능한 안전한 알고리즘의 목록과 해당 암호화 유형의 안전성을 보장하기 위한 최소한의 키 길이 및 형태에 대한 기준을 정의한다.

구분		알고리즘	최소 키 길이	
			1 등급 데이터	2 등급 이상 데이터
암·복호화	대칭키	AES, SEED, ARIA, TWOFISH	128	128
	비대칭키	RSA, ElGamal	2048	2048
	타원곡선	ECC-ElGamal	224	224
전자서명		DSS, DSA, RSA	2048	2048
해쉬		MD5, SHA-1, SHA-512	256	256
MAC		HMAC-MD5, SHA-1	256	256

그림 2. 암호화 알고리즘 및 키 채택 기준(예시)

4. 암호화 키 관리 기준

암호화 키의 안전한 관리를 위한 다음 그림 3과 같은 관리 기준을 정의한다.

키 관리 영역	키 관리 원칙 (예시)
키 생성(Generation)	모든 암호키는 승인된 알고리즘에 의해 생성 비밀키는 접근이 통제되는 설비에서 생성 마스터키와 세션키는 분리해서 관리
키 분배(Distribution) 및 등록(Registration)	분배를 위해 전송 중인 암호키는 유출, 변조되지 않고 수신자에게 전달 분배를 위해 전송 중인 키 재료(Keying Material)는 유출, 변조되지 않고 수신자에게 안전하게 전달 공개키를 등록할 때에는 그 무결성 및 신뢰성이 확인되어야 함
키 저장(Storage), 예비(Backup), 보관(Archive) 및 복구(Recovery)	모든 암호키 및 키 재료(Keying Material)는 운용 중 복구를 위해 적절한 백업이 이루어져야 함 유효기간 이후에도 복구가 필요한 암호키 및 키 재료(Keying Material)는 적절이 보관되어야 함 e.g. 서명 검증키, 키 암호화키, 마스터키 등
키의 삭제(Destruction) 및 폐기(Revocation)	폐기 예정 키의 모든 복사된 키는 삭제되어야 함 키가 등록해제 되기 전에 사용되었던 키 재료(Keying Material)는 삭제되어야 함

그림 3. 암호화 키 관리 기준(예시)

III. 암호화의 실례

암호화의 실례로서 암호화 프로그램 및 키 관리와 1등급 데이터의 암호화에 관한 상세 요건을 다음 표 1에서 설명하고 있다.

표 1. 암호화 프로그램 및 키 관리

요건 ID	요건명	번호	상세 요건
O-O-01	암호화 프로그램 및 키 관리	1	암호 프로그램은 담당자를 정하고 원시 프로그램은 봉인하여 별도로 보관한다.
		2	암호 및 인증 시스템에 적용되는 키에 대하여 주입, 운용, 갱신, 폐기에 대한 절차 및 방법을 마련하여 안전하게 관리 하여야한다.
		3	상용 암호화 솔루션 채택 시 국가 기관의 보안적합성 심의 제품 또는 CC 인증 획득 여부를 확인한다.

IV. 결론

암호화는 중요 정보의 전송 또는 저장 시 정보의 기밀성과 무결성을 보장하여야 한다는 것과 단방향 및 양방향 암호화를 적용하여야 한다는 것, 그리고 암호화 키는 안전성이 보장되어야 한다는 것도 제시하였다.

참고문헌

[1] http://terms.naver.com/entry.nhn?docId=932499&cid= 43667&categoryId=43667

[2] http://cafe.naver.com/handrake/46

[3] Hyun-wook Kim, Sung-eun Park, Seong-yul Euh, “The Distributed Encryption Processing System for Large Capacity Personal Information based on MapReduce,” J. Korea Inst. Inf. Commun. Eng., Vol. 18, No. 3, pp. 576~585, Mar. 2014

[4] Seonyoung Park, Youngseok Lee, “A Performance Analysis of Encryption in HDFS,” Journal of KIISE : Database, Vol. 41, No. 2, pp. 21-27, 2014

[5] Hyun-Jun Choi, “Data Encryption Technique for Depth-map Contents Security in DWT domain,” J. Korea Inst. Inf. Commun. Eng., Vol. 17, No. 5, pp. 1245-1252, 2013