# 암호화와 PKI를 이용한 웹 어플리케이션 인증시스템

허 진 경*

**요 약**

최근의 해킹 동향은 해킹 방법이 더욱 복잡해지고 프로그램화 되며, 자동화 되었다. 과거에는 서버의 허점을 이용한 패스워드 크랙, 루트권한 뺏기 등이 주된 방법이었으나, 최근에는 네트워크에 대한 DoS 공격, 윈도우 시스템에 대한 DoS 공격, 바이러스 등이 주종을 이루고 있다. 그리고 특정 호스트를 대상으로 하기보다는 네트워크나 도메인 전체를 대상으로 하는 공격이 주를 이루고 있다. 또한 네트워크 규모가 커지고, 이에 대한 의존도가 높아지면서, 대량의 데이터들이 아무런 여과 없이 네트워크를 통해 전송되고 있다. 해킹 기술은 발전하고 데이터의 양은 증가하는 상황에서의 웹 어플리케이션 시스템 구축은 보안상 많은 취약점을 나타낼 수 있다. 뿐만 아니라 사용자수에 비례하여 네트워크를 통해 전달되는 데이터의 양이 많아지므로 보안 시스템에 심각한 병목 현상을 초래할 수 있다. 본 논문에서는 웹 어플리케이션 암호화 시스템에서 병목현상을 방지하고 PKI를 이용한 암호화/복호하시에 공개키 신뢰성 문제점을 해결하기 위한 시스템을 제안한다.

# Web Application Authentication System using Encipherment and PKI

Jin Kyoung Heo*

**ABSTRACT**

The hacking method came to be more complicated, became program ant it was automated. That is hacking trend of recent times. Before, The password crack, catch root authority is trend of hacking which uses the vulnerability of server. Hacker attack network or all of domain not some host. Web application system at hacking technique develops and improve transmitted data through the network shows many vulnerability. The massive data are transmitted through the network without encipherment filtering. It will be able to bring about the neck of a bottle actual condition which is serious in security system because of the network where the user comes to be many it leads and the data which is delivered comes to be many. In this paper, we propose web application system to prevent overload from bottleneck in encipherment system. It can solve security key trust problem in encoding and decoding with public key infrastructure.

Key words : Encipherment, PKI(Public Key Infrastructure)

* 호원대학교 사이버수사경찰학부 연구교수

## 1. 서 론

오늘날 해킹 툴의 발달로 필요한 지식수준이 갈수록 낮아져 시스템에 대한 상세한 지식 없이 정교한 공격이 가능해졌다. 최근의 해킹 동향은 해킹 방법이 더욱 복잡해지고 프로그램화 되며, 자동화 되었다. 뿐만 아니라 유닉스 서버에 대한 공격에서 MS사의 윈도우 시스템에 대한 공격이 많아지고 있으며, 과거에는 서버의 허점을 이용한 패스워드 크랙, 루트권한 뺏기 등이 주된 방법이었으나, 최근에는 네트워크에 대한 DoS 공격, 윈도우 시스템에 대한 DoS 공격, 바이러스 등이 주종을 이루고 있다. 그리고 특정 호스트를 대상으로 하기보다는 네트워크나 도메인 전체를 대상으로 하는 공격이 주를 이루고 있다. 네트워크 규모가 커지고, 이에 대한 의존도가 높아지면서, 데이터의 대량화가 이루어지고 있다. 이로 인해 개인의 정보 등 중요 데이터들이 암호화 없이 네트워크를 통해 전송되고 있다.

본 논문에서는 효과적인 암호화와 PKI를 위한 웹 어플리케이션 시스템을 제안한다. 제안한 시스템은 사용자의 요구를 처리하는 웹 어플리케이션 서버(WAS : Web Applicatjion Server)를 개인용(Private)과 기업용(Enterprise)으로 나누어 분산처리하였으며, 인증과 관련된 서버는 네트워크상의 DMZ와 분리하였다. 이로 인해 대량의 암호화 데이터를 처리하기 위한 WAS에서 어느 한곳이 데이터 병목현상으로 인한 서비스 지연이 발생하더라도 다른 WAS에는 영향을 주지 않게 된다. 또한 인증관련 서버를 DMZ와 분리하여 외부의 허가되지 않은 접근을 원천적으로 차단하여 보안을 한층 강화하였다.

## 2. 암호화

암호화 알고리즘은 크게 대칭키 알고리즘, 해쉬 알고리즘, 공개키 알고리즘이 있다. 대칭키 암호 알고리즘은 암호화 할 때 사용하는 키를 복호화 할 때 반대로 사용하면 복호화 되는 알고리즘이다. 메시지를 전송하는 송신측에서 사용하는 암호화키와 수신측에서 사용하는 복호화 키가 대칭을 이룬다고 해서 대칭키 알고리즘이라고 하며 비밀키(Secret Key) 방식이라고도 한다. 대칭키 암호 방식은 메시지를 보내는 송신측과 받는 수신측이 같은 키를 사용하여 암호화/복호화를 수행 한다. 대칭키 알고리즘은 다양한 알고리즘 개발이 용이하며, 안전성 검장방법이 비교적 정형화 되어 있다. 그리고 암호화 및 복호화 속도가 매우 빠른 장점이 있다. 그러나 키 관리 및 키 분배의 어려움이 있다. 그 이유는 Entry 쌍의 개수만큼의 키가 필요한데, N명의 사용자가 대화하기 위해서는 n(n-1)/2 쌍의 비밀키가 필요하다. 예를 들면 1천명의 사용자가 대화하기 위해서는 50만여 개의 키가 필요하게 된다. 뿐만 아니라 디지털 서명, 부인방지 등의 기능이 불가능하게 되고, 어느 한쪽이 키를 분실하면 시스템에 위험을 초래하게 되는 키 공유의 문제가 발생하는 등의 단점이 존재하게 된다. 대칭키 알고리즘은 주로 대용량 데이터 암호화에 사용한다.

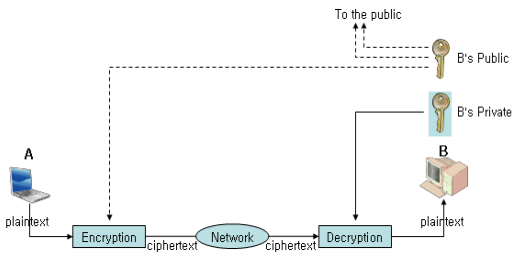
### 2.1 공개키 암호 방식

공개키 암호 알고리즘이 나타나기 전에는 대칭키 암호 알고리즘식이 사용되었다. 그러나 이러한 방식은 송신자의 비밀키를 사용하여 메시지를 암호화한 후 수신자에게 전달하는 방식으로, 수신자가 암호화된 메시지를 해독하기 위해서는 송신자의 복호화 키를 알고 있어야 한다. 따라서 이 방식은 복호화 키를 아는 사람은 누구라도 암호문을 복호화 할 수 있으므로 복호화 키를 수신자에게 전달할 때에는 각별한 주의가 필요하다.

이러한 단점을 극복한 방식이 바로 공개키 암호 알고리즘인데 이 방식은 복호화 키를 공유해야 하는 어려움을 해결하였다. 공개키 암호 알고리즘에

서는 암호화키와 복호화와 키 중 암호화키를 외부에 공개한다. 그러나 이 공개된 암호화키로 복호화 키를 알아낼 수는 없다. 따라서 공개키 암호방식을 이용하여 특정인에게 비밀 메시지를 보내고자 하는 사람은 공개된 특정인의 암호화키를 이용하여 메시지를 암호화해서 보낸다. 그러면 그 특정인은 자신만이 아는 복호화 키로 메시지를 복호화 할 수 있다. 이런 이유 때문에 공개키 암호방식에서는 암호화키를 공개키라고 부른다. 다시 말해서 공개키 암호방식은 암호화키와 복호화 키가 서로 다른 암호 방식을 말한다.

공개키 암호 알고리즘은 암호화 할 때 사용하는 키와 복호화 할 때 사용하는 키가 대칭을 이루지 않는다. 따라서 비대칭 키 방식이라고도 부른다. 공개키 암호 알고리즘은 비대칭이므로 1쌍, 즉 두 개의 키가 필요하다. 두 개의 키는 각각 공개키(Public Key)와 개인키(Private Key)로 부른다. 공개키는 인증기관을 통해 공개하는 키 이며, 비공개로 본인만이 소유하게 된다.




(그림 1) 공개키 암호 방식

(그림 1)은 공개키 암호방식을 보여주고 있다. (그림 1)에서는 송신측에서 암호화 할 때의 키와 수신측에서 암호화된 데이터를 복호화 하는데 사용하는 키가 서로 다르게 되어 있다. 공개키 암호방식의 경우는 키의 크기가 크고, 또한 각 키는 특수한 성질을 요구하기 때문에 비밀키 암호화 방식의 키와 같이 사용자가 직접 원하는 키를 만들지는 못한다. 많이 사용되는 공개키 암호방식의 키 크기는 높은 안전성을 갖도록 하기 위하여 현재 사용되는 공개키 암호 방식 보안 제품은 중 RSA는 1,024bits의 키를 사용하고 있다

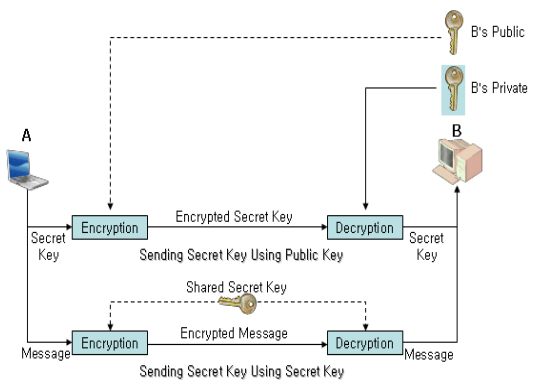
공개키 암호 알고리즘은 기밀성과 인증을 제공하며, 부인불가에 사용될 수 있다. 기밀성은 공개키는 인증기관을 통해 알 수 있으므로, 수신자의 공개키를 이용하여 메시지를 암호화 하면 수신자 외의 누구도 메시지를 복호화 할 수 없다. 즉, 사용자 A가 사용자 B에게 평문 메시지를 사용자 B의 공개키를 사용하여 암호화 하여 보내고, 사용자 B는 자신의 비밀키로 암호화된 메시지를 복호화 하여 평문 메시지를 얻는다. 사용자 B가 복호화에 사용되는 비밀키는 자신만이 가지고 있으므로 자신 외에는 아무도 자신의 비밀키로 암호화 된 메시지를 복호화 하여 볼 수 없다. 따라서 사용자 B만 메시지를 볼 수 있는 기밀성을 제공한다. 인증은 송신자가 자신의 개인키로 메시지를 암호화 하면 수신자가 송신자의 공개키로 복호화 하여 송신자에 대한 확인이 가능하다. 즉, 사용자 A가 사용자 B에게 평문 메시지를 자신의 비밀키를 사용 암호화 하여 보내고, 사용자 B는 사용자 A의 공개키로 암호화된 메시지를 복호화 하여 평문 메시지를 얻는다. 사용자 A가 암호화에 사용하는 비밀키는 자신만이 가지고 있으므로 자신 외에는 아무도 메시지를 암호화 할 수 없다. 따라서 암호화된 메시지는 사용자 A로부터 왔다는 인증을 제공한다. 이 경우에는 수신자를 제외한 제 3자(해커)도 복호화 할 수 있다.

공개키 방식의 특징은 서로 연관된 키 쌍(개인키/공개키)이 필요하고, 하나의 키로 암호화 한 경과는 반드시 쌍이 되는 키로만 복호화가 가능하다. 그리고 구조상 복잡한 수학연산이 필요하고, 안전성이 이러한 수학적 이론에 근거한다. 또한 N명의 사용자가 있으면 N개의 공개/개인키 쌍으로 충분하기 때문에 키 관리 문제를 해결 할 수 있다. 또한 서명기능, 기밀성 등의 기능이 가능하다. 그러나 공개키 방식의 단점으로는 동일한 양의 데이터를 암호화 시 대칭키 암호화에 비해 매우 느린데,

DES에 비하여 하드웨어 구현에서 1000배 가량 더 시간이 소요된다.

### 2.2 공개키와 대칭키 조합

공개키 방식은 기밀성 및 인증이 가능하므로 공개키 방식만 사용해도 된다. 그러나 공개키 방식은 암호 알고리즘이 복잡하여 연산속도가 느려지므로, 대용량 데이터를 암호화 하는 데는 부적절하다. 반면, 대칭키 방식은 빠른 속도로 데이터를 암호화/복호화 수행한다. 따라서 일반적으로 메시지는 대칭키 방식으로 암호화 하고, 비밀키만 공개키 방식으로 암호화 하게 되면, 효율적인 방식으로 암호화/복호화를 할 수 있다. 다음 (그림 2)는 A와 B사이에서 메시지와 비밀키의 암호화를 보여주고 있다.




(그림 2) 대칭키와 공개키 조합

(그림 2)에서 송신자는 수신자에게 보낼 메시지를 대칭키 암호 방식을 이용하여 암호화 한다. 이때 수신자가 메시지를 복호화 하기 위해 필요로 하는 키는 공개키 암호 방식으로 암호화 한 후 수신자에게 전송된다. 수신자는 자신의 개인키를 이용해 송신측에서 전송되어진 비밀키를 복호화 한다. 그리고 비밀키를 이용해 메시지를 복호화 하는 방법을 사용하게 된다. 이러한 방법을 사용하면 웹 어플리케이션에서 전송되어야 할 대량의 데이터는 대칭키 암호 방법을 통해 보다 빠르게 암호화 할 수 있고, 그 외에 비밀키 또는 기밀성과 인증이 요구되는 데이터는 공개키를 사용하여 암호화 할 수 있다.

## 3. PKI

PKI(Public Key Infrastructure)는 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하기 위한 복합적인 보안 시스템 환경을 말한다. 즉, 암호화와 복호화키로 구성된 공개키를 이용해 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템을 말한다.

데이터를 암호화하는 방법은 크게 공개키(비대칭키)와 비밀키(대칭키) 방식으로 구분할 수 있다. 비밀키 암호 시스템이 송수신자 양측에서 똑같은 비밀키를 공유하는 데 반해 공개키는 암호화와 복호화키가 다르다. 따라서 공개키방식은 데이터를 암호화하고 이를 다시 풀 수 있는 열쇠가 다르기 때문에 거의 완벽한 데이터 보안이 가능하고 정보 유출의 가능성은 그만큼 적어진다.

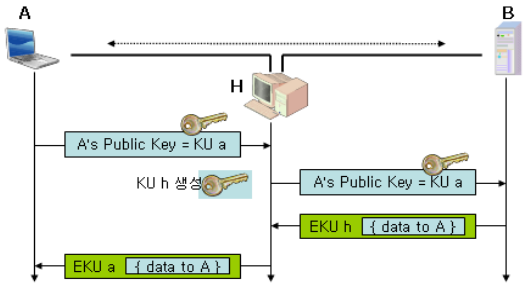
공개키 암호의 상용화를 위해서는 무엇보다 키의 생성과 인증이 필요하며 이런 것들의 분배와 안전한 관리를 위한 체계가 필요한데, 이런 시스템을 PKI라 하는 것이다. 여기에는 공개키에 대한 인증서를 발급하는 '인증기관', 사용자들의 인증서 신청시 인증기관 대신 그들의 신분과 소속을 확인하는 '등록기관', 인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 취소 목록 등을 저장·검색하는 장소인 '디렉토리', 또한 다양한 응용에서 공개키를 이용하여 전자서명을 생성하고 검증하며 데이터에 대한 암호, 복호를 수행하는 사용자 등이 포함된다.

PKI는 광범위한 기업 응용프로그램에 보안 솔루션을 제공한다. 솔루션은 웹 보안, 전자우편 보안, 원격접속, 전자문서, 전자상거래 어플리케이션 등 매우 다양한 분야에서 사용될 수 있다.

PKI를 도입하여 전자상거래를 할 경우, 전자상거래를 위해 전자서명을 한 뒤 공인인증기관의 인증을 받아 상대에게 제시함으로써 거래가 이뤄짐으로써 개인정보나 거래정보가 외부에 노출되지 않아 안전하게 거래할 수 있다.

### 3.1 공개키 신뢰

전자상거래에서 결제 시 거래 상대방의 공개키를 이용하여 결제 정보를 암호화하여 전송하게 된다. 그러나, 거래 상대방이 보낸 공개키가 과연 진짜로 거래 상대방일지 의심하게 된다.




(그림 3) 공개키 가로 체기

(그림 3)에서는 H는 A의 공개키를 가로채서 자신의 공개키로 바꾸어 B에게 전송한다. B는 이 공개키가 A의 것으로 알고 데이터를 암호화 해서 전송한다. H는 이 암호화된 메시지를 복호화하여 볼 수 있고, A에게 전송한다. A는 H의 공개키로 암호화 되어 있어 메시지를 볼 수 없게 된다. 이러한 이유로 공개키를 인증하는 인증기관이 필요하게 된다. 인증기관은 믿을 수 있는 기관이어야 하므로 인증기관을 관리하는 상위 인증기관이 필요하게 된다. 이러한 인증 시스템을 PKI라고 한다.

### 3.2 국내 공인 인증 체계

(그림 4)는 현재 국내 공인 인증 체계를 보이고 있다. 최상위 기관에는 정보통신부가 있다. 정보통신부에서는 법/제도의 정비, 국가 인증관리 체계 확립, 공인인증기관 지정 및 감독을 수행하고, 그 아래 루트 인증기관(Root CA)에는 한국 정보보호진흥원 산하 전자서명인증관리센터에서 관리하고 있다. 이곳에서는 국가인증체계 운영 및 공인인증기관 지정 심사, 공인인증기관 인증서 발급 등의 업무를 하고 있다. 그리고 그 아래에는 현재 6개의 공인 인증기관이 있는데 공인 인증기관에서는 이증업무준칙 제정, 공인 인증서비스 제공, 가입자 인증서 발급, 인증서 폐지 및 갱신 등을 담당하고 있다.


(그림 4) 국내 공인 인증 체계

인증기관을 대신하여 인증서 등록업무를 수행하고, 인증서 요청을 한 개인의 신원을 입증하고 확인하는 등록기관(RA)가 있는데, 이곳에서는 인증서를 발행할 수는 없지만, 사용자와 인증기관 사이의 중개인으로서의 역할을 수행한다.

인증서는 인증기관이 요청된 인감등록에 대하여 본인 확인 후 발행한 일종의 인감증명서로, 안전하게 컴퓨터 통신을 하기 위해 개인, 호스트 등이 자기 자신임을 증명하는데 사용한다. 일반적으로 X.509 v3 포맷을 따르는데 SSL을 포함한 많은 암호 프로토콜이 사용된다. 현재 국내의 최상위 인증기관 인증서 신뢰 목록 버전은 X.509 v1이다. 인증서에는 인증서 소유자의 인증에 필요한 여러

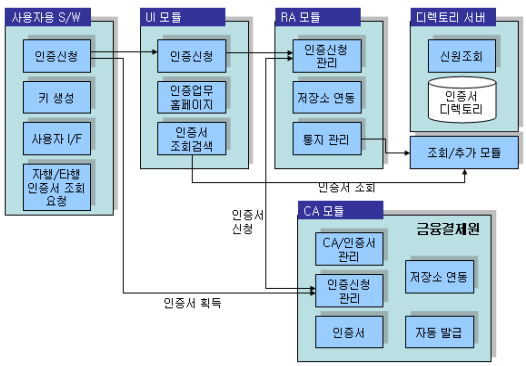
정보와 이 정보의 확실성을 보장하기 위한 인증기관의 서명이 포함되어 있다.

### 3.3 공개키 암호화의 문제

공개키를 암호화는 몇 가지 문재들을 내포하고 있다. 첫 번째, 공개키를 어떻게 얻어오는가? 두 번째, 이 공개키가 누구의 것인가? 세 번째, 이 공개키가 정말로 그 사람의 것인가? 네 번째, 공개키가 해커에 의해 공격당할 수 있는가? 등이 있다. 공개키 암호화의 문제 해결을 위해서는, 먼저 공개키를 LDAP과 같은 저장소(Repository)로부터 얻어옴으로써 공개키를 가져올 문제점을 해결 할 수 있을 것이다. 두 번째로 공개키가 누구의 것인가 하는 문제는 인증서의 Subject정보로부터 알 수 있다. 세 번째 해당 공개키가 자신의 것인지 확인은 믿을만한 CA를 이용하는 것이다. CA를 믿을 수 있다면 CA가 그 사람의 것이 맞다 고 인증하였으므로 믿는다.

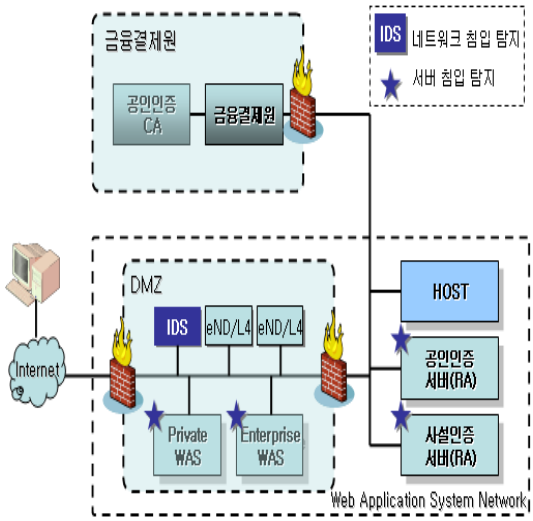
## 4. 인증시스템 구성

(그림 5)는 인증서 관리 시스템를 보이고 있다. 사용자 S/W에서는 UI모듈을 통해 인증서를 신청하면 UI모듈은 다시 RA모듈에게 인증서를 신청한다. RA모듈은 CA모듈의 인증서 신청/관리를 대신해 준다. 이로 인해 사용자용 S/W는 UI모듈을 통해 만들어진 인증서를 CA모듈에서 만들어진 인증서와 같은 인증서를 가질 수 있다. 인증서 조회 및 검색은 LDAP같은 디렉토리 서버 내의 저장소를 통해 이루어진다.




(그림 5) 인증서 관리

(그림 6)은 웹 어플리케이션 시스템에서 PKI를 이용하는 인증 시스템 네트워크 구성도를 보이고 있다. 사용자는 인터넷을 통해 WAS에 접근을 시도한다. 웹 어플리케이션이 존재하게 되는 WAS부분은 DMZ로 설정하여 보안을 한층 강화하기 위해 방화벽 및 침입탐지 시스템을 설정하였다. 클라이언트의 요구가 있을 때 방화벽을 통과한 후, WAS (Web Application Server)에서는 서버의 침입탐지 시스템이 가동된다. 마찬가지로 IDS를 통해 네트워크의 침입탐지 시스템도 가동하게 된데. WAS에서는 사용자 인증을 통해 인증 서버에 접속을 시도하게 된다. 이때에도 WAS는 인증서버 접속을 위해 방화벽을 통하도록 설정해 놓았다. 인증서버들은 각각 서버 침입탐지 시스템이 구축되어 있어야 한다.




(그림 6) 인증시스템 네트워크 구성도

## 5. 결 론

본 논문은 웹 어플리케이션 시스템에서 암호화와 인증을 위한 시스템의 구현을 제안하였다. 이를 위해 관련 암호화 기술의 소개와 PKI, 그리고 이들의 장/단점에 대하여 정의하였다. 이들을 바탕으로 하여 인증시스템의 네트워크 내부 구조를 설계하였다.

해킹 기술의 발전과 암호화 처리 데이터의 양은 증가하는 상황에서의 웹 어플리케이션 시스템 구축은 보안상 많은 취약점을 나타낼 수 있다. 뿐만 아니라 사용자수에 비례하는 네트워크 트래픽은 보안 시스템에 심각한 병목 현상을 초래할 수 있다.

본 논문에서는 웹 어플리케이션 암호화 시스템에서 병목현상을 방지하고 PKI를 이용한 암호화/복호하시에 비밀키 신뢰성 문제점을 해결하기 위한 시스템을 제안하였다. 제안된 이 시스템은 제안한 인증시스템에서는 인증 서버를 DMZ와 분리하여 외부로부터의 보안을 한층 더 강화하였다. 이로 인해 CA를 더욱 신뢰할 수 있고 이로 인해 공개키의 소유주를 분명하게 할 수 있다. 또한 WAS를 Private WAS와 Enterprise WAS로 분리하여 급증하는 데이터로 인해 병목현상이 발생하더라도 이와 관련되지 않는 다른 WAS가 제공하는 서비스에는 영향을 주지 않도록 하였다.

향후 연구 과제로는 메시지를 안전하게 전송하기 위해서 SSL, IPsec 등의 방법을 적용하여 VPN에서 보안 통신에 관한 연구가 필요하다.

## 참 고 문 헌

[1] 한국전산원, “웹 환경 구축 및 운영을 위한 보안 기술 연구”, NCA III-RER-97052, 1997.

[2] 김신규, 한광택, “안전한 웹 응용프로그램 개발에 관한 연구”, 2004.

[3] Nam-Deok Cho, Eun-ser Lee, Hyun Gun Park, “Security Intelligence : Web Contents Security System for Semantic Web”, KES, LNCS, ISBN 978-3-540-46537-9, Volume 4252/2006, pp. 819-828, 2006.

[4] 한국썬교육센터, “웹 어플리케이션 보안”, 2007.

[5] Roger Fournier저 유해영 역, “웹 어플리케이션 개발 방법론”, 이한출판사, 2002.

[6] Mike Shema McGraw-Hill Hacknotes, “Web Security Portable Reference”, Companies Inc, 2003.

[7] S. McClure, S. Shad, “Web Hacking : Attacks and Defense”, Addison Wesley, 2003.

[8] Saumil Shah, “One-way Web Hacking”, Addison Wesley, 2003.

[9] 정보통신부 한국정보보호진흥원, 웹 어플리케이션 보안 템플릿, 2006.

[10] 정보통신부 한국정보보호진흥원, 홈페이지 개발 보안 가이드, 2005.

[11] 과학기술부, 새로운 방식의 공개열쇠 암호의 제작과 기존 방식의 공개열쇠 암호의 연구, 2002.

**허 진 경**

1998년 호원대학교 전자계산학과 (이학사)

2000년 조선대학교 전산통계학과 (이학석사)

2004년 조선대학교 전산통계학과 (이학박사)

2006년 현재 호원대학교 사이버수사경찰학부 연구교수