인트라넷과 연동되는 데이터베이스의 암호화 모델 설계

임 재 흥
경기대학교 대학원 정보보호기술공학과

요 약

본 논문에서는 조직내의 인트라넷과 연동되는 데이터베이스를 암호화할 수 있는 모델을 설계하였다. 웹과 데이터베이스의 연동을 통해 기존의 클라이언트/서버 컴퓨팅 환경을 대체하려하고 있으며, 인트라넷과 연동되는 데이터베이스의 보안이 중요한 문제점으로 떠오르고 있다. 이에 인트라넷에 접속할 때 일반적으로 사용되는 인증수단인 ID와 패스워드를 통하여 암호화할 수 있는 암호화 키를 생성하고, 그 키를 통하여 데이터베이스 테이블의 정보를 암호화하는 모델을 본 논문에서 제시한다. 또한 그 키의 관리 방안을 제시한다.

Designing Database Encryption Models to interwork with Intranet

Im Jae Heung

ABSTRACT

This treatise deals with designing a database encryption model that interworks with Intranet within a system. Today attempts are being made to substitute legacy client/server computing environment with what interworks with web and database, and thus the question how the security for the database that interworks with Intranet can be secured is emerging as a matter of great importance. This treatise, therefore, offers an encryption model which offers how to create an encryption key using an ID and a password most widely used in Intranet access and by using this key, how to encipher information in a DB table, providing a maintenance scheme for the Key as well.

1. 서 론

인터넷의 급속한 확산과 수요자의 요구사항이 다양화함에 따라 웹을 이용한 응용들이 등장하게 되었는데, 그 중 표준화되어 있고 개방성을 가진 인터넷 기술의 특징을 살려 조직 내부의 업무 효율화에 활용하고자 하는 목적에서 등장한 것이 인트라넷(Intranet)이다.

인트라넷은 인터넷과 관련된 표준 기술을 기반으로 하여 조직 내부망과 전산 환경을 구축함으로서, 조직 내부의 업무 및 이에 따른 정보처리를 효율적으로 하고자 하는 조직내 네트워크 및 전산 환경으로 정의된다. 여기에서 말하는 조직 내부란 물리적이라기 보다는 외부망과 논리적으로 단절된 특정 조직에 속한다는 개념적인 의미를 가진다.

따라서 인트라넷은 동일한 네트워크를 이용하는 기업이나 단체 뿐만 아니라 지역적으로 흩어져 있는 지사, 대리점 등을 가진 업체 혹은 지방자치시대의 정부 공공기관을 위해서도 효율적인 전산 환경을 위한 도구가 될 수 있다.

개발 업체별로 별도의 기술을 사용함으로서 비개방성이라는 문제점을 가져왔던 기존의 그룹웨어와 달리, 인트라넷은 표준화된 인터넷 기술에 바탕을 둔 웹을 근간으로 하여 시스템을 통합하고 있다. 하지만 보안에 취약한 TCP/IP 프로토콜을 사용함으로 인해 효과적인 인트라넷의 구축에 있어 가장 필수적인 전제가 조직 내부의 전산 자원을 보호하기 위한 안정적이고 신뢰성있는 보안 기술의 확보로 나타나고 있다. 이와 같이 안정적인 보안성 확보와 함께 인터넷 기술을 바탕으로 인트라넷을 기업 또는 특정 조직에 구축함으로서, 내부의 정보 인프라 환경을 비용 경제적으로 구축함과 동시에 신속한 업무 처리와 부드러운 조직내 정보 흐름을 가능하게 한다.

웹을 이용한 조직내 문서의 온라인 검색 및 배포가 인트라넷을 탄생시킨 목적이 되었다면, 현재는 웹과 데이터베이스의 연동을 통해 기존의 클라이언트/서버 컴퓨팅 환경을 대체하려하고 있으며, 인트라넷과 연동되는 데이터베이스의 보안이 중요한 문제점으로 떠오르고 있다.

이에 본 논문에서는 인트라넷과 연동되는 데이터베이스에서 암호화하여 보안을 강화하는 방안에 대해 논의하고자 한다.

2. 인트라넷 보안

인트라넷 시스템의 보안을 적용하는데 가장 중요한 것은 무엇인가? 인트라넷 보안을 바라볼 때 중요한 세 가지 관점을 먼저 제시하고자 한다.

① 제도와 관리

인트라넷 보안 시스템은 먼저 보안이 필요한 업무를 분석하고 관련된 정보와 관련된 사람들을 분류하는데서 시작된다. 그리고 모든 보안 침해는 바로 사람으로부터 시작된다는 관점에서 사람을 관리하는 제도와 관리시스템을 구축하는 것이 필요하다.

이렇게 하기 위해서는 먼저 보안대상 정보의 보안등급분류가 필요하다. 보안이 필요한 정보와 그렇지 않은 정보 그리고 보안이 필요한 레벨을 구분하는 기준이 있어야 하며, 이를 근거로 정보의 보안등급을 매기는 작업이 선행되어야 하며, 해당 정보를 다루는 사람들의 등급을 매겨 해당 사용자의 사용등급을 관리하는 일이 보안에 있어서 중요한 첫걸음이 된다. 또 이런 보안 시스템을 제도적으로 관리하고 유지하기 위한 제도적 장치와 관리장치가 필요하다. 대부분의 기업들이 방화벽을 설치할 때 용역업체에서 초기에 한번 설치하면 끝이라고 생각하고 더 이상 관리하지 않는 실수를 범한다. 보안은 매

우 유기적이며 발전하는 것이기 때문에 보안점 담직원을 두는 것이 많은 비용을 들여 외부 컨설팅을 받는 것보다 훨씬 효과적이다.

② 시스템 보안

정보통신시대에서 인트라넷 시스템 보안은 특히 네트웍의 발달로 원격에서 네트웍을 통해 침입해서 불법적으로 인트라넷 시스템 및 그와 연동되는 데이터베이스 시스템을 사용하거나 파괴하는 일이 종종 일어난다. 일반적으로 말해서 해커라고 불리우는 외부의 침입자로부터 시스템을 보호하는 일이 필요하게 된다.

외부의 침입자는 주로 컴퓨터 네트웍 즉 일반적으로 인터넷에 연결된 컴퓨터시스템내의 시스템소프트웨어나 응용시스템의 보안허점을 이용해 불법적으로 계정을 얻고, 그 계정을 통해 수퍼유저의 계정을 획득해 시스템내의 정보를 취득하게 된다. 또 하나의 방법은 일반적으로 외부에서 로그인 접속해서 시스템을 사용할 때 누출된 패스워드를 이용해 정상적인 방법으로 시스템에 침입해 들어오는 방법도 있다. 이런 시스템에의 침입을 대비한 보안에는 방화벽, 침입탐지시스템, 취약점 분석 스캐너 등의 시스템들이 있다.

그러나 이런 시스템을 도입할 때 고려해야하는 요소들이 있다. 첫째는 시스템침입을 막기 위해 방화벽을 설치할 때는 그만큼 내부사용자도 불편함을 겪거나 시스템의 일부기능은 사용하지 못하게 된다는 점이 있다. 또 전체 네트웍의 속도도 약간 느려지게 된다.

③ 암호화

보안을 이야기하면 궁극적으로는 기업 혹은 어떤 기관의 정보를 권한이 없는 사람으로부터 누출되는 것을 방지하는 것이 가장 중요한 요소가 된다.

정보를 보호하기 위해 제도도 만들고 외부로부터 시스템에로 침입을 막기도 한다. 그러나 궁극적인 해결책은 바로 정보를 믿을만한 암호화기술로 암호화하는 방법이 바로 궁극적인 해결책이다. 방화벽이나 시스템 침입을 방지하는 기술들은 방화벽 내부의 시스템에 있는 정보를 보호하는데는 도움이 될 수 있을 것이다. 그러나 많은 정보들은 네트웍을 타고 이리로 저리로 흘러다닌다. 이런 흘러다니는 정보에 대한 보안은 어떤 방법으로도 확보하지 못한다. 그러므로 궁극적으로는 암호화기술을 이용해 보안위험이 있는 정보를 암호화해서 보호하는 것이다.

3. 데이터베이스 보안

3.1 데이터베이스 보안 위협

데이터베이스 보안에 대한 위반은 데이터의 부적절한 열람, 변경 또는 삭제로 이루어지며, 이러한 위반을 유발하는 사건을 위협(threat)이라고 한다. 따라서 위협은 데이터베이스 시스템에 의하여 관리되는 정보를 우연히 혹은 의도적으로 노출시키거나 변경하는 적대적인 행위라고 정의할 수 있다.

데이터베이스 보안에 대한 위협은 부적절한 정보의 노출, 부적절한 데이터의 변경, 서비스의 거부 등이 있다.

3.2 데이터베이스 보안 요구사항

보안 위협으로부터 데이터베이스를 보호하기 위해서는 우연한 혹은 의도적인 열람 및 변경으로부터 데이터베이스에 저장되어 있는 데이터를 보호해야 한다.

① 부적절한 접근 방지

부적절한 접근으로부터 데이터베이스를 보호하기 위해서는 승인된 사용자에게만 접근 권한

을 부여하여야 하고, 사용자 혹은 응용 시스템의 접근 요청은 데이터베이스 관리시스템에 의해서 검사되어야 한다.

데이터베이스에 대한 접근 통제는 운영체제에 의하여 관리되는 파일에 대한 접근 통제보다 더욱 복잡하다. 이는 데이터베이스 환경에서는 레코드(record), 애트리뷰트(attribute), 필드(field) 등과 같이 파일보다 세밀한 객체 접근 통제를 적용하여야 하기 때문이다. 또한 데이터베이스 내의 데이터는 의미적으로 상호 연관되어 있어 데이터에 직접 접근하지 않아도 이미 가용한 데이터 값을 이용한 추론(inference)을 통하여 다른 데이터의 값을 알 수 있다.

② 추론 방지

추론(inference)은 보통의 일반적인 데이터로부터 비밀 정보를 획득할 수 있는 가능성을 의미한다. 특히 추론 문제는 사용자가 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 하여야 하는 통계 데이터베이스에 많은 영향을 미친다.

③ 데이터베이스의 무결성 보장

데이터의 내용을 수정할 수 있는 인가되지 않은 접근, 그리고 저장 데이터를 손상시킬 수 있는 시스템 오류, 고장, 파업 등으로부터 데이터베이스를 보호하여야 한다. 이러한 유형의 보호는 적절한 시스템 통제, 다양한 백업 및 복구 절차, 임시적인 보안 절차 등을 통하여 데이터베이스 관리시스템이 수행한다.

시스템 고장시, 데이터베이스는 더 이상 일관성을 유지하지 못할 수도 있다. 일관성을 보존하기 위하여 모든 트랜잭션은 원자적(atomic)이어야 한다. 복구 시스템은 로그 파일을 사용한다. 각각의 트랜잭션에 대하여, 로그 파일은 데이터에 수행된 작업(읽기, 쓰기, 삽입, 삭제 등), 트랜잭션 제어 연산, 레코드의 수정 전후 값 등을 포함한다. 복구 시스템은 트랜잭션의 처리를 재수행할 것인지(redo), 혹은 무효화할 것인지(undo)를 결정하기 위하여 로그 파일을 사용한다. 임시적인 보안 절차는 인가되지 않은 수정, 변경, 삽입 및 삭제 등으로부터 데이터를 보호하기 위한 것이다. 이러한 보호 절차는 데이터베이스의 논리적 보안과 관련된다.

④ 데이터의 운영적 무결성 보장

트랜잭션의 병행 처리 동안에 데이터베이스 내의 데이터에 대한 논리적 일관성을 보장하여야 한다. 이러한 요구사항은 데이터베이스 관리시스템의 병행 수행 관리자에 의하여 보장된다. 병행 수행 관리자는 트랜잭션의 직렬성을 보장한다. 임의의 트랜잭션에 대한 병행 수행의 결과가 직렬 수행의 결과와 동일하면 트랜잭션의 수행은 직렬 가능하다고 하며, 이는 트랜잭션 수행의 정확성에 대한 기준이 된다.

서로 다른 트랜잭션이 동일한 데이터 항목에 동시적으로 접근하여도 데이터의 일관성이 손상되지 않도록 하기 위해서는 로킹 기법 등과 같은 병행 수행 제어 기법을 사용하여야 한다. 로킹 기법은 공유 가능한 데이터에 대한 접근을 상호 배타적으로 통제하는 병행 수행 제어 기법으로 데이터의 논리적 일관성을 보장한다.

⑤ 데이터의 의미적 무결성 보장

데이터베이스는 데이터에 대한 허용값을 통제함으로써 변경 데이터의 논리적 일관성을 보장하여야 한다. 데이터 값에 대한 이러한 제약조건은 무결성 제약조건으로 표현된다. 무결성 제약조건의 검사에는 많은 비용이 요구되므로, 적은 노력으로 검사할 수 있는 무결성 제약조건을 고려하여야 한다.

⑥ 감사

다양한 응용 처리에서 데이터베이스에 대한

모든 접근의 감사기록을 생성하여야 한다. 감사 기록은 데이터베이스의 무결성을 유지하는데 도움을 주며, 데이터베이스 접근에 대한 후속적인 분석을 가능하게 한다. 또한 추론에 의한 기밀 데이터가 노출되었는지를 판단하는 데에도 유용하다.

⑦ 사용자 인증

데이터베이스 관리시스템은 엄격한 사용자 인증을 필요로 한다. 또한 데이터베이스 관리시스템의 사용자 인증은 운영체제에서 수행하는 사용자 인증보다 더욱 엄격하여야 한다. 전형적으로 데이터베이스 관리시스템은 운영체제상의 응용 프로그램으로서 실행된다. 이는 운영체제와 데이터베이스 관리시스템 사이에 신뢰할 수 있는 경로가 없음을 의미한다. 따라서 데이터베이스 관리시스템은 사용자 인증을 포함한 각종 데이터를 운영체제로부터 수신할 때, 신뢰할 수 있는지의 여부를 점검하여야 한다. 따라서 데이터베이스 관리시스템은 반드시 별도의 사용자 인증 절차를 보유하여야 한다.

⑧ 비밀 데이터의 관리 및 보호

데이터베이스는 공개해서는 안되는 비밀 데이터를 포함할 수 있다. 비밀 데이터와 보통의 데이터를 혼합해서 갖고 있는 데이터베이스는 보다 복잡한 보호 문제를 야기시킨다. 데이터는 다양한 요인에 의하여 비밀이 될 수 있는데, 이러한 요인에는 원천적 비밀성, 선언된 비밀성, 비밀 출처로부터의 비밀성, 이미 노출된 정보와 관련된 비밀성 등이 포함된다.

비밀 데이터를 포함하고 있는 데이터베이스에 대한 접근 통제는 기본적으로 비밀 데이터의 비밀성을 보호하고, 인가된 사용자에 대해서만 접근을 허용하는 것으로 구성된다. 인가된 사용자는 비밀 데이터에 대한 일련의 운영 권한을 부여받지만, 이러한 권한의 양도는 금지되어야 한다. 또한 비밀 데이터를 사용하도록 인가된 사용자는 다른 사용자를 방해하지 않으면서 보통의 일반적인 데이터를 사용할 수 있어야 한다.

4. 암호화 키 관리

암호화하기 위해서는 암호화 키가 사용되는데, 키 관리(key management)는 키의 생성(generation)에서부터 분배(distribution), 갱신(update), 취소(revocation), 그리고 폐기(destruction)까지를 망라하는 개념이며, 이것 이외에도 키의 공유(sharing), 설치(installation), 저장(storage), 복구(recovery) 등의 부수적인 것도 포함된다.

키 관리의 궁극적인 목표는 비밀키 또는 개인키의 외부 노출, 키의 불법적인 변조 그리고 유효기간이 지났거나 이미 취소된 키의 불법적인 사용 등을 사전에 방지하기 위하여 키 또는 키와 관련된 정보들을 안전하게 유지하는데 있다. 따라서 키를 생성하고 사용하며, 마지막으로 폐기될 때까지 키를 안전하게 보호하기 위한 통제 지침이 마련되어야 한다.

키에 의해서 보호되는 정보의 유형에 따라서 다음과 같이 3개의 키로 분류된다.

4.1 암호화 키 분류

① 세션 키

일반적으로 메시지의 기밀성 또는 무결성을 유지하기 위해 비밀키 암호를 통한 암호화에 사용되는 키를 세션 키(session key)라고 한다. 보안상의 안전성을 높이기 위해서는 두 당사자들 간의 새로이 설정되는 매 세션마다 서로 다른 키를 사용해야 한다. 따라서 세션 키는 사용기간이 비교적 짧고, 상호간에 키를 갱신해야 하는 절차가 필요하다. 이를 세션 키의 설정 또는

분배라고 한다.

② 키-암호화 키

세션키의 설정 또는 설정된 세션 키의 저장에는 비밀키 암호시스템의 비밀키나 공개키 암호시스템의 개인키가 사용되는데, 이를 키-암호화 키(key-encrypting key)라고 한다. 일반적으로 키-암호화 키는 세션 키보다는 그 사용기간이 비교적 길고, 모든 사용자 들은 사전에 기밀성과 무결성이 보장되는 채널을 통해 제공받게 되고, 매 세션마다 새롭게 소요되는 세션 키의 설정에 사용된다.

③ 마스터 키

응용분야에 따라서 키-암호화 키 역시 다른 유형의 키에 의해서 보호될 수가 있는데, 이런 키를 마스터 키(master key)라고 한다. 마스터 키 자체에 대해서는 보안 관리자(security manager)에 의해서 마스터 키가 생성되고, 수작업으로 분배되고 초기화되는 절차상의 보호를 받는다.

위 키들의 관계는 아래 그림2와 같으며, 위에서 아래로 내려갈수록 키의 개수는 많아지고 사용기간은 짧아진다.

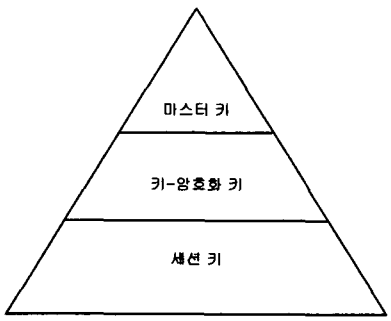

그림 1 키의 종류와 관계

5. 데이터베이스 암호화 방안

5.1 인트라넷과 연동되는 데이터베이스에서의 암호화 방안

인트라넷에 로그인하기 위해서 보통 인트라넷 시스템에 ID와 패스워드를 통해 인증받아 접속하게 된다.

인트라넷 시스템은 데이터베이스와 연결되어 사내의 수많은 정보를 저장하고 있다.

예로 제시하는 데이터베이스 테이블의 구성은 아래와 같다.

• 직원 정보 Table

구분	ID	패스워드	이름	주민등록번호
직원 A				
직원 B				
직원 C				

• 인사 Table

구분	급여	평가	근태	개인 신상
직원 A				
직원 B				
직원 C				

그림 2 데이터베이스 테이블 구성

위의 테이블 중에 인사 테이블은 암호화해서 저장하여, 보안 요구사항은 직원 상호간에는 내용을 볼 수 없어야 한다는 것이다.

데이터베이스 필드 암호화에 사용되는 키는 직원이 입력하는 ID와 패스워드의 조합에 의하여 생성되는 대칭키로 인사 테이블의 모든 필드를 암호화한다.

직원은 인사 테이블에서 그 직원에 대한 정보만 볼 수 있으며, 다른 직원의 정보는 볼 수 없다.

직원은 자신의 ID와 패스워드의 조합에 의하여 인사 테이블의 정보가 암호화되어 있기 때문

에, 로그인 시 입력되는 ID와 패스워드로 인사 테이블의 정보를 복호화 하여 그 정보를 볼 수 있으며, 직원의 ID와 패스워드를 알 수 없는 다른 직원들은 그 정보를 볼 수 없다.

직원이 인트라넷에 로그인 시, 직원은 ID와 패스워드를 입력하고, 입력받은 직원의 ID를 키로 삼아 테이블을 조회한다.

ID와 패스워드에 대한 해쉬 값을 산출하고, 이전에 해쉬 값이 산출되어 저장된 해쉬 값과 비교해서 일치하면 직원의 접근을 승인한다.

이때 예시로 제시한 직원정보 테이블은 아래 그림3과 같이 재구성되어야 한다.

• 직원 정보 Table (변경 전)

구분	ID	패스워드	이름	주민등록번호
직원 A				
직원 B				
직원 C				

• 직원 정보 Table (변경 후)

구분	ID	패스워드	••••	Hash(PW)	마스터키(PW)
직원 A					
직원 B					
직원 C					

그림 3 데이터베이스 테이블 재구성

직원의 패스워드를 해쉬한 값이 테이블에 추가되며, 직원의 패스워드를 데이터베이스 관리자의 마스터키로 암호화한 값을 테이블에 추가하여 저장한다. 그리고, 관리자의 마스터키는 관리자의 공개키로 암호화된다.

4.2 키 관리 방안

직원의 패스워드의 암호화에 사용되는 관리자의 마스터키의 관리는 스마트 카드를 사용할 경우와 사용하지 않을 경우로 나뉠 수 있다.

스마트 카드 사용할 경우, 스마트 카드 안에 패스워드 암호화에 사용되는 마스터키를 저장하고, 또한 마스터키는 관리자만이 알 수 있는 패스워드로 암호화한다. 스마트카드가 분실되었을 경우에 대비하여 똑같은 스마트카드를 생성하여 안전한 장소에 보관한다.

스마트 카드를 사용하지 않을 경우, 패스워드 암호화에 사용되는 마스터키를 지정된 서버에 파일 형태로 저장한다. 서버에 파일로 저장 시 관리자만이 알 수 있는 패스워드로 암호화한다.

파일이 손실되었을 경우나, 관리자가 바뀔 경우를 대비하여 암호화되지 않은 형태의 파일로 디스켓에 저장하고 안전한 장소에 보관하도록 한다.

두 가지 키 관리방안의 장단점은 아래의 표1과 같다.

<표 1> 키 관리방안 비교

구분	스마트 카드 사용	지정된 서버 저장
보안성	스마트카드 안에 저장되어 있는 마스터 키에 접근하기 위해서는 스마트 카드의 PIN(Personal Identification Number)와 마스터 키 암호화에 사용된 패스워드를 모두 알아야만 접근이 가능하기 때문에 보안성이 뛰어나다	지정된 서버의 위치만 알면 파일의 접근이 가능하기 때문에 스마트 카드 저장에 비해 보안성이 떨어진다. 다만 파일로 저장 시 파일은 관리자만 알 수 있는 패스워드로 암호화되어 저장된다
성능	마스터 키에 대한 RSA연산이 추가되므로, 조회 시간이 오래 걸린다	대칭키 방식의 암호화 알고리즘만 사용되므로, RSA 공개키 알고리즘 연산에 비해 조회 시간이 현저히 줄어든다
편리성	관리자가 스마트카드를 가지고 다녀야 하는 불편함이 있다	지정된 서버의 위치만 알면 되므로, 이동성이 편리하다

5. 결 론

본 논문에서는 조직내의 인트라넷과 연동되는 데이터베이스를 암호화할 수 있는 모델을 설계하였다. 인트라넷에 로그인하기 위해서 보통 인트라넷 시스템에 ID와 패스워드를 통해 인증

받아 접속하게 된다. 데이터베이스 필드 암호화에 사용되는 키는 직원이 입력하는 ID와 패스워드의 조합에 의하여 대칭키를 생성하고, 그 대칭키로 테이블의 필드를 암호화한다.

직원은 자신의 ID와 패스워드의 조합에 의하여 테이블의 정보가 암호화되어 있기 때문에, 로그인 시 입력되는 ID와 패스워드로 테이블의 정보를 복호화 하여 그 정보를 볼 수 있으며, 직원의 ID와 패스워드를 알 수 없는 다른 직원들은 그 정보를 볼 수 없다.

그리고, 암호화 키의 관리 방안으로 스마트카드를 사용하는 것과 지정된 서버에 저장하는 것으로 구분하여 보안성, 성능, 편리성 측면에서 장단점을 기술하였다.

인트라넷의 인증방법이 보통 ID와 패스워드로 이루어져 있어, 이것을 통하여 암호화 키를 생성하고, 암호화 모델을 제시하였다.

향후 PKI(Public Key Infrastructure)를 통하여 암호화 키를 생성하고 암호화 모델을 고려해 볼 수 있다.

참고문헌

[1] 한국전산원, 인트라넷 구축 및 보안 지침서, 1998

[2] 한국통신기술협회, 인트라넷 구축 지침서, 1998

[3] 이용석, 이한출판사, 인트라넷 구축 실무, 1997

[4] 한국정보보호진흥원, 교우사, 정보보호개론, 2000

[5] 이동훈, 이애듀넷닷컴, 정보보호전문가, 2001

[6] 유영남, 연세대, Intranet 구축을 위한 윌드와이드 웹과 데이타베이스 연동, 1997

임 재 홍

1997년 한남대학교 전자계산공학과 (학사)

2001년 동국대학교 정보보호학과 (석사)

2002년 ~ 현재 경기대학교 정보보호기술공학과(박사과정)