개인정보 암호화 기술에 관한 연구

김지현* ,이동훈*

*고려대학교 정보보호대학원

Survey on Personal Information Encryption Technology

Ji Hyun Kim* Dong Hoon Lee*

*Graduate School of Information Security,Korea University

E-mail : mmlpl@hanmail.net

요 약

개인정보 보호법 제2조는 개인식별정보, 비밀정보 및 바이오 정보 등을 개인정보로 정의하고 제29조에서 개인정보에 대한 불법열람 및 유출을 방지하기 위해 적정한 수준의 기술,적관리적, 물리적 안전조치를 취해야 하는 것으로 명시하고 있다 정보통신망법 제28조 제1항, 시행규칙 제9조, 방송통신위원회 고시에서도 이에 관해 규정하고 있다 이를 만족하기 위해서 개인정보의 안전성 확보조치를 취해야 하는 공공기관이나 기업들 등의 주체들이 기술적 조치를 적용하고이를 지속적으로 운영하고 관리하기 위해 적극적인 방안을 수립하고 실천해 나갈 것이 요구된다기술적 안전성 확보는 개인정보에 대한 암호화, 암호화키에 대한 안전한 관리와 운용, 개인정보 열람에 대한 접근제어와 감사를 제공하는 개인정보 보호수준을 도입함으로써 가능하다 이 논문에서는 개인정보의 기술적 안전성 조치로서 핵심요소인 개인정보의 암호화에 대해서 다양한 기술을 분석하고자 한다이는 개인정보 보호의 기술방안을 선택하는데 있어 도움이 될 수 있을 것이다

ABSTRACT

Personal Information Article2 defines personal authentication information, secret information, bio information for personal information and it is stipulated under article29 that the one who have duties must take adequate technological, administrative, physical measures to prevent from illegal reading and sneaking. Also it is stipulated under information communication network law28①, enforcement regulation9, Korea Communications Commitee notice. To satisfy this, the one who have to take security actions of personal information are required to take technological measures and establish positive measures to continuously manage it.The insurance of technological security is possible by encryption of personal information, secure management and operation of encryption key,taking personal information security level of providin access control of personal information reading and audit.In this paper, we will analyze various technologies of personal information encryption which are essencial component in technological security measuresof personal information. This paper will help choose which technological measures you should take in personal information security.

키워드

개인정보 암호화 기술, 시스템 계층별 개인정보 암호화, 개인정보보호법, 보안위협,안전성 확보 조치

* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정"지원사업의 연구결과로 수행되었음

Ⅰ. 서 론

개인 보호법은 제2조에서 개인식별정보, 비밀정보 및 바이오 정보 등을 개인정보로 정의하고 제29조에서 개인정보에 대한 불법열람 및 유출을 방지하기 위해 적정한 수준의 기술적, 관리적, 물리적 안전조치를 취해야 하는 것으로 명시하고 있다.[1] 정보통신망법 제28조 제1항, 시행규칙 제9조[2], 방송통신위원회 고시[4]에서도 이에 관해 규정하고 있다. 이를 만족하기 위해서 개인정보의 안전성 확보조치를 취해야 하는 공공기관이나 기업들 등의 주체들이 기술적 조치를 적용하고 이를 지속적으로 운영하고 관리하기 위해 적극적인 방안을 수립하고 실천해나갈 것을 요구한다. 기술적 안전성 확보는 개인정보에 대한 암호화, 암호화키에 대한 안전한 관리와 운용, 개인정보 열람에 대한 접근제어와 감사를 제공하는 개인정보 보호수준을 도입함으로써 가능하다. 데이터 암호화란 데이터 보안확보 유형 중 가장 일반화되어 있는 방식으로 기업내 저장되어 관리하고 있는 데이터를 인증 받은 암호화 알고리즘을 통해 암호화하는 데이터를 안전하게 관리할 수 있도록 하는 기술이다[3].이 논문에서는 개인정보의 기술적 안전성 조치로서 핵심요소인 개인정보의 암호화에 대해서 다양한 기술을 분석하고자 한다.이는 개인정보 보호의 기술 방안을 선택함에 있어서 도움이 될 수 있을 것이다.

Ⅱ. 시스템의 계층별 개인정보 암호화

1. 네트워크 계층의 개인정보 암호화

네트워크 계층에서는 서버와 서버 사이, 서버와 클라이언트 사이, 클라이언트와 클라이언트 사이에서 개인정보의 송신과 수신이 이루어진다. 응용 서버와 DB 서버 사이, 네트워크로 연결되는 저장장치와 서버 사이, 서버와 사용자 단말 사이 등의 통신이 이에 해당한다. 공격자는 통신채널을 도청하거나 감청하여 송수신 데이터를 수집함으로써 개인정보를 얻을 수 있다. 도청이나 감청으로부터 개인정보를 보호하는 방법은 송수신 데이터를 암호화하는 것으로서 두 가지 세부방법이 있다.

첫 번째 방법은 송신자와 수신자 사이의 통신채널 자체를 암호화하는 방법이다. 송신자와 수신자는 인증 기술로 상대방을 인증하고 키 교환 기술을 이용하여 암호화 통신을 위한 키를 상호교환함으로써 암호화된 채널을 생성할 수 있다. 송신자가 송신하는 개인정보 뿐만 아니라 개인정보가 아닌 모든 데이터를 암호화하게 되므로 효율성이 떨어질 수 있으나,개인정보를 송수신했다는 사실까지도 노출되지는 않으므로 일부 환경에서는 더욱 안전한 방법이 될 수도 있다.

두 번째 방법은 둘 사이에 송수신되는 데이터 중에서 개인정보만을 선택적으로 암호화하여 송수신하는 것이다.개인정보는 암호화로 보호하면서도 꼭 필요한 데이터에 대해서만 암호화를 수행함으로써 성능을 개선한 방법이다. 통신채널 암호화 방법과 거의 동일하지만, 개인정보만을 암호화하기 위한 선택적 암호화 기술이 요구된다.

네트워크로 연결되는 저장장치와 서버 사이에서는 서버와 서버 사이 또는 서버와 클라이언트 사이와는 다른 보안의 측면이 있다. 서버는 개인정보를 네트워크 저장장치로 전송하고, 개인정보를 수신한 저장장치는 저장을 하여 보관하게 되므로 보관되는 개인정보를 위한 암호화가 필요하다. 서버가 개인정보를 저장할 때, 네트워크 저장장치는 개인정보를 수신하여 암호화한 뒤 저장한다. 서버가 개인정보를 읽을 때에는 네트워크 저장장치가 암호화된 개인정보를 읽어서 복호화한 뒤 서버로 전송한다. 네트워크 저장장치를 위한 암호화는 다음에서 설명하는 OS계층의 개인정보 암호화 중에서 저장장치가 암호화를 수행하는 방법과 유사하지만, 네트워크를 통한 송수신에 기반하고저장장치가 DB서버와 분리되어 있음으로써 DB관리자와 보안관리자를 분리할 수 있고 암호화 키를 독립적으로 관리할 수 있는 장점이 있다.

2. Operating System(OS)계층의 개인정보 암호화

개인정보를 비롯한 모든 데이터는 컴퓨터에 저장될 때 파일의 형태로 저장된다. 데이터가 DB내부에 저장된다고 하더라도, DB의 내용 전체가 저장되는 것은 파일의 형태가 된다. OS가 파일시스템을 사용하여 파일을 저장장치에 저장하는 과정에 암호화 단계를 추가하는 것이 OS계층에서 이용할 수 있는 개인정보 암호화의 방법이며, 크게 3가지로 나눌 수 있다.

첫째, 저장장치가 암호화 기능을 탑재하여 OS가 파일을 읽고 쓸 때 저장장치가 암호화와 복호화를 수행하는 방법이다. 파일시스템이나OS는 파일이 암호화되었는지 여부를 알 수 없으며, 저장장치에 저장되는 모든 파일들이 암호화된다.

둘째,파일시스템이 암호화와 복호화를 수행하는 방법이다. 저장장치는 논리적으로 구분되는 복수개의 논리적 저장소로 구분되며 각 저장소는 서로 다른 파일시스템에 이해서 관리된다.파일시스템이 OS와 저장장치 사이에서 암호화와 복호화를 수행하기 때문에 OS나 저장장치는 파일의 암호화 여부를 인식할 수 없다. 저장장치나 파일시스템에서 암호화를 수행하는 방법은 저장장치의 분실이나 도난에도 개인정보를 보호하기 위해 제안된 방법이다.

셋째, 특정파일만 암호화하여 저장하는 방법이다. OS가 선택된 파일을 암호화하여 관리하는 방식이며 파일들의 집합인 디렉토리나 폴더 단위로 암호화하는 변형도 가능하다.

OS계층에서 개인정보 암호화를 적용하면 OS보다

상위계층에 있는 DB나 응용 프로그램은 데이터의 암호화 처리 여부를 신경쓰지 않아도 되므로 기존 시스템에 적용할 때 프로그램의 수정이나 변경이 전혀 없다는 점은 큰 장점이다. 그러나 이는 보안성의 관점에서 큰 한계를 가진다.

파일시스템이 암호화를 수행하거나 OS가 파일을 선택적으로 암호화하는 경우에 암호화 키는 사용자가 기억할 수 있는 패스워드로부터 변환되는 값을 사용하는 것이 일반적이다. 암호화 키를 모르는 공격자의 암호 해독 난이도를 고려하여, 대칭키 알고리즘의 키는 192비트나 256비트 이상이 권장되고 있다. 패스워드로부터 변환되는 키는 길이면에서 192비트나 256비트에 현저하게 부족하기 때문에 안전성을 담보하기 어렵다. 가령, 숫자나 영문자 8자리 정도로 정해진 패스워드를 사용한다면 수분 내에 암호화에 사용된 키를 얻고 암호화된 파일들을 복호화할 수 있다.이를 극복하기 위해 별도의 키관리 서버를 채용하여 암호화 키의 자유도를 보장하고 암호화 자체의 안전성을 높이는 방법이 가능하다. 그러나, OS계층에서 파일 단위로만 암호화가 적용되기 때문에 발생하는 근본적인 문제들을 해결할 수는 없다.

3. DBMS Engine계층의 개인정보 암호화

DBMS Engine은 DB서버의 내부에서 데이터의 입출력과 저장을 관리하는 기능을 담당하는 핵심 모듈이다. 많은 DBMS제품들은 자체적으로 암호화 기능을 제공하는데, Oracle사의 11g와 Microsoft사의 MS-SQL 200에 탑재된 TDE(Transparent Data Encryption)기술이 이에 해당한다. DB의 관리자(DBA)가 DB의 관리도구에서 암호화 옵션을 선택하면 DB에서 관리하는 데이터가 파일로 쓰여질 때 DB Engine에서 암호화를 자동으로 처리하는 방식이므로 DBMS를 이용하는 응용프로그램은 암호화 여부를 인지할 수 없다. 암호프로그램은 DB에 개인정보를 저장하거나 DB에서 개인정보를 읽을 때 암호화 적용 이후로 동일한 동작을 하기 때문에 기존 응용 프로그램은 수정될 필요가 없는 장점이 있다. 이러한 특징을 응용 프로그램에 대한 투명성(Transparency)라 정의하고 TDE라 부르게 되었다.

TDE방식은 DB의 내용을 파일 단위(MS-SQL)또는 테이블 단위(Oracle)로 암호화하여 저장하게 되는데, 서비스를 위해서는 암호화된 데이터 전부를 복호화하여 메모리에 두게 되므로 OS 계층의 암호화 방식과 동일한 데이터 유출의 위험을 안고 있다. 키관리의 측면에서, 암호화 키가 DB Engine에 의해 관리되고 데이터가 기록되는 DB파일과 함께 동일한 저장소에 저장되기 때문에 안전성의 위험이 존재한다. 암호화키를 저장할 때 마스터 키, 패스워드, 인증서 등을 이용하여 안전성을 높이기는 하지만, DB시스템의 서비스 가용성과 연속성을 위해 DB서버의 자동 설정으로 암호화를 해지할 수 있도록 운영되는 것이 보통이다. 이 경우, DB과 관리하는 파일들이 저장되어 있는 저장장치가 분실 또는 도난 당했을 때 저장장치 안에 존재하는 암호화된 데이터를 쉽게 복구할 수 있게 되므로 심각한 위험이 된다. 접근제어 측면에서, 응용프로그램을 이용하는 사용자에 대해서 IP와 MAC주소로 접근제어를 적용할 수 있어야 하지만 현재의 TDE기술은 이를 제공해주지 못하고 있다.

DBMS Engine계층에서 암호화를 적용하는 다른 방법은, DB Engine이 데이터를 읽고 쓰기 위해 저장소에 접근할 때 이를 매개하는 기능모듈인 Storage Engine을 추가 또는 수정하여 Storage Engine이 암호화와 복호화를 처리하는 것이다. 이 방식은 TDE방식과 마찬가지로 응용프로그램에 대한 투명성의 장점을 가진다.

TDE는 키관리, 접근제어, 권한 분리의 측면에서 많은 단점을 가지지만, Storage Engine을 이용하는 방식은 별도의 키관리 서버를 채용함으로써TDE의 단점을 해결할 수 있다. 키관리 서버가 암호화키를 별도의 저장소에서 안전하게 관리함으로써 암호화 키의 기밀성을 보장할 수 있고, 암호화된 데이터를 복호화하기 위하여 암호화 L를 요청할 때 IP나 MAC주소를 기반으로 사용자 인증을 함으로써 세밀한 접근 제어가 가능하다.

4. DBMS Package계층의 개인정보 암호화

응용프로그램이나 외부 서버로부터 데이터 추가 혹은 조회 등의 요청을 수신하여 해독하고 DB Engine이 데이터 처리 작업을 수행할 수 있도록 지시와 관리를 하는 기능들이 DBMS Package계층에서 이루어진다. 새로운 개인정보를 추가할 때 DBMS Package계층에서 암호화가 이루어지면, DBMS Package 계층보다 높은 계층에 존재하는 응용프로그램은 암호화되지 않은 개인정보를 사용할 수 있으므로 기존 응용 시스템에 적용할 때 응용프로그램을 수정하지 않아도 되는 장점이 있다. 또, DBMS Engine은 이미 암호화된 데이터를 받아서 저장하고 이를 조회하기 때문에DB서비스가 구동되는 동안 사용하는 메모리 공간에서도 암호화된 채로 존재하므로 OS계층이나 DBMS Engine에서의 암호화보다 보안성이 강화될 수 있다. DB파일이나 테이블 자체를 암호화하지 않아도 되며 DB테이블의 컬럼을 지정하여 암호화를 적용하는 방법도 가능하기 때문에 암호화가 필요 없는 데이터에 대해서는 암호화를 적용하지 않음으로써 전체 테이블이나 파일을 암호화하는 방식에 비해 성능면에서도 우수한 방법이다. DBMS Package계층에서의 암호화 적용을 위해 별도의 키관리 서버를 사용하여 보안성을 높일 수 있다. 키관리 서버를 이용함으로써 암호화키의 기밀성 IP나 MAC주소를 기반으로 한 세밀한 접근제어 권한 분리를 적용한 운영이 가능하다. 그러나, 개인정보 암호화 시장을 선도하는 기업들은 암호화된 데이터에 대해서도 빠른 검색이 가능하도록 인덱스 생성법을 제공하고 있다. DB서버에 개인정보가 추가되거나 조회될 때마다 암호화와 복호화가 필요하므로 연산을 수행하게 되는 DB서버에 부담을 줄 수 있는 단점도 있다. 그러나, 실제 환경에서 적절한 적용 방법을 선택함으로써 서버의 부

담을 줄일 수 있다.

5. DBMS Procedure계층의 개인정보 암호화

DBMS Procedure계층에 존재하는 소프트웨어는 응용프로그램으로 SQL문과 같이 DBMS의 API를 외부에서 활용한다. 이 계층에 특화된 암호화 방법은 응용 프로그램이 DB서버의 DBMS Package를 호출할 때 암호화를 적용하는 방법이다. 응용프로그램이 DB서버의 데이터를 이용하기 위해 DBMS의 기능을 직접 호출하는 것이 아니라 DBMS의 기능을 대행해 주는 모듈을 호출하고 모듈이 설정에 따라 보호가 필요한 개인정보를 암호화하거나 복호화한다.

기존 응용서비스로 운영되고 있는 응용프로그램은 DBMS Package를 호출하는 대신 새로운 모듈을 호출하는 것으로 수정되어야 하기 때문에 적용에 비용과 리스크 등의 부담이 따를 수 있다. 그러나,DBMS Package계층의 암호화 방법이 가지는 모든 장점과 암호화와 복호화를 처리하는 연산의 처리부담이 DB서버에 전가되지 않는다는 장점이 있다. 또한 응용서버 내에서 개인정보가 암호화 완료되어 DB서버로 전송되기 때문에 DB서버와 응용 서버가 네트워크로 연결되어 있는 환경에서도 네트워크 구간에서 발생할 수 있는 보안위험에 대비할 수 있다.

6. Web Application계층의 개인정보 암호화

최근의 많은 온라인 정보 서비스는 웹서버 웹 어플리케이션 서버, DB서버의 구성으로 이루어져 있다. 웹 어플리케이션 서버는 사용자에게UI를 제공하는 웹서버와 데이터나 정보를 제공하는 DB서버를 중개하는 기능을 하며 데이터의 흐름을 제어하는 역할을 맡는다. 웹어플리케이션 서버는 계층 모델에서 DBMS Procedure계층보다 상위에 존재하지만,DB서버와 연결하는 부분의 기능은 DBMS Procedure의 응용프로그램과 동일한 가능을 수행하기 때문에 웹 어플리케이션 계층의 암호화 방법은 DBMS Procedure계층의 암호화 방법과 동일하며 동일한 장단점을 가진다.

7. Business Application계층의 개인정보 암호화

Business Application은 응용시스템들 혹은 응용 프로그램들을 통합한 거대시스템인 경우가 많다. 이 계층에서 암호화를 적용하기 위해서는 내부 저장소를 관리하는 서브시스템을 수정하거나 서브시스템을 보조할 수 있는 새로운 서브시스템이 추가되어야 한다. 개인정보를 저장하여야 하는 서브시스템은 DBMS나 저장소를 관리하는 저장소 서브시스템에게 개인정보를 전송하게 되는데, 저장소 서브시스템을 수정할 경우에 저장소 서브시스템이 암호화를 수행하여 암호화된 개인정보를 저장하게 된다. 암호화를 전담하는 새로운 서브시스템이 추가될 경우,개인정보를 저장하여야 하는 서브시스템은 암호화 서브시스템에게 개인정보를 전송하고 암호화 서브시스템이 암호화한 개인정보를 저장 서브시스템에게 전송하게 된다.

Ⅲ.결 론

개인정보 처리자는 개인정보가 분실도난·유출·변조 또는 훼손되지 않도록 내부 관리계획을 수립하고, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적,관리적 및 물리적 조치를 해야 한다(제29조). 개인정보 보호를 위한 기술 중 "개인정보 암호화"는 가장 안전하고도 신뢰성 있는 방법이다. 개인정보 암호화는 상황에 따라 어떤 계층에서 암호화가 필요한지가 달라지며, 계층별 암호화는 암호화되는 계층에 따라 키기밀성/키 관리 보안, 접근제어, 관리 권한 분리적인 측면에서의 보안성 및 기존 시스템 변경 여부가 달라진다. 이를 잘 활용하여 점점 더 지능화, 고도화되고 있는 개인정보의 보안위협에 효과적으로 대응할 수 있는 방안을 강구하는 것이 바람직하다.

참고문헌

[1]이창범, 개인정보보호법, 법문사, 2012, p277

[2]김동례, 심기창, 전문석, "개인정보보호법을 대비한 개인정보보호 시스템에 관한 연구,정보보호학회지, 제21권, 2011, p17

[3]이병엽, 박준호, 김미경, 유재수, 데이터베이스 규제준수, 암호화, 접근제어 유형 분류에 따른 체크리스트 구현, 한국콘텐츠학회 논문지, 제11권, 2011,p64

[4]방송통신위원회 고시