차세대 네트워크 보안 시스템을 위한 STEALTH 프로토콜 제안

오승희[0] 남택용 손승원
한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀
(seunghee5, tynam, swsohn)@etri.re.kr

Proposal of STEALTH Protocol for Advanced Network Security Systems

Seung-Hee Oh[O], Taekyong Nam, Sungwon Sohn
Electronic and Telecommunications Research Institute,
Information Security Technology Division, Network Security Architecture Research Team
(seunghee5, tynam,swsohn)@etri.re.kr

요 약

복잡한 네트워크상의 지능적이고 다양한 방식의 사이버 테러로부터 안전하고 효율적으로 네트워크를 총체적으로 관리하기 위해서는 개별 네트워크 노드간의 정보 교환은 필수적이다. STEALTH 프로토콜이란 거대망에서 네트워크 노드들 사이에 안전한 정보 교환을 위한 일종의 보안 프로토콜로 기존의 보안 프로토콜이 지닌 트래픽의 속도 저하 및 암호화로 인한 네트워크의 과부하를 최소화한 프르토콜이다. 여기서는 기존의 보안 프로토콜에 대해서 그 종류와 기능을 살펴본 후, 제안하는 STEALTH 프로토콜의 요구사항 및 기능에 대해서 다룬다. 마지막으로 STEALTH 프로토콜이 적용된 시나리오를 통해 이 프로토콜의 역할과 기능을 상세히 설명한다

1. 서론

네트워크가 증대되고 복잡해짐과 더불어 네트워크를 통한 침입이 갈수록 지능적이고 정교해짐으로써 단순한 네트워크 관리 뿐만 아니라 네트워크를 안전하게 보호하는 보안 측면에 관심이 집중되고 있다. 사이버 테러로부터 네트워크를 안전하게 보호하기 위해서 대부분의 네트워크에 침입차단시스템, 침입탐지시스템, 항바이러스 시스템 등을 추가하고 있다. 그러나 날마다 신문의 새로운 기사처럼 새로운 변종 바이러스들이 등장하고, 네트워크 침입 방식도 다양해지고 있는 상황에서 기존의 정보에만 의존한 보안이란 눈 가리고 아웅하는 식의 임시방편에 불가하다. 따라서, 기존의 수동적이고 정적인 보안 방식이 아닌 새운 정보를 받아들이고 적용하는 능동적이고 적극적인 보안 방식이 요구된다. 이러한 능동적이고 적극적인 보안을 위해서는 네트워크 노드간의 정보 교환 및 협력이 필수적인데, 이때 주고받는 정보들을 신뢰할 수 있는 방식을 통해 전달해야 함은 너무도 자명한 사실이다.

이를 제공해주기 위해서 새로운 개념의 보안 프로토콜인 STEALTH 프로토콜이 필요한 것이다[1].

2. 기존의 보안 프로토콜

2.1. 보안 프로토콜의 정의

보안 프로토콜이란 주고 받는 데이터의 안전성을 보장해주기 위해서 인증, 암호화 기능을 기본적으로 포함한 프로토콜이다. 여기서는 지금 존재하고 있는 보안 프로토콜에는 어떤 것이 있으며, 각각의 특성에 대해서 살펴본다.

2.2 기존의 보안 프로토콜들

기존의 보안 프로토콜들은 적용 계층에 따라서 아래의 표와 같이 분류할 수 있다.

<표 1> OSI 계층별 보안 프로토콜

계층(OSI 7 layer 기준)	보안 프로토콜
Data Link Layer	PPTP, L2TP
Network Layer	IPSec
Session Layer	Socks v5
Application Layer	SSL/TLS, SSH

2.2.1 PPTP (Point to Point Tunneling Protocol)

Microsoft에 의해 제안되어 현재 Windows 2000, NT 등에 기본으로 탑재되어 있는 PPTP는 2계층 터널링 프로토콜로써, remote access VPN(Virtual Private Network)에서 많이 사용된다. PPP (Point-to-Point Protocol)를 기반으로 하여 원격 사용자의 인증을 제공하고 PPP 패킷의 암호화를 위해 GRE (Generic Routing Encapsulation)를 적용한다[2][3].

2.2.2 L2TP (Layer 2 Tunneling Protocol)

PPTP 와 마찬가지로 2 계층 터널링 프로토콜인 L2TP 는 Cisco 의 L2F(Layer 2 Forwarding)과 Microsoft 의 PPTP 를 통합하여 만든 것으로 PPTP 와 달리 하나의 터널에 여러 세션의 생성이 가능하다. 자체의 보안성은 미미하여 IPSec 의 일부 보안 기능을 이용하여 인증, 암호화를 제공한다[2][3].

2.2.3 IPSec (IP Security)

IPSec 은 네트워크 계층에서 통신 상대간 안전한 통신을 하도록 하는 IP 보안 프로토콜로 IETF (The Internet Engineering Task Force)의 Security Area 의 IPSec Working Group(WG)에서 표준으로 제정되었다. 이 프로토콜은 IP 보안 구조, 인터넷 키 교환 (Internet Key Exchange: IKE), 그리고 보안 서비스를 제공해주는 IP AH (Authentication Header)와 IP ESP (Encapsulating Security Payload) 의 두 헤더, 연결 관리와 정책 관리를 위한 SPD(Security Policy Database)와, SAD(Security Association Database)로 구성된다.

IP 패킷은 헤더와 페이로드 두 부분으로 나눌 수 있고, IP 헤더의 내용에 대해 보안 서비스를 적용하기 위하여 AH 헤더를 IP 확장 헤더로 추가하고, IP 페이로드의 내용에 대해 보안 서비스를 적용시키기 위하여 사용자 데이터를 ESP 로 암호화한 후 헤더에 추가한다. AH 와 ESP 는 각 프로토콜 내부에서 사용하는 암호화 및 인증 등의 알고리즘과 독립적인 구조를 가지고 있으며, IP 계층에서 사용하는 프로토콜 이외의 다른 보안 메커니즘을 필요치 않다.

IPSec 는 암호화로 인해 속도가 느려진다는 점과 키 관리에 너무 많은 오버헤드가 발생한다는 단점을 가지고 있다. 이를 해결하기 위해 IETF 의 ipsec WG 에서는 키 관리 및 분배를 간소화하는 IKEv2 에 대한 표준화가 진행 중이다.

2.2.4 Socks v5

세션 계층의 proxy 프로토콜인 Socks v5 는 기존의 Socks v4 에서 사용자 인증, 암호화 협상 및 UDP Proxy 등과 같은 보안 기능이 추가되었다. Socks v5 는 응용 계층에서 필터링을 지원하며 응용 계층의 보안 프로토콜인 SSL/TLS 과 결합 사용이 가능하다. Socks 는 기본적으로 기업의 내부 네트워크에서 사용자들로부터 요청을 받아 인터넷으로 전달할 수 있도록 하기 위해, 프록시 서버가 사용할 수 있는 프로토콜이다. Socks 는 개개의 접속을 표현하고, 추적하기 위해 소켓을 사용한다.

2.2.5 SSL (Secure Socket Layer)/TLS (Transport Layer Security)

인터넷 사이트에 접속 시 가장 일반적으로 사용되는 SSL 은 HTTP 를 사용하여 데이터를 주고 받을 때 모든 데이터를 암호화하여 안전한 송수신을 지원하는 프로토콜로써, 데이터 암호화를 위해서 대칭키 방식을 사용하고 대칭키를 송부하기 위해 공개키 암호화 방식을 이용한다. 1994년에 Netscape에 의해 개발된 SSL은 1995년에 버전 3까지 발표되었으며, 1996년에 IETF의 Security Area에서 WG이 구성되어 1999년 1월에 SSL v3를 바탕으로 새롭게 발표한 것이 TLS이다.

2.2.6 SSH (Secure SHell)

IETF Security Area의 SSH WG에서 표준으로 현재 SSH2까지 제안되어 있는 SSH는 원격 컴퓨터에 안전하게 액세스하기 위한 유닉스 기반의 명령 인터페이스 및 프로토콜이다.

SSH는 네트워크 관리자들이 웹 서버를 포함한 여러 종류의 서버들을 원격지에서 제어하기 위해 사용되며, 실제로 초창기 유닉스 유틸리티인 rlogin, rsh, rcp에 보안 기능이 추가된 버전, slogin, ssh, 그리고 scp 등의 세 가지 유틸리티들의 모음을 가지고 있다.

3. STEALTH 프로토콜

3.1 STEALTH 프로토콜의 정의

STEALTH 프로토콜이란 개별 노드(예: STEALTH Engine)간의 안전한 통신을 보장해주기 위해 요구되는 보안 프로토콜의 한 종류로써, Secure Protocol[4]과 Security Protocol[5]의 의미를 포함하는 개념이다.

기존의 네트워크 보안 서비스에는 관제 서비스, 항바이러스 서비스, 침입탐지 서비스 및 접근 제어 서비스 등이 있었다. 기존의 보안 프로토콜은 사용자 사이에 인증 및 권한 부여가 이루어졌던 것에 반해 STEALTH 프로토콜은 차세대 네트워크 보안 시스템 개발 과제의 일부분으로 통신 주체가 보안 노드 또는 중앙의 네트워크 관리 서버라는 점이 다르다. 여기서 보안 노드란 보안 기능을 가진 네트워크 노드를 의미하며, 거대망에서 Connection point, Access point, Service point 역할을 한다.

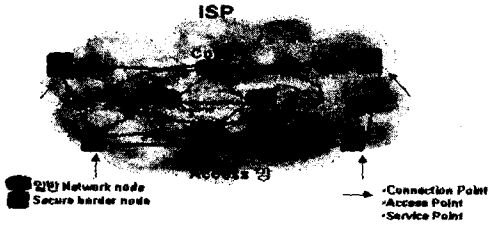
STEALTH 프로토콜은 ISP와 같은 거대망에서 보안 노드사이와 보안 노드와 중앙의 네트워크 관리 서버간에 정보 교환 및 정책, 보안 서비스에 대한 내용을 전달하는 데 사용한다. 그림 1과 같이 보안 노드는 Access 망의 인입점에 위치하고 그 안에는 다시 일반 네트워크 노드들로 구성된 Core 망이 존재한다.

STEALTH 프로토콜의 주요 역할은 다음과 같으며, 이것은 보안 노드 노드간에 또는 네트워크 노드(보안 노드 포함)와 네트워크 관리 서버간에 일어난다.

- 각 네트워크 노드의 상태 정보 및 관리 정보 전달
- 네트워크 노드에 안전하게 보안 정책 전달 및 업데이트

신뢰할 수 있는 인증서 교환 자동적인 라우팅 정보 교환 전송되는 데이터의 안전성 보장

<그림 1> STEALTH 프로토콜의 적용 범위



3.2 STEALTH 프로토콜의 요구사항 및 기능

STEALTH 프로토콜의 기본적인 요구사항은 다음과 같다.

- 네트워크 노드간의 안전한 통신 기능이 요구됨
- 전송하는 데이터에 대한 보호 기능이 요구됨
- 프로토콜 자체 보안 기능이 요구됨

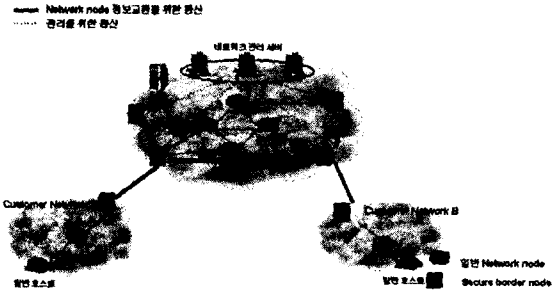
STEALTH 프로토콜은 기본적인 보안 프로토콜의 기능을 포함하여 다음처럼 크게 4 가지의 기능을 가지고 있다.

- 상호 인증: 통신이 생성되기 전에 통신의 양쪽 주체를 확인하기 위한 것으로 안전한 통신을 위해 반드시 필요한 선행 과정이다.
- 데이터 암호화: 통신이 설정된 후에 주고 받는 데이터의 안전성을 보장하기 위해서 데이터 자체를 암호 알고리즘을 통해 암호화한다.
- 액세스 제어: 허가받지 않은 사용자(네트워크 노드)의 불법적인 접근을 차단하는 것이다.
- 터널링: 통신 주체가 안전하도록 데이터가 전달되는 곳의 IP 주소가 노출되지 않도록 보장한다.

4. STEALTH 프로토콜 적용망 테스트베드

현재 제안하는 STEALTH 프로토콜의 적용 범위는 ISP 와 같은 거대망에서 네트워크 관리 서버와 네트워크 노드간, 그리고 네트워크 노드들 간의 통신에 적용된다. 즉, 네트워크 노드간에 정보 교환을 위해서 이루어지는 통신과 네트워크 관리 서버가 해당 구역의 네트워크 노드들을 관리하기 위해 이루어지는 통신에 한정된다. 향후 STEALTH 프로토콜 적용 시 발생하는 오버헤드가 최소화될 수 있는 최적화 방식이 제공되면 일반 호스트까지 확장될 수도 있다.

그림 2 는 STEALTH 프로토콜이 적용된 테스트베드를 보여주고 있는 것이다. 앞서 설명한 바와 같이 STEALTH 프로토콜은 두 가지 범위에서 사용되며, 중앙에 별도의 CA(Certificate Authority) 가 존재하여 암호화를 위한 키 관리를 제공한다. 본 STEALTH 프로토콜에서는 키 분배 및 키 관리의 overhead 를 최소화하기 위하여 일괄적으로 키에 대한 모든 관리는 중앙의 CA 에서 이루어진다. 이는 네트워크 노드에서의 광대하게 발생하는 트래픽의 속도 저하를 최소화하기 위함과 ISP 와 같은 거대망의 네트워크 노드라 하더라도 그 수가 한정적이기 때문에 자동적인 키 관리 방식 대신 매뉴얼한 키 관리 방식을 채택한 것이다.



<그림 2> STEALTH 프로토콜 적용된 테스트베드

5. 결론

여기서는 현재 네트워크 보안의 중요성과 더불어 네트워크 노드들의 정보 공유가 필수적인 상황에서 차세대 네트워크 보안 시스템에 적용될 네트워크 노드 사이와 네트워크 노드와 네트워크 관리 서버간의 안전하면서도 네트워크 트래픽에 영향을 최소화할 수 있는 보안 프로토콜인 STEALTH 프로토콜을 정의하였다.

보안 프로토콜의 특성상 암호화 및 보안을 위한 여러 기능 및 단계가 추가되기 때문에 네트워크 트래픽의 속도 저하는 피할 수 없는 단점이다. 향후에는 STEALTH 프로토콜의 키 관리 방식과 최적화된 암호 알고리즘 개발을 통해 트래픽의 속도 저하를 최소화하는 방식에 대해 연구될 것이다.

참고문헌

[1] 차세대 네트워크 보안 시스템 기술 백서", ETRI, 2002

[2] 오승희, et. al., "다양한 트래픽을 이용한 VPN 프로토콜 성능 평가", 정보처리학회 논문지, Vol.8-C, No. 6, Dec. 2001

[3] 채기준,"가상사설망 보안", 제 5 회 정보통신응용워크숍 차세대 네트워크 기술 발표집 II, pp.145~173

[4] Ran Canetti, "Security and Composition of Multi-party Cryptographic Protocols", Journal of Cryptology: the journal of the International Association for Cryptologic Research, 1999

[5] R. Needham and M. Schroeder, "Using encryption for authentication in large networks of computers", Communications of ACM, 21(12), Dec.1978