스트림 제어 전송 프로토콜의 보안에 관한 연구

조 은 경, 권 영 희
대덕대학 인터넷정보기술계열
ekcho@mail.ddc.ac.kr, yhkwon@mail.ddc.ac.kr

A Study of Security for Stream Control Transmission Protocol

Eun Kyung Cho, Young Hee Kwon
Dept. of Internet Information Technology, Daeduk College
ekcho@mail.ddc.ac.kr, yhkwon@mail.ddc.ac.kr

Abstract

This paper has been studied some security issues of stream control transmission protocol and designed some functional requirement for IPsec and IKE to facilitate their use for securing SCTP. In particular, some additional support in the form of new ID type in IKE and some implementation choices in the Ipsec processing to accomodate for the multiplicity of source and destination addresses associated with a single SCTP association.

I. 서론

IP 네트워크에서 TCP는 신뢰할 수 있는 데이터 전송을 위해 엄청난 서비스를 수행해 왔다. 그러나 최근 증가하는 응용으로 인하여 TCP는 너무 제한적이라는 것이 발견되었고 그로 인해 UDP의 상위 계층에 응용 자체의 신뢰할만한 전송 프로토콜을 통합시켰다. 많은 응용 중 IP 네트워크에서 PSTN signalling 메세지를 전송하고자하는 많은 연구가 진행되어TCP의 제약점을 극복하기 위한 스트림제어 전송프로토콜[1]이 제안되었다.

스트림제어 전송프로토콜은 PSTN signalling 메세지가 IP 네트워크로 전송되는 과정에서 PSTN에 비해 상대적으로 보안이 약하다는 점과 TCP가 비교적 서비스 부인공격에 약한 점을 고려하고 설계되어 블라인드 서비스부인 공격과 블라인드 가장 공격에 어느 정도 방어가 가능하나, 사용자 메세지 인증, 무결성 및 기밀성 기능에 있어서는 직접적으로 어떤 프로토콜도 제공하지 않고 설계되었다. 이와 같은 서비스를 제공하기 위해서는 IPsec 프로토콜과 스트림제어 전송프로토콜의 상위 응용 프로토콜의 보안기능과 구조에 의존하게 되는데 이 연구에서는 스트림제어 전송프로토콜의 보안 이슈와 IPsec 프로토콜을 스트림제어 전송프로토콜과 사용하는데 있어서의 고려되어야 할 이슈 등을 기술하고자 한다.

II. 스트림제어 전송프로토콜 및 IP 보안개요

스트림 제어 전송 프로토콜(SCTP: Stream Control Transmission Protocl)은 IP 네트워크 위에 PSTN 신호 메시지를 전송하기 위해 고안된 프로토콜로써 IETF의 SIGTRAN(Signalling Transport) 워킹그룹에 의해 표준화되었으며 RFC2960[1]으로 권고하고 있다. SCTP의 주요 특성으로는 신뢰성 있는 서비스와 TCP와 같은 연결지향 메커니즘 및 시그널링 전송을 위해 채택된 여러 가지 기능을 제공한다는 것이다. 또한 TCP처럼 엄격한 순서 보장을 원하지 않는 경우 옵션에 따라서 불필요한 지연을 방지할 수 있으며, TCP의 SYN에 의한 해킹에 보다 강한 매커니즘을 가지고 있으며, Multi-streaming과 Multi-homing을 지원하는 특성이 있다.

IP 보안[2]은 AH[3]와 ESP[4]프로토콜에 의하여 제공되며, 키의 교환은 IKE를 이용하여 제공한다. 그림 1에서 보는 바와 같이 AH 프로토콜에서는 IP 데이터그램에 대한 무결성과 인증서비스 및 선택적으로 재연방지 서비스를 제공한다. 또한 ESP 프로토콜에서는 무결성 및 인증, 그리고 암호서비스를 제공하며, 마찬가지로 선택적으로 재연방지 서비스를 제공한다.

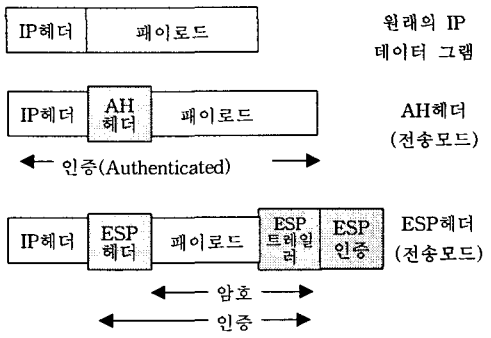

그림 1. AH와 ESP(전송모드)

AH와 ESP 프로토콜에서 사용될 각종 암호 키의 자동화된 생성 및 재생, 그리고 보안연계의 자동 생성을 위해 IKE[5,6]가 사용된다. IKE(그림 2 참조)는 두 단계의 협상으로 이루어져 1단계 협상에서는 마스터 키를 설정한다. 이 마스터키를 이용하여 모든 암호학적인 키가 사용자의 데이터 트래픽을 보호하기 위해 계속해서 유도되어진다. 일반적으로 통신 시스템사이에서 IKE 보안연계를 설정하고 2단계 협상에서 사용될 IKE메시지를 보호하기 위해 사용될 키를 설정하기 위해 공개키 암호가 사용된다. 2단계에서는 통신시스템간 사용자 데이타 교환을 보호하기 위한 보안연계와 키들을 협상한다. 이때 2단계에서 사용되는 IKE메시지는 1단계에서 생성된 IKE보안연계에 의해 보호되어진다.

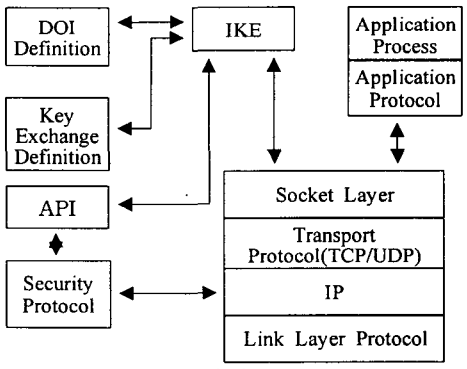

그림 2. IKE와의 관계

III. 스트림제어전송 프로토콜의 보안 이슈

SCTP는 TCP에서의 경험으로 설계되어 위조된 SCTP 다이어그램을 기존의 Association에 삽입하는 블라인드 공격에 강하도록 하나의 SCTP Association의 양측에서 32비트의 검증태그를 사용하여 데이터그램이 실제로 기존의 Association에 속한다는 것을 보증한다. 확립된 Association에 속하는 소스와 목적 트랜스포트 주소의 조합외에 타당한 SCTP 데이타그램은 또한 수신자에 의해 받아들여 지도록 올바른 태그를 갖어야만 한다.

TCP와 달리 Association 설정에서 쿠키의 사용은 SCTP에서 필수이다. 서버에 있어서 새로운 Association은 INIT, INIT-ACK, COOKIE-ECHO 청크를 포함하는 메시지가 교환된 후에 완전히 설정된다. 쿠키는 서버측에서의 Tranmission Control Block과 이를 안전하게 하기 위해 사용되는 HMAC을 초기화하는 모든 관련 데이터를 포함하는 가변길이의 매개변수이다. 이 HMAC은 쿠키와 안전한 서버 소유의 키에 대해 계산된다. 올바른 COOKIE-ECHO 청크가 클라이언트에 의해 수신되는 경우와 이 새로운 쿠키에 대해 계산된 HMAC이 쿠키에 포함된 HMAC과 일치하는 경우에만 새로운 Association에 대해 부가적인 자원이 예약되어질 수 있다. 공격자가 쿠키에 포함된 HMAC의 올바른 값으로 모든 실질적인 목적이 무시되는 2^{128}에서 1보다 작게 추축할 수 도 있으므로 SCTP에 있어서 공격자가 연결을 위조할 수 있는 가능성은 SYN-Cookies를 사용한 TCP의 경우보다 훨씬 적다.

SCTP는 사용자 메세지인증, 무결성 및 기밀성과 관련 되는 직접적인 어떤 프로토콜 메카니즘을 포함하지 않으므로 그런 기능을 위해서는 IPsec 프로토콜과 구조 그리고/또는 응용 프로토콜의 보안 기능에 의존하게 된다. SCTP를 사용한 트랜스포트 계층 보안은 항상 In-order 스트림을 사용해야만 한다. TCP 또는 SCTP는 설정된 세션이 공격자가 어느 한 쪽으로 부터의 트래픽을 관찰하여 자신의 패킷을 어느 한쪽으로 삽입하는 Man-in-the-middle 공격으로부터 보호되지 않는다. 또한 블라인드 연결/세션 설정 위조를 막기 위해 SYN-cookies를 지원하는 TCP 구현과 SCTP구현은 HMAC데이타를 보호하기 위해 서버가 아는 비밀키에 의존하게 된다.

IV. IP보안 프로토콜의 설계

IPsec 보안을 SCTP와 함께 사용하기 위해서는 몇 가지 IPsec 보안에 기능요구사항이 있다 이에 대한 설계를 하고자 한다. SCTP가 IP네트워크에서 사용될 때 무결성과 기밀성을 위해 IP보안프로토콜을 활용할 수 있다. 동적으로 IPsec Security Association (SA)를 설정하기 위해서는 IKE와 같은 키 협상 프로토콜이 사용될 수 있다.

4.1 SCTP와 IPsec

AH 또는 ESP프로토콜을 활용하여 보안서비스를 제공할때 SCTP 프레임 또한 IP위에서 또 하나의 트랜스포트계층 프로토콜로 처리된다. IPsec구현은 이미 보안정책 데이타베이스(Security Policy Database : SPD)의 선택자로 IANA에서 할당된 SCTP 트랜스포트 프로토콜 번호를 사용할 수 있어야 하며, SPD에서의 선택자로 SCTP 소스 및 목적지 포트번호를 사용하는 것이 가능하여만 한다. 트랜스포트 헤더의 포트 개념과 이것의 위치가 프로토콜에 따라 다르므로 트랜스포트 프로토콜 포트를 식별하는데 책임이 있는 IPsec코드는 적절히 수정되어야만 한다.

SCTP는 하나의 Association 문맥에서 사용될 수 있는 소스 및 목적지 주소의 집합을 협상할 수 있으므로 SPD가 이를 수용할 수 있어야만 한다. 직접적이며 고비용의 방법은 협상된 소스/목적지 주소의 각 쌍에 대해 하나의 SPD목록을 생성하는 것이며, 좀더 나은 방법은 주소들의 집합을 각 SPD목록의 소스와 목적지 선택자들과 연결시키는 것이다. SCTP에 맞게 선택자를 수용하기 위해 SPD를 설계하거나 수정할 때 개발자는 이를 따르던지 비슷한 접근을 하여야 한다. 비슷하게 SA들이 복수의 관련된 소스와 목적지 주소를 갖을 수 있다. 그래서 하나의 SA는 ({목적지주소의 집합}, SPI, 보안 프로토콜)로 확장되어 식별되어진다. 목적지주소가 협상된 상대방 주소중의 하나인 (목적지주소, SPI, 보안프로토콜)을 사용하여 보안연결 데이타베이스(Security Association DB:SADB)를 검색하는 경우 동일한 SA를 반환해야만 한다.

다음으로 터널모드로 동작할 때 터널 목적지 주소로 어떤 것을 사용하는 가에 대한 문제가 제기될 수 있다. 세 가지 경우가 있을 수 있는데 End 호스트가 또한 터널 Endpoint인 경우, 어떤 호스트도 터널 Endpoint가 아닌 경우(터널 Endpoint가 보안게이트웨이인 경우), 호스트중의 하나가 터널 Endpoint인 경우이다. 첫 번째 경우 바깥쪽 주소가 터널의 안쪽 주소와 같아야만 하며, 보안게이트웨이인 두 번째 경우 특별한 처리 없이 두개의 서로 다른 End 호스트를 위한 것과 마찬가지로 주소선택이 진행된다. 세 번째의 경우 터널 목적지 주소로서 보안게이트웨이의 주소를 사용하며, 안쪽의 패킷 주소와 동일한 소스주소를 사용해야만 한다. 대칭적으로 보안게이트웨이는 자신의 주소를 터널의 소스주소로 사용하고, 바깥쪽 헤더에 있는 동일한 목적지 주소를 내부패킷의 주소로 사용한다.

4.2 SCTP와 IKE

SCTP 트래픽에 대한 보호를 위해 협상할 때 IKE 사용과 관련해서는 두 가지의 이슈가 있다

○ SCTP는 복수의 소스와 목적지 네트워크 주소를 하나의 SCTP Association과 연계시키는 것을 허용하므로, IKE가 이들을 2단계 Quick mode 교환에서 효율적으로 협상하는 것이 가능하여야만 하므로 2단계에서 복수의 선택자를 기술하는 방법이 요구된다. 이를 위해 ID의 새로운 타입으로 ID를 순환적으로 포함시키는 것을 허용하는 ID_LIST를 정의한다. 응답자 ID도 마찬가지이다. 이 ID_LIST ID는 ID_LIST ID 패이로드 안에 나타날 수는 없으며 관련 규격에서 정의된 ID 타입의 어떤 것도 ID_LIST ID안에 포함될 수 있다. ID_LIST ID에 포함된 각각의 ID는 완벽한 식별패이로드 헤더를 포함해야만 한다. 그림 3은 두 개의 ID_FQDN 패이로드를 포함하는 ID_LIST ID의 내용을 예로 보여주고 있다.

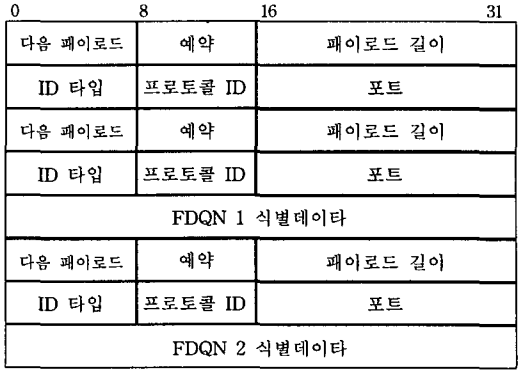

그림 3. ID_LIST ID 패이로드의 내용 예시

ID_FQDN과 ID_IPV4_ ADDR과 같이 여러 가지 형태의 ID는 동일한 ID_LIST ID안에 포함될 수 있다. ID_LIST ID 패이로드에 포함된 ID 타입이 ID_LIST ID가 사용된 문맥에서 타당하지 않은 경우 전체 ID_LIST가 잘못되어지는 것으로 간주되어야 한다. 예를 들면 ID_FQDN을 포함하는 ID_LIST ID

패이로드와 ID_IPV4_ADDR이 IKE 빠른 모드 교환 동안 수신되는 경우 수신자는 송신자에게 오류를 알려야 하며 메시지의 처리를 멈춘다. ID_LIST ID를 위해 IANA에서 아직 번호는 할당되지 않았으므로 앞으로 이에 대한 정의가 요구된다.

o IKE가 2단계 선택자를 검증할 수 있기 위해서는 1단계 동안 충분한 정보를 교환하는 것이 가능하여야만 한다. IP주소에 대응하는 1단계 ID를 사용하고 1단계 교환을 인증하기 위해 사용된 인증서의 Subj AltName에 그러한 동일한 주소를 인코딩하여 현재 IKE는 간단한 경우는 직접적으로 수용할 수 있다. 좀 더 복잡한 경우의 시나리오에 대해서 외부의 정책이나 어떤 다른 방법이 2단계 선택자와 SA 매개변수를 검증하기 위해 참조될 필요가 있다. 하나의 SCTP 연계에 복수개의 소스/목적지 주소의 문맥에서 동일한 시나리오를 수용하기 위해 다음과 같은 것이 가능하여야만 한다.

- 2단계 매개변수 특히 2단계 선택자를 검증하기 위해 사용될 수 있는 복수개의 1단계 ID를 기술한다. ID_LIST ID 타입에 관한 정의에 따라 복수개의 1 단계 ID를 기술하기 위해 동일한 방법을 사용하는 것이 가능하다.
- 여러 가지의 1단계 ID가 진짜임을 증명한다. 미리 공유된 키 인증을 사용하여 동일한 공유키를 모든 수용가능한 상대 1단계 ID와 연계하여 이것이 가능하다. 인증서의 경우에 두가지 선택이 있다. 첫 번째로, 동일한 인증서는 ASN.1표기에 의해 SubjAltName필드에 인코드된 복수의 ID를 포함할 수 있다. 이것은 이미 가능하므로 선호되는 해결책이며 개발시 이를 지원하여야만 한다. 다른 하나는 복수개의 인증서가 복수의 CERT 패이로드로 1단계 교환동안 전달될 수 있다. 이러한 기능은 또한 현재의 규격에 의해 지원된다. 하나의 서명만이 IKE 1단계 교환당 발급되므로 모든 인증서가 그들의 Subject와 동일한 키를 포함하는 것이 필요하다. 그러나 이런 접근은 첫번째에 비해 어떤 중요한 장점을 제공하지는 않으므로 개발시 위 두 가지 중 선택적으로 지원할 수 있다. 어느 경우든 IKE구현은 교환에서 수신된 모든 그러한 ID에 대해 상대방에서 주장하는 1단계 ID의 타당성을 검증하는 것이 요구된다. 후자가 사용중인 동안 SCTP는 하나의 SCTP 연계와 관련되어진 주소의 수정을 비록 SCTP는 현재 지원하지 않을지라도 앞으로 지원될 수 있는 기능으로 주소의 집합이 극히 자주 변경되지 않는한 적절한 선택자와 SA를 설정하기 위해 전체 1단계와 2단계 교환을 하는 것이 충분하다.

SCTP와 IKE에 대한 마지막 이슈는 발기자에 의한 2단계 선택자 ID의 초기제안에 관한 것이다. 현재의 IKE 규격에 의하면 응답자는 첫 번째 메시지로 수신된 ID를 Quick mode의 두 번째 메시지로 송신해야만 한다. 그래서 이 SCTP 연계와 관련된 모든 선택자를 발기자가 이미 안다고 가정된다. 그러나 대부분의 경우 응답자는 여러주소에 대한 좀더 정확한 지식을 가지므로 설정된 IPsec선택자가 잠재적으로 불충분하거나 부정확할 수 있다. 제안된 선택자들의 집합은 응답자의 관점으로부터 정확하지 않다면 후자는 새로운 Quick mode 교환을 시작할 수 있어 이 새로운 Quick mode 교환에서 발기자와 응답자의 역할이 바뀐다. 그래서 새로운 발기자는 이전의 Quick mode메시지로부터 SA와 선택자를 복사해야만하고 실제로 일치하도록 선택자의 집합을 수정해야만 한다. SCTP를 지원하는 모든 IKE는 이렇게 동작 할 수 있어야만 한다.

VI. 결론 및 연구방향

이 논문에서는 스트림제어 전송프로토콜의 보안 이슈에 대한 연구와 IPsec 보안을 SCTP와 함께 사용하기 위한 몇 가지 IPsec 보안에 대한 기능요구사항 및 설계를 수행하였다.

비록 SCTP는 TCP에 나타난 문제중의 일부를 피할 수 있도록 조심스럽게 설계되었을지라도 현재 아직은 널리 사용되고 있지는 않기에 앞으로 새로운 보안 이슈가 제기될 가능성이 많이 있으므로 이에 대한 향후 많은 연구가 이루어져야 할 것으로 보인다.

참고문헌

[1] R. Stewart, etc, "Stream Control Transmission Protocol", 2000.10.

[2] Atkinson, R., and S. Kent, "Security Architecture for the Internet Protocol", RFC 2401, 1998.11.

[3] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, 1998. 11.

[4] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, 1998.11.

[5] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, 1998.11.

[6] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, 1998. 11.