SSL HANDSHAKE 보완을 위한 EKI(External Key Insert)기능의 구현

홍세영O, 박재필*
O(주)시큐위즈 기술연구소,
*(주)시큐위즈 기술연구소
e-mail: foxyfeel@secuwiz.co.kr*, hsykwb@naver.comO

AN Implement EKI system for TLS HANDSHAKE

se-young HongO, Jae-Pil Park*
OSECUWIZ CO. tech leb,
*SECUWIZ CO. tech leb

● 요 약 ●

본 논문에서는 SSL VPN 장비에서 사용되는 대칭키 교환을 위한 TLS HANDSHAKE 과정 중, 중간자 공격을 방어하기 위한 공유 대칭키를 별도로 주입하는 기능을 개발한다. 일반적으로 TLS 프로토콜은 공격자에 안전하다고 알려져 있으나 TLS 중간자 공격으로 대칭키가 노출될 위험이 존재한다. 또한 양자컴퓨팅의 발전으로 비대칭키 연산 역시 노출될 가능성이 대두되고 있다. 본 논문에서는 이렇한 공격들을 효과적으로 방어 할 수 있는 양자키분배기(QKD)로 부터 넘겨받은 양자키를 TLS HANDSHAKE 과정에 넣어 주어 이 같은 공격에 안전한 시스템을 구축할 수 있도록 구현한다.

키워드: 양자키(Quantum Key), SSL VPN, 중간자 공격(Man In the Middle attack)

I. Introduction

현재 국내 보안장비중 원격 접속을 안전하게 수행할 수 있는 장비로 SSL VPN 장비가 널리 사용되고 있다.이는 전통적인 VPN방식인 IPsec 과는 달리 VPN 터널의 수립에 TLS 방식을 사용하여 사용자 편의성과 VPN CLIENT의 다양한 환경을 지원 할 수 있어 사용량이 점점 증가하고 있는 추세이다.

본 연구에서는 이러한 SSL VPN에서 키교환에 사용되는 PROTOCOL인 TLS HANDSHAKE 과정에 양자키분배기(QKD)로 부터 공급받은 양자키를 주입하므로써 TLS 중간자 공격을 방어할 수 있는 기능을 구현 하고자 한다.

II. Preliminaries

1. Related works

1.1 국내 동향

양자컴퓨팅 기술이 발전함에 따라 국내 에서도 양자 난수 발생기나 양자내성 암호등 양자컴퓨팅 시대에 기존 암호 알고리즘을 보완하기 위한 움직임들이 생기고 있다.

실제로 양자 난수 발생기는 기존 보안장비들에서 난수의 randomness를 증가 시킬 목적으로 기존 시스템의 난수 발생기를 대체하여 사용되고 있기도 하다.

이에 원격접속 시스템으로 최근 가장 보편적으로 사용되고 있는 SSL VPN장비도 양자 난수 발생기나 양자 내성 암호를 지원하려는 움직임이 점차로 일고있다. 그러나 국내 공공 보안 시장의 특성상 암호알고리즘 검증 제도인 KCMVP와 암호장비 인증 제도인 CC를 준용하여야만 하는 시장 특성상 표준에 정의되지 않은 기능들을 상용화 할 수 없는 실정이다.

이에 본 연구에서는 KCMVP와 CC인증을 준용 하면서도 실질적으로 양자키를 보안장비에 응용하여 보안성을 강화하는 기능을 구현하고자 한다.

III. The Proposed Scheme

가. TLS 프로토콜

1) TLS 프로토콜의 개요

세션 연결의 제어하기 위해 사용된 TLS 프로토콜에는 3개의 부프로토콜 즉, handshake 프로토콜, change Cipher_spec 프로토콜, alert

프로토콜이 존재한다.

TLS handshake 프로토콜은 세션 파라미터들을 협의하기 위해 사용되고, alert 프로토콜은 오류 상황을 공지하기 위해 사용된다. change Cipher_spec 프로토콜은 세션의 암호학적 파라미터들을 교환하기 위해 사용된다.

따라서 클라이언트와 서버는 협상된 cipher_suite들로 준비된 보안 서비스들로 보호된 어플리케이션 데이터들을 교환할 수 있다.

이러한 보안 서비스들은 handshake로 협의되고 성립된다. TLS 프로토콜 스택은 다음 그림 1과 같다.

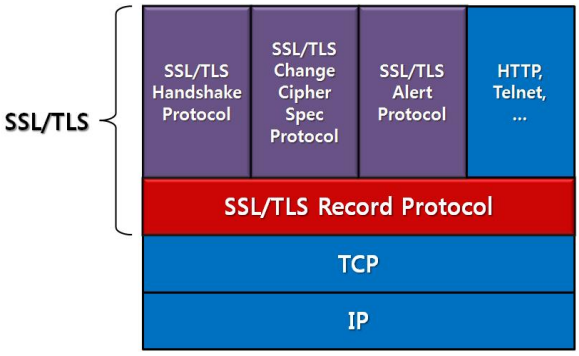

Fig. 1. TLS 프로토콜 스택

2) Handshake 프로토콜의 개요

Handshake 프로토콜은 클라이언트와 서버사이에 일련의 메시지 교환으로 이루어지며, 이 과정으로 클라이언트와 서버는 하나 이상의 보안 서비스 즉, 기밀성, 메시지 무결성, 인증, 재생방지를 형성할 수 있다.

따라서 클라이언트와 서버는 이것을 위해 알고리즘들을 협상하고 대칭키들을 유도하며, 데이터 해시와 같은 다른 세션 파라미터들을 설정해야 한다. 협상된 인증, 기밀성, 무결성 알고리즘들의 모음을 cipher_suite라 부른다.

아래 그림은 handshake 프로토콜 과정을 보여준다.

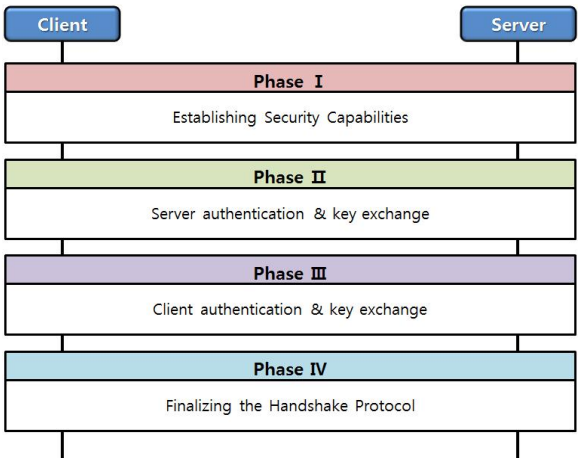

Fig. 2. Handshake 프로토콜 과정

3) EKI(External Key Insert)

해당 기능은 SSL VPN의 SSL Handshake 중 중간자 공격을 방어하기 위한 공유 대칭키를 별도로 주입하는 기능을 말한다.

SSL VPN은 server와 client연결을 위한 SSL Handshake과정을 거치며, 이때 나오는 session key를 기반으로 데이터 채널의 암복호화에 사용한다. 이 session key와 EKI키를 자체 인코딩과정을 거쳐 암복호화 키로 사용한다.

EKI를 사용하는 이유는 SSL Handshake 중 일어날 수 있는 취약점을 미연에 방지하기 위함이며, 기존 session Key와 EKI Key를 함께 사용하므로 보다 안전한 암복호화가 가능하다.

EKI는 server와 client가 각각 같은 키를 가지고 있어야 한다.

(server는 client를 인식 할 수 있는 유니크(인증서의 Common Name)한 값을 가지고 해당 Client의 EKI Key를 찾아서 암복호화에 사용한다)

EKI의 생성하는 방법에는 Key Delivery Server를 통해 받아오거나, 아래와 같이 자체적으로 생성 또는 별도로 제공한 Key를 사용한다

n EKI는 별도의 파일로 제공 되며, 해당 파일에는 10개의 Key가 있다

n EKI 생성 과정은 10개의 랜덤넘버를 HASH(sha256)하여 생성한다.

EKI Key 교체 주기는 Key Delivery Server 스펙에 또는 환경에 따라 다르며, 기본 제공에서는 교체 주기는 없다. 교체 주기가 없는 이유는 session Key가 주기적으로 변경 되므로 EKI Key를 변경할 필요성이 없기 때문이다.

IV. Conclusions

본연구의 목표는 국내에서 점차 활성화 되고있는 다양한 양자응용 보안기술들을 상용장비에 적용할 수 있는 방법을 모색함으로써 양자 보안기술들을 국내 인증 제도의 영향 받지 않고 적용할 수 있는 방법을 구현하는데 그 의의를 둘수있다고 하겠다. 본 연구가 국내 응용 보안 장비 및 프로그램들의 보안성 향상에 기여할 수 있을것으로 기대된다.

REFERENCES

[1] Korea Cryptographic Module Validation
[2] Transport Layer Security
[4] Common Criteria SO/IEC 15408