

# SSL(Secure Socket Layer) 기반에서 향상된 정보보호 메커니즘의 설계

최성\*, 유성진\*, 김성열\*, 정일용\*

\*조선대학교 전자계산학과

e-mail : dory9241@stmail.chosun.ac.kr

## The Design of Improved Information Security Mechanism based on SSL(Secure Socket Layer)

Seong Choi\*, Seong-Jin You\*, Seong-Yeol Kim\*,  
Il-Yong Chung\*

\*Dept of Computer Science, Chosun University

### 요 약

SSL 프로토콜은 최근 네트워크 시스템에서 광범위 하게 사용되는 메커니즘중의 하나이다. 본 논문에서는 SSL 프로토콜을 기반으로 향상된 정보보호 메커니즘을 설계하였다. 여기에서는 네가지 중요한 정보보호 서비스를 제공한다. 첫번째는 SSL에서 제공하는 인증서를 이용한 인증서비스이고, 두번째는 DES 암호 알고리즘을 이용한 메시지 암호화 서비스이다. 세번째는 해쉬 알고리즘을 이용한 메시지의 무결성 서비스이고 네번째는 부인봉쇄 정보 서비스이다.

그러므로, 정보는 본 논문에서 특별히 설계된 부인봉쇄 서비스를 이용한 정보보호 메커니즘을 통해 안전하게 전송된다.

### ABSTRACT

The SSL(Secure Socket Layer) protocol is one of the mechanism widely used in the recent network system. The improved information security mechanism based on the SSL is designed in this paper. There are important four information security services. The first is the authentication service using the Certificate offered from the SSL(Secure Socket Layer), the second is the message confidentiality service using the DES encryption algorithm, the third is the message integrity service using Hash function, and the fourth is Non-repudiation service.

Therefore, information could be transferred securely under the information security mechanism including Non-repudiation service especially designed in this paper.

### I. 서 론

정보통신 및 전자기술의 발전<sup>[1]</sup>에 힘입어 현대사회는 과거 산업사회로부터 정보사회로 급속하게 진전되고 있다. 최근 그 발전 속도는 엄청난 가속력을 가지고 빠르게 진행되고 있다. 그 결과 과거에는 상

상조차 할 수 없었던 정보서비스<sup>[4]</sup>의 편리함과 효율성 그리고 신속성을 제공받고 있으며 이러한 결과는 컴퓨터 네트워크<sup>[6]</sup>를 통하여 모든 사람에게 전달 가능하게 됨으로서 누구나 문명의 이기를 공유할 수 있게 되었다.

최근에는 웹 및 자바<sup>[8]</sup> 등의 신기술을 이용한 정

보시스템의 구축 및 전자상거래<sup>[8]</sup> 등의 응용 서비스가 활발히 이루어짐에 따라 개인정보의 유출과 중요 정보의 악용을 제거하기 위한 정보보호 메커니즘<sup>[5]</sup>이 요구되고 있다. 정보보호 메커니즘에는 SET, IPsec, TLS, PCT, SSH, SSL등 여러가지 메커니즘이 있다. 이 중 SSL은 소켓을 기반으로 하는 메커니즘이기 때문에 소켓을 이용하는 어떤 응용 프로그램에도 SSL을 쉽게 적용 시키는게 가능하다. 그리고 근래의 인터넷 사이트에서는 SSL을 적용시켜 사용하고 있다.

인터넷과 같은 개방망 환경에서의 거래는 실환경에서와는 달리 많은 위협 요소들이 존재한다. 예를 들면, 신분의 위장이나 문서의 위조 개인 신상 정보의 노출 등이 이러한 것들인데 안전한 전자상거래를 구현하기 위해서는 이러한 위협들을 효과적으로 방어할 수 있는 장치를 필요로 하게 된다. 이러한 장치들이 만족해야 하는 요건들은 인증, 기밀성, 무결성, 부인방지, 익명성 및 중복사용방지<sup>[4]</sup> 등으로 요약할 수 있다.

네트워크상의 이러한 문제점들을 해결하기 위해 여러 가지 정보보호 서비스들이 제공된다. 즉, 정보보호의 중요성 및 인증, 암호화, 무결성, 부인봉쇄 등 여러 가지 정보보호 서비스들을 이용하여 이러한 정보보호 서비스를 제공하기 위한 방법론으로 여러 가지 정보보호 메커니즘들을 살펴본다. 그리고 응용 프로그램 개발 도구에서도 본 연구에 핵심이 되는 SSL<sup>[15,16]</sup>에서 제공하는 정보보호 메커니즘을 살펴보고 이것을 개선하여 향상된 SSL의 정보 보호 메커니즘을 설계한다.

## II 정보보호 메커니즘의 분석

### 1. 정보보호 서비스

정보보호 서비스<sup>[4]</sup>는 통상 물리적인 문서와 관련된 기능의 유형을 갖는 것으로 생각할 수 있다. 통신망에서 제공되는 기본적인 정보보호 서비스는 기밀성, 인증, 무결성, 접근제어, 부인봉쇄, 가용성이 있다.

### 2. 정보보호 메커니즘

서로 신뢰하지 않는 사람들간에서 제기되는 비밀성, 인증, 무결성 문제를 해결하는 기술이라 정의할 수 있으며, 크게 암호화 기술과 정보보호 프로토콜 기술로 나누어진다. 현재까지 암호기술 중에서 가장 많이 사용되는 기술은 통신보안의 핵심기술인 암호화 기술이다.

### 3 네트워크 보안 기술

네트워크 보안 기술에는 SET, IPsec, TLS, PCT, SSH, SSL등이 있다. 이를 간단히 설명하면, SET(Secure Electronic Transaction)은 인터넷과 같은 공개된 네트워크(Open Network)상에서의 신용카드 지불을 위한 Protocol이라 할 수 있다. IPsec은 데이터 인증, 패킷 무결성, 데이터 신뢰성, 응답보호, 암호화 키 자동 관리 및 SA(Security Association)등을 규정하고 있다. TLS는 두 개의 통신응용프로그램 사이에서 개인의 정보보호와 데이터의 무결성을 제공하기 위해 만들어졌고, TLS Record 프로토콜과 TLS Handshake 프로토콜로 구성되어 있고, PCT(Private Communication Technology)는 두 통신 응용간에 비밀보장과 적어도 하나(주로 서버)에 대한 인증 서비스를 제공하기 위해 설계되었다.

SSH(Secure Shell)는 rlogin, rsh, rcp, rdist와 telnet을 대체하기 위해 설계된 방식으로 안전하지 않은 네트워크 상에서 안전한 로그인 세션과 통신을 제공하는 응용이라고 할 수 있고, SSL(Secure Socket layer)은 Netscape사에서 개발된 프로토콜로 특정 응용을 위한 보안 프로토콜이 아닌 일반적인 인터넷 보안 프로토콜로 사용될 수 있다.

## III SSL(Secure Socket Layer) 분석

### 1. SSL Protocol의 소개

SSL은 Layer를 기반으로 하는 protocol이다. 각 layer의 메시지는 length, description, content field 들을 포함할 수 있다. SSL이 전송해야할 message를 가질 때, SSL은 그것을 제어 가능한 크기의 block으로 나누고, 선택적으로 data압축과정을 거친 후, 메시지 인증 코드(MAC : Message Authentication

Code)를 추가하고 암호화를 한 후, 결과를 전송한다. data가 도착하게 되면 복호화를 하고, 메시지 인증 코드를 verify한 후, 압축된 data를 원상태로 만들고, block을 재배열하여 얻어진 message를 상위레벨로 넘겨주게 된다.

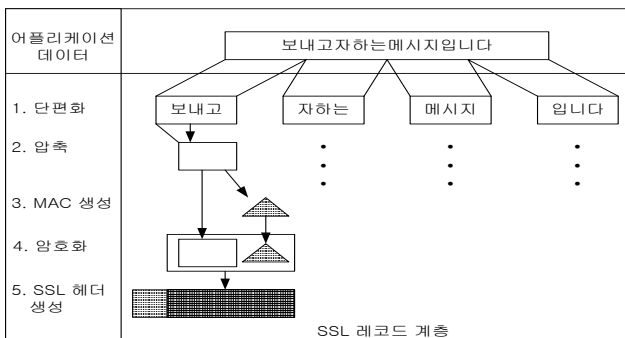
### 2. SSL의 구조

SSL은 크게 Record layer와 Handshake layer로 나누어 볼 수 있다. Handshake Layer는 암호화 방법이나 열쇠의 결정 및 협상을 담당하고, 크게 Change Cipher Spec Protocol, Alert protocol, Handshake protocol로 나누어진다. Record Layer는 change cipher spec, alert, handshake, application data의 네 가지 content type을 가질 수 있고, 데이터에 대한 정보와 실제 데이터가 들어가게 된다.

그 구조는 SSL Header와 SSL Body로 나누어진다. SSL Header에는 Message Type, 버전, 데이터 길이를 포함하고 있고 [그림1]과 같이 구성된다. SSL Body에는 [그림 2]와 같이 단편화, 압축, MAC 생성, 암호화과정을 거치게 된다.

Content Type(8bit)	Major Version(8bit)	Minor Version(8bit)
Compress Length(16bit)		
암호화 데이터		

[그림 1] SSL 데이터의 구조



[그림 2] SSL 레코드 계층

### 3. SSL의 정보보호 서비스

SSL 3.0이 지원하고 있는 정보보호 서비스는 암호화, 인증, 메시지의 무결성을 제공하고 있다. SSL에서 제공하는 인증에서는 클라이언트와 서버가 서

로 자신의 인증서(Certificate)를 교환하고, 각각은 자신이 받은 인증서에 기록되어 있는 유효기간, 서명을 확인함으로써 인증 과정을 거치게 된다. SSL에서 제공하는 암호화는 클라이언트가 이후에 수행될 암호화와 메시지 인증 코드(MAC : Message Authentication Code)의 생성에 필요한 난수(비밀키)를 생성하여 이것을 서버의 공개키로 암호화하여 서버에게 전송한다. 서비스를 받는 동안 사용할 암호화 알고리즘과 해쉬함수의 종류를 결정한다. 이 과정에서는 클라이언트는 자신이 제공할 수 있는 암호화 알고리즘의 리스트를 서버에게 제시하고 이들 중에서 하나를 서버가 선택하여 클라이언트에게로 보낸다. SSL에서 제공하는 무결성은 서버나 클라이언트가 자신이 수신한 메시지가 정말로 송신자가 보낼 때의 메시지와 똑같은 것인지를 확인하기 위해서는 키가 있는 암호학적 해쉬함수를 이용한다. 송신자는 메시지를 키를 이용하여 해쉬함수에 입력하여 그 결과인 일정한 길이의 데이터 (이것을 MAC이라고 부른다)를 보내려는 메시지와 함께 보낸다. 그러면 수신자는 수신된 메시지를 키를 이용하여 해쉬함수에 입력하여 그 결과를 자신이 수신한 MAC과 비교한다.

### 3.4 SSL에서 제공하지 못하는 서비스

SSL에서는 인증, 암호화, 무결성을 제공하고 있지만 부인봉쇄를 제공하고 있지 않다. 그래서 SSL에서 제공하지 못하는 부인봉쇄 서비스를 설계함으로써 향상된 SSL기반 정보보안 시스템을 설계한다.

## IV SSL기반 향상된 정보보호 메커니즘 설계

### 1. SSL기반 향상된 정보보호 메커니즘 설계

#### 1.1 Secrets 생성 및 전송

클라이언트는 pre\_master\_secret 생성 하고 이것을 서버의 공개키로 암호화 하여 서버에게 보내준다. pre\_master\_secret는 Client의 SSL버전(2 바이트)과 랜덤값(46바이트)으로 구성되고, 랜덤값은 안전하게 생성된 값이다. 그다음은 Client로부터 받은 pre\_master\_secret를 이용하여 master\_secret 생성한다. 그리고 마지막으로 실제

사용할 키를 생성한다. 여기에는 client-Mac-secret, server-Mac-secret, client-write-key, server-write-key, client-write-IV, server-write-IV 값이 생성된다.

### 1.2 향상된 SSL정보보호 메커니즘

본 논문에서 제안한 향상된 SSL정보보호 메커니즘을 설계한다. 여기에서는 클라이언트와 서버간의 상호인증, 메시지의 무결성, 비밀성, 부인봉쇄 서비스의 실현과정을 설명 하고자 한다.

먼저 상호인증은 인증기관에서 인증서를 발급 받아서 클라이언트와 서버가 서로 교환을 하기 때문에 상호인증이 이루어진다. 그 다음 클라이언트는 서버로부터 받은 공개키를 이용하여 MAC Secret, 공통키와 초기벡터 값에 사용될 Secret 값을 서버의 공개키로 암호화 시켜서 서버에게 전달한다. 이 과정으로 서로 메시지를 암호화시킬 수 있는 공통키를 교환한다. 그리고 해쉬함수를 이용하여 MAC을 생성한다. 이것은 메시지의 무결성을 검사하기 위하여 사용된다. 마지막으로 부인봉쇄 정보를 생성하는데 이것은 사용자의 uid, 호스트 이름, IP 주소로 이루어져 있다. 이렇게 생성된 MAC과 부인봉쇄 정보를 메시지와 함께 통신키로 암호화 시켜서 클라이언트는 서버에게 전달하고, 서버는 클라이언트에게 같은 방법으로 메시지를 전달함으로써 향상된 SSL정보보호 메커니즘을 실현 할 수 있다.

#### 1) Notation

- C : client
- S : server
- SK<sub>i</sub> : 노드 i의 비밀키
- PK<sub>i</sub> : 노드 i의 공개키
- Ver<sub>i</sub>: 노드 i의 버전
- CK<sub>i</sub> : 노드 i의 통신키
- Suite<sub>i</sub> : 노드 i에서 지원할 수 있는 암호화 알고리즘 리스트
- Message : Message Header와 Message Content로 구성됨
- N<sub>i</sub> : Random number와 Time stamp로 구성된 구조

체

- Message Header : 사용자에게 대한 정보 저장
- Message Content : 실제 데이터 부분
- MAC : Message Authenticate Code
- P : 사용자 P가 어떤 검증을 하기 위한 계산단계
- P → Q:M : 사용자 P가 사용자 Q에게 메시지 M을 보내는 교환단계
- (p, PK<sub>p</sub>)Cert<sub>i</sub> : 인증기관 i에서 발행한 p의 인증서
- pre\_master\_secret : SSL Version과 Random number로 구성된 구조체
- Pad : 길이를 맞추기 위한 Pad
- Msgs : ClientHello의 메시지부터 자기자신 메시지 전단계의 모든 메시지
- M : A || B : M은 A와 B로 구성되어 있다.
- {M}A : A를 암호화키로 하여 메시지 M을 암호화
- Master : pre\_master\_secret를 계산하여 생성된 Master키
- (M)Hash : 메시지 M을 Hash알고리즘으로 수행

#### 2) 알고리즘

##### (1) Connect

- C → S : C, Ver<sub>c</sub>, Suite<sub>c</sub>, N<sub>c</sub>
- /\* Suite<sub>c</sub>는 클라이언트에서 지원할 수 있는 암호화 알고리즘 리스트\*/*
- S → C : Ver<sub>s</sub>, Suite<sub>s</sub>, N<sub>s</sub>
- /\*서버의 버전 암호화리스트, 랜덤값과 타임스탬프로된 구조체 전달\*/*

##### (2) Certificate or KeyExchange

- S → C : {S, PK<sub>s</sub>}Cert<sub>CA</sub>
- /\*인증기관으로부터 서명된 인증서를 PEM방식으로 client에게 전달\*/*
- C → S : {C, PK<sub>c</sub>}Cert<sub>CA</sub>, {premaster\_secret<sub>c</sub>}PK<sub>s</sub>
- /\* pre\_master\_secret(48byte)를 서버의 공개키로 암호화시켜 서버에게로 전달\*/*

##### (3) ClientVerify

- C → S : {(Master + Pad2 + (Msgs + Master) Hash + Pad1)Hash}SK<sub>c</sub>
- Master : N<sub>c</sub> || N<sub>s</sub> || pre\_master\_secret<sub>c</sub>
- Msgs : Connect || KeyExchange

##### (4) Finished

- S → C : {(Master + Pad2 + (Msgs + S + Master + Pad1)Hash) Hash}Master

Master :  $N_c || N_s || \text{pre\_master\_secret}_c$   
 Msgs : Connect || KeyExchange || ClientVerify

C → S : {(Master + Pad2 + (Msgs + C + Master + Pad1)Hash)Hash}Master

Master :  $N_c || N_s || \text{pre\_master\_secret}_c$   
 Msgs : Connect

(5) Data Exchange

C → S : {Message<sub>c</sub>}CK<sub>c</sub>

/\* 통신키로 메시지를 암호화하여 전달 \*/

Message<sub>c</sub> : Message Header<sub>c</sub> || Message content<sub>c</sub>

Message Header<sub>c</sub> : Type<sub>c</sub> || MajorVer<sub>c</sub> || MinorVer<sub>c</sub> || CompressLen<sub>c</sub>

Message content<sub>c</sub> : {UID<sub>c</sub>, UID<sub>s</sub>, IP<sub>c</sub>, IP<sub>s</sub>, MAC<sub>c</sub>}SK<sub>c</sub> || Data<sub>c</sub>

S → C : {Message<sub>s</sub>}CK<sub>s</sub>

/\* MAC 검증 :  $MAC_c == MAC_s$  \*/

1.3 제안된 알고리즘 분석

클라이언트와 서버는 각각 자신이 가지고 있는 통신키와 DES 알고리즘을 이용하여 Message를 암호화하여 Message의 비밀성을 보장하고, 신뢰된 인증기관에서 인증서를 발급 받아서 클라이언트와 서버가 안전하게 인증서를 서로 교환함으로써, 클라이언트와 서버는 서로 신뢰 할수 있게 된다. 그리고 클라이언트는 해쉬함수를 이용하여 MAC 생성한후에 서버에게 전달하고, 서버는 클라이언트로 부터 받은 MAC과 자신이 생성한 MAC을 비교하여 같은 값이 나오는지 확인한다. 같은 값일 경우 메시지의 무결성이 검증 되는 것이고 그렇지 않을 경우는 위조 또는 변조되었음을 알 수 있다.

본 논문에서 특별히 제안된 알고리즘은 부인봉쇄를 추가함으로써 분쟁을 해결 할수가 있게 되었다. 기존의 SSL3.0에서는 부인봉쇄를 지원하지 못하기 때문에 클라이언트와 서버사이에 분쟁이 일어나도 해결을 하지 못한다. 그러나, 제안된 알고리즘에서는 클라이언트와 서버는 각각 부인봉쇄 정보를 생성하여 서로 교환함으로써 향후 분쟁이 일어나도 이를 해결 할 수 있게 된다.

V 결론

정보통신의 급속한 발전과 더불어 대부분의 컴퓨터들은 Internet등 각종 통신망으로 연결되어 있으며, 이러한 네트워크의 상호 연결을 통해 사람들은 생활에 편리함을 누리고 있다. 통신망에서 보내는 자료는 중요하지 않은 자료도 있지만 전자 상거래나, 인터넷 쇼핑, 홈뱅킹에서 사용되는 비밀이 보장되어야만 하는 중요한 자료가 오고갈 수 있다. 따라서 정보보호시스템의 이용확대와 함께 정보보호 사업이 크게 부각되었다.

정보보호의 중요성이 부각되고, 정보보호 산업이 정보통신산업에서 차지하는 비중이 높아짐에 따라, 본 논문에서는 정보보호의 중요성과 인증, 비밀성, 무결성, 부인봉쇄 등 여러 가지 정보보호 서비스들에 대하여 기술 하였다. 또한 정보보호 서비스를 제공하기 위한 방법론으로 여러 가지 정보보호 메커니즘들을 살펴보고, 이 중에서 본 논문의 핵심이 되는 SSL의 구조 및 정보보호 서비스를 분석하여 지금의 SSL3.0은 제한적인 정보보호 서비스를 제공하고 있다는 것을 밝혀 내었다.

따라서 본 논문은 SSL을 기반으로 한 클라이언트와 서버의 인증 및 클라이언트와 서버사이의 주고받는 메시지의 비밀성 및 무결성 그리고 부인봉쇄를 보장할 수 있는 SSL기반의 향상된 정보보호 메커니즘을 설계하였다. 제시된 정보보호 메커니즘의 장점은 다음과 같다.

첫째, 클라이언트와 서버는 각각 인증서를 교환함으로써 상호 인증을 할 수 있다.

둘째, 해쉬함수를 이용하여 메시지의 Digest를 생성함으로써 전송되는 데이터의 무결성을 보장할 수 있다.

셋째, 클라이언트와 서버간에 전송되는 메시지를 관용알고리즘인 DES를 이용하여 암호화함으로써 메시지의 비밀성을 보장한다.

넷째, 기존의 SSL3.0에서 지원하지 않는 부인봉쇄를 본 논문에서는 지원 가능 하다.

본 연구에서는 정보보호 서비스 중에서 비밀성, 무결성, 인증 및 부인봉쇄 서비스가 가능 하도록 설

계하였다. 향후에는 이를 직접 지원하는 시스템을 구현하고자 한다.

### [참 고 문 헌]

[ 1 ] 정태성, “안전한 데이터 전송을 위한 개선된 RPC기반 정보보호 메커니즘의 구현”, 조선대학교 대학원 석사학위 논문, 1997.

[ 2 ] 김미선·고영한·김도윤·서재현, “권한 관련성을 지원하는 망기반 접근제어”, 정보과학회지 제 26권 제1호, pp.494-496, 1999.

[ 3 ] 이임영·박춘식, “암호기법”, 정보과학회지 제 15권 제4호, pp.14-20, 1997.

[ 4 ] William Stallings, 통신망 정보보호, 그린출판사, 1996.

[ 5 ] William Stallings, 인터넷 보안, 도서출판비앤씨, 1996.

[ 6 ] 김화중, 컴퓨터 네트워크 프로그래밍, 홍릉과학출판사, 1997.

[ 7 ] 김건우·장희진·박보석·김상욱, “대규모 망에서의 계층적 보안 유지” 정보과학회지 제 26권 제1호, pp.506 ~ 508, 1999.

[ 8 ] 조은경·박정수·강신각·박성열, “SecWeb : S-HTTP 기반의 안전한 웹 시스템 개발” 정보처리논문지 제 5권 제12호, pp.3165 ~ 3175, 1998.

[ 9 ] 강창구·박진호·최용락, “통합 정보 모델을 이용한 접근제어 메커니즘 설계 및 구현” 정보처리논문지 제 4권 제9호, pp.2354 ~ 2365, 1997.

[10] 나선희·장승주, “Network Packet 관리 및 보안 도구 개발” 정보과학회지 제 26권 제1호, pp.485 ~ 487, 1999.

[11] 김윤기·이계영·김규식, “확장된 네트워크 보안 모니터” 정보과학회지 제 26권 제1호, pp.497 ~ 499, 1999.

[12] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY : Published by Jone Wiley & Sons, Inc., pp.234 ~ 560, 1996.

[13] JENNIFER SEBERRY·JOSEF, PIEPRZYK CRYPTOGRAPH: Prentice Hall of Australia

Pty Ltd, pp.1 ~ 60, 1989.

[14] 김철, 암호학의 이해, (주)영풍문고, pp.55 ~ 204, 1996.10.

[15] David Wagner·Bruce Schneier “Analysis of the SSL 3.0 Protocol” The Second USENIX Workshop on Electronic Commerce Proceedings USENIXPress : pp.29 ~ 40, 1996.

[16] <http://home.netscape.com/eng/ssl3/3-SPEC.HTM>, SSL 3.0 SPECIFICATION, 1996.

[17] <http://home.netscape.com/eng/ssl3/4-appn.ps>, SSL 3.0 APPENDIX, 1996.