보안정책정보 전달을 위한 COPS-SECURITY 프로토콜

윤승용[0] 안개일 류걸우 장종수
한국전자통신연구원 네트워크보안연구부
(syyoon, fogone, kwryu, jsjang)@etri.re.kr

COPS-SECURITY Protocol for Security Policy Information

Seung-Yong Yoon[0] Gae-Il Ahn Kuel-Woo Ryu Jong-Soo Jang

Dept. of Network Security, Electronics and Telecommunications Research Institute

요 약

인터넷의 성장과 더불어 네트워크를 통한 침입의 가능성이 증가됨에 따라 시스템이나 네트워크 침입을 탐지하고 대응할 수 있는 기술들이 필요하게 되었다. 이와 관련하여 많은 연구가 이루어지고 있으나, 보안정책정보 전달을 위한 방법에 대해서는 아직까지 활발히 이루어지고 있지 않는 실정이다. 본 논문에서는 기존의 정책전달 프로토콜인 COPS 프로토콜을 확장, 수정하여 보안정책정보(Security Policy Information)를 전달할 수 있는 COPS- SECURITY 프로토콜에 대해 기술한다.

1. 서 론

COPS(Common Open Policy Service) 프로토콜은 정책서버(Policy Decision Point: PDP)와 클라이언트(Policy Enforcement Point: PEP) 사이의 정책정보 전달을 위한 TCP 기반의 간단한 질의/응답 프로토콜이다[1]. COPS 프로토콜은 그 자체를 수정하지 않고 다양한 클라이언트 타입을 지원할 수 있는 확장성을 가지는데, IntServ에서의 신호 프로토콜인 RSVP를 지원하기 위한 COPS-RSVP, DiffServ에서 정책을 Provisioning하기 위한 COPS-PR 등이 현재 제안되어 있다[2].

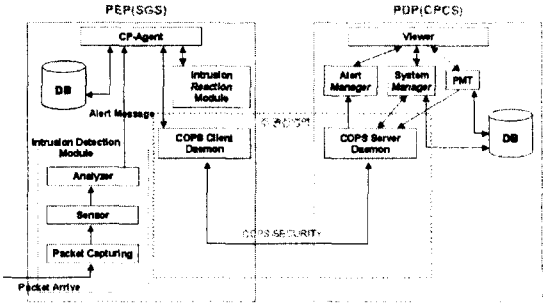
본 논문에서는 기존의 기본 COPS 프로토콜과 여러 COPS 확장 프로토콜들이 QoS(Quality of Service) 정책에 초점을 맞추어 제안된 것과는 달리, 주된 정책정보가 보안정책정보(Security Policy Information)로서 이를 전달하기 위해 COPS 프로토콜을 확장, 수정한 " COPS-SECURITY" 프로토콜을 제안하고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하고 있는 COPS-SECURITY에 대해서, 3장에서는 구동 시나리오에 대해서 기술하고, 끝으로 4장에서는 결론을 맺는다.

2. COPS-SECURITY 프로토콜

2.1 COPS-SECURITY 기반 보안제어 시스템 구조

COPS-SECURITY 기반 보안제어 시스템의 기본 구조는 [그림 1]와 같다. PEP로서 기능 하는 SGS(Secure Gateway System)에는 침입탐지를 위한 모듈과 침입대응 모듈, Manager로서 동작하는 CP-Agent 모듈이 있다. 그리고 COPS Client Daemon이 존재하는데, 이 모듈이 PDP인 CPCS(Central Policy Control Server)의 COPS Server Daemon과 COPS-SECURITY 프로토콜을 통하여 보안정책정보를 주고 받게 된다. CPCS에는 경보 메시지를 관리하는 Alert Manager, 시스템 관련 정보를 관리하는 System Manager, 보안정책정보를 관리하는 PMT(Policy Management Tool) 모듈이 있는데, 관리자는 Viewer를 통하여 이러한 정보들을 감시하고 관리하게 된다.

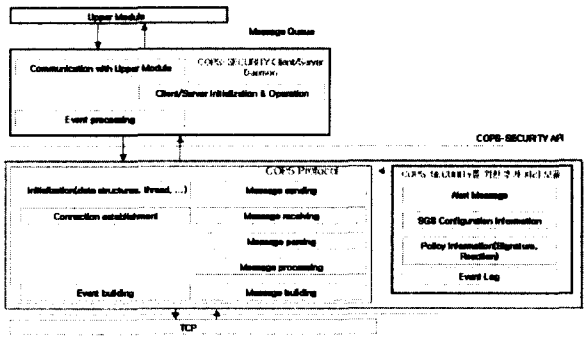


[그림 1] COPS-SECURITY 기반 시스템 기본 구조

본 논문에서는 시스템 기본 구조 중 [그림 1]에 나타난 것처럼 보안정책정보를 나르는 COPS-SECURITY 프로토콜에 주된 초점을 맞추어 기술한다.

2.2 기능 블록도

[그림 2]는 COPS-SECURITY 프로토콜에 대한 기능 블록도를 나타내고 있다. 기본 COPS 프로토콜에서 제공하는 10개의 메시지들을 처리하기 위한 모듈들이 API로 제공되는데, 메시지를 만들어서 보내고, 받고, 파싱하고, 처리하는 모듈과 초기화 모듈, 그리고 연결을 설정하는 모듈이 기본 COPS 프로토콜 스택에 포함되어 있다. 여기에 상위 모듈과의 연동을 위한 처리 모듈, 초기화 및 구동 모듈, 이벤트 처리 모듈 등이 클라이언트/서버 Daemon에 포함되어 있는데, 상위 모듈과는 Message Queue를 통하여, 하위 모듈과는 COPS-SECURITY API를 이용하여 보안정책정보를 전달하게 된다. COPS-SECURITY에는 기본 COPS 프로토콜에 몇 가지 추가적인 모듈이 필요하다. Sensor와 Analyzer를 통해 침입을 탐지하면 그 침입탐지 정보를 전송하기 위한 Alert Message 처리 모듈과 SGS 구성정보 전달모듈, 그리고 Signature, Reaction과 같은 보안정책정보를 전달하기 위한 모듈, 이벤트 로그 처리 모듈 등이 추가된다.



[그림 2] 기능 블록도

2.3 COPS-SECURITY를 위한 추가 모듈 정보

2.3.1 SGS 구성 정보

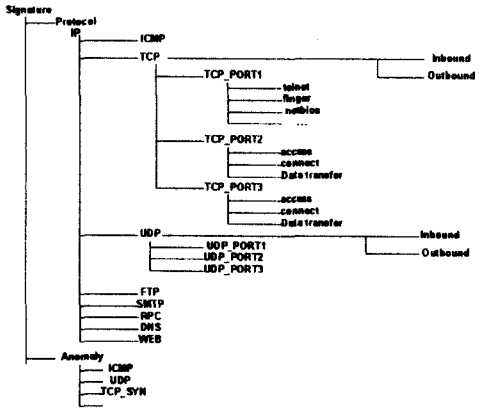
SGS는 보안정책정보를 전달 받기 위하여 CPCS로 연결을 설정하고, CPCS는 정책 도메인 내의 여러 SGS들을 관리하기 위해 각각의 정보를 알아야 하는데, SGS는 자신의 구성정보를 메시지에 담아 전송하게 된다. SGS 자신에 대한 정보, 네트워크 정보, Sensor, Analyzer에 대한 정보 및 OS에 관한 정보들이 포함된다. 이 정보는 SGS에서 CPCS로 전달 되어 관리되는데, CPCS는 이 정보를 참조하여 SGS에 정책을 배포한다.

2.3.2 Alert Message

SGS에서 침입 탐지를 하면 그에 대한 정보를 CPCS에 전달하여 관리하게 되는데, 침입을 탐지한 SGS, Sensor, Analyzer에 대한 정보, 침입 유형, 시간, 프로토콜, IP 주소, 포트, 그리고 시스템에 미치는 영향에 관한 정보들도 포함된다.

2.3.3 보안 정책 정보(Signature, Reaction)

보안정책정보는 PIB(Policy Information Base)로 저장되는데 [3, 4], 침입탐지를 위한 패턴 정보인 Signature, 침입 대응에 해당하는 Reaction으로 구성된다. 이러한 정보들은 COPS-PR에서 정의한 PRID, EPD Object을 이용하여 메시지 형태로 전달된다. [그림 3]은 Signature PIB 를 보여주고 있다.



[그림 3] Signature PIB

기본적인 Signature PIB 구성은 트래픽의 양, 패턴 수, 패턴의 정합성에 의해 분류되는데, 프로토콜 별 분석을 통한 오용 탐지를 위하여 ICMP, TCP, UDP, 그리고 이들 중 2개 이상의 프로토콜에 해당하는 경우와 패턴수가 매우 많은 중요한 프로토콜(FTP, SMTP, RPC, DNS, WEB)은 별도로 분류하고 있다

침입 대응에 관한 정책 정보(Reaction)는 크게 경보 동작과 차단 동작이 있는데, 이 외에도 세션기록저장, 역추적 및 ICMP Unreachable 메시지 전송 등이 있다.

2.4 기본 메시지

COPS-SECURITY에서는 COPS의 기본 메시지들 중 일부를 수정, 확장하여 보안정책정보를 전달한다. 대표적인 메시지로는 Request, Decision, Report State 메시지가 있다.

2.4.1 공통 헤더

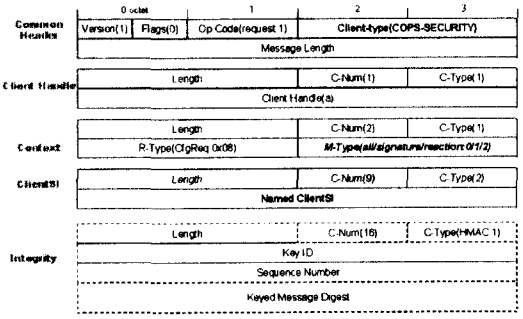
COPS 메시지들은 공통적인 기본 헤더를 포함하고 있는데, 여러 필드 중 Client-Type 필드에 기존의 COPS-RSVP나 COPS-PR이 아닌 본 논문에서는 새롭게 정의하고 있는 COPS-SECURITY 타입으로 채워진다.

2.4.2 Request(REQ) Message

Request 메시지는 PEP에서 집행하게 될 보안정책정보를 PDP로 요청하는 것으로 상황에 따라 Context Object와 Client

Specific Information Object(ClientSI)에 실어 나르는 정보가 달라지게 된다. 여기서는 Context Object의 R-Type과 M-Type 필드를 이용하여 침입탐지 및 차단, 대응에 대한 정책정보를 구분한다. R-Type 필드는 Configuration Request(0x08)로 채워지고, M-Type 필드는 다음 3가지로 세분화 된다.

1) all(0): PEP에 어떠한 보안정책정보도 없을 때, 모든 정보(signature, reaction)를 PDP로 요청한다.
2) Signature(1): 침입탐지에 적용할 패턴정보를 요청한다.
3) Reaction(2): 침입에 대한 대응정보를 요청한다.



[그림 4] Request(REQ) Message

2.4.3 Decision(DEC) Message

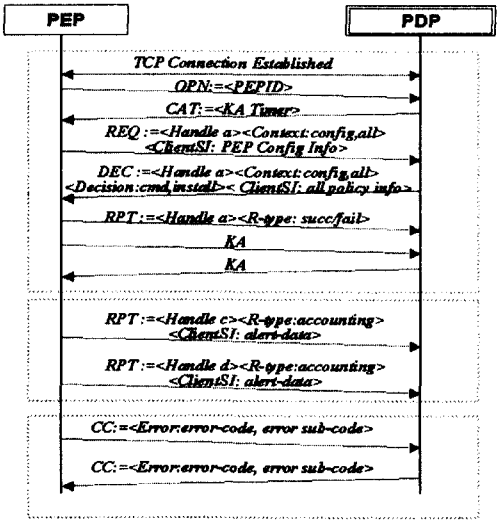
PEP의 Request 요청에 응답하여 PDP는 적절한 Decision 을 내려주는데, Request 메시지와 마찬가지로 Context Object의 R-Type과 M-Type 필드에 의해 보안정책정보를 구분하고, 이에 대한 보안정책정보들이 *Decision Object*에 실리게 된다. Decision Object는 그 타입에 따라 5가지로 분류되지만 필수적으로 포함해야만 하는 Decision Flags Object 와 Named Decision Data Object(C-Type = 5)를 이용하여 정책정보를 전송하게 된다.

2.4.4 Report State(RPT) Message

COPS에서는 Report-Type 필드에 정책적용에 대한 결과를 알려주는 Success, Failure 이외에 Accounting을 정의해 놓고 있는데, COPS-SECURITY에서는 이 Accounting을 이용하여 Alert 메시지를 전송한다.

3. 시나리오

[그림 5]은 PEP와 PDP 사이의 동작 시나리오를 나타낸 것이다. 우선 TCP Connection이 이루어진 후, COPS-SECURITY Client-Type Session을 열기 위해 PEPID를 담은 OPN 메시지를 PDP로 보낸다. 그러면 PDP는 Keep-Alive Time을 CAT 메시지에 실어 PEP로 보냄으로써 COPS-SECURITY Session 설정이 이루어진다. 이후 PEP와 PDP는 REQ, DEC, RPT 메시지를 통하여 보안정책정보를 주고 받게 되고, KA 메시지를 통하여 상호 연결 상태를 확인하면서 통신을 하게 된다. PEP에서의 침입 탐지에 대한 Alert-Data는 RPT 메시지를 통하여 PDP로 전송되고, 연결 종료는 CC 메시지를 통하여 이루어진다.



[그림 5] 구동 시나리오

4. 결 론

기존의 정책전달 프로토콜인 COPS 프로토콜은 대부분 QoS 정책 전달에 초점을 맞추어 제안되었고, 아직까지 보안정책을 전달하기 위한 구체적인 방안에 대해서는 논의가 되고 있지 않다. 이에 본 논문에서는 기존의 COPS 프로토콜을 확장, 수정하여 보안정책정보(Security Policy Information)를 전달할 수 있는 COPS- SECURITY 프로토콜에 대해 기술하였다.

5. 참고 문헌

[1] Boyle, J., Cohen, R., Durham, D., Herzog, S., Raja, R. and A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[2] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, A. Smith, "COPS Usage for Policy Provisioning (COPS-PR)", RFC 3084, March 2001.

[3] M. Fine, K. McCloghrie, J. Seligson, K. Chan, S. Hahn, A. Smith, F. Reichmeyer., "Structure of Policy Provisioning Information," draft-ietf-rap-sppi-07.txt, May 2001.

[4] M. Fine, K. McCloghrie, J. Seligson, K. Chan, S. Hahn, A. Smith, F. Reichmeyer "Framework Policy Information Base", draft-ietf-rap-frameworkpib-05.txt, July 2001.