암호화에서 보안 요건 정의

신성윤* · 김창호* · 장대현* · 이현창** · 이양원*

*군산대학교

**원광대학교

Definition of Security Requirement in Encryption

Seong-Yoon Shin* · Chang-Ho Kim* · Dai-Hyun Jang* · Hyun Chang Lee** · Yang-Won Rhee*

*Kunsan National University

**Wonkwang University

E-mail : {s3397220, over386, daihjang, ywrhee}@kunsan.ac.kr, hclglory@wku.ac.kr

요 약

암호화란 데이터 전송 시 타인의 불법적인 방법에 의해 데이터가 손실되거나 변경되는 것을 방지하기 위해 데이터를 변환하여 전송하는 방법이다. 중요정보(데이터) 전송 또는 저장 시 정보의 기밀성, 무결성을 보장하여야 한다. 암호화는 단방향 및 양방향 암호화를 적용한다. 암호화 키는 안전성이 보장되어야 한다.

ABSTRACT

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted. Important information (data) information during transmission or storage of the confidentiality, integrity should be guaranteed. Encryption is one-way and two-way encryption is applied. The encryption key must be guaranteed safety

키워드

encryption, hacking, integrity, two-way encryption

Ⅰ. 서 론

암호화란 의미를 알 수 없는 형식(암호문)으로 정보를 변환하는 것. 암호문의 형태로 정보를 기억 장치에 저장하거나 통신 회선을 통해 전송함으로써 정보를 보호할 수 있다[1].

모든 데이터를 수집해 분석하려다 보면 정작 중요한 데이터를 놓칠 가능성이 높아진다. 빅데이터 보안 기업들에게 가장 의미 있는 로그 중 하나는 암호화된 데이터다. 암호화 됐다는 것은 그만큼 기업/기관 내에서 중요하게 생각하는 내용을 담고 있을 가능성이 높다[2].

Ⅱ. 암호화를 위한 원칙

암호화를 적용하기 위한 대상 데이터는 사전에 합의된 기준에 따라 식별되어야 하며, 암호화의 실행을 위한 알고리즘과 키의 강도 및 암호화키 관리 요건은 명확하게 정의되어야 한다.

III. 암호화 대상 선정

데이터의 등급 및 해당 데이터의 존재 양태에 따라서 정의한다.

[데이터 암호화 기준 정의 (예시)]

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. 암호화 기준 정의

IV. 암호화 알고리즘 및 키 선정 기준

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

[암호화 알고리즘 및 키 채택 기준 (예시)]

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

V. 암호화 키 관리 기준

암호화 키의 안전한 관리를 위한 다음의 관리 기준을 정의한다.

[암호화 키 관리 기준 (예시)]

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 적절히 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

VI. 결론

암호화란 데이터 전송 시 반드시 필요한 기술로서 남의 불법적인 방법에 의한 데이터가 손실과 변경을 막기 위해 데이터를 변환하여 전송하는 방법이다. 암호화는 중요한 데이터의 전송이나 저장할 때 데이터나 정보의 기밀성과 무결성을 보장하여야 한다. 암호화는 단방향과 양방향 암호화를 모두 적용하고 암호화 키는 안전성이 있어야 한다.

참고문헌

[1] http://terms.naver.com/entry.nhn?docId=984473&cid=518&categoryId=518

[2] 손경호, “빅데이터 시대, 암호화 데이터가 가장 중요,” zdnet 기사, 2014. 4. 29