이기종의 침입탐지 시스템과 SDMS-RTIR의 실시간 상호연동을 지원하는 침입탐지 메시지 교환 라이브러리 구현

유 일 선[†] · 이 동 련[††] · 오 은 숙[††]

요 약

본 논문에서는 한국정보보호진흥원에서 계층적 침입시도 탐지 및 대응을 위해 개발하였던 SDMS-RTIR(Scan Detection Management System with Real Time Incidence Response)을 지원하는 침입탐지 메시지 교환 프로토콜 라이브러리 IDMEPL을 구현하였다. IDMEPL은 IDWG의 IDMEF와 IAP를 기반으로 이기종의 침입(시도)탐지 시스템과 SDMS-RTIR의 실시간 상호연동을 제공하며 TLS 프로토콜을 통해 보안위협에 안전한 메시지 교환을 지원한다. 특히, IDMEPL은 유연성 있는 침입탐지 메시지 교환 프로토콜 선택 과정과 패스워드 기반의 암호화 프로토콜을 제공함으로써 각 침입(시도)탐지 시스템들로 하여금 자신의 네트워크 환경에 적절한 메시지 교환 프로토콜과 암호화 통신 방법을 선택할 수 있게 하였다. 이처럼 IDMEPL이 탑재된 SDMS-RTIR은 대규모의 네트워크 환경에서 이기종의 다양한 침입(시도)탐지 시스템들로부터 침입탐지 메시지를 실시간으로 접수하고 분석할 수 있다.

Implementing an Intrusion Detection Message Exchange Library for Realtime Interaction between SDMS-RTIR and Heterogeneous Systems

Il Sun Yun[†] · Dong Ryun Lee[††] · Eun-Sook Oh[††]

ABSTRACT

This paper implements an intrusion detection message exchange protocol library (IDMEPL) for SDMS-RTIR, which Korea Information Security Agency (KISA) has developed to hierarchically detect and respond to network vulnerability scan attacks. The IDMEPL, based on the IDMEF and the IAP of the IDWG, enables SDMS-RTIR to interact with other intrusion detection systems (IDS) in realtime, and supports the TLS protocol to prevent security threats in exchanging messages between its server and its agents. Especially, with the protocol selection stage, the IDMEPL can support various protocols such as the IDXP besides the IAP. Furthermore, it can allow for agents to choose an appropriate security protocol for their own network, achieving security stronger than mutual authentication. With the IDMEPL, SDMS-RTIR can receive massive intrusion detection messages from heterogeneous IDSes in large-scale networks and analyze them.

키워드 : 침입 탐지(Intrusion Detection), 네트워크 취약점 분석(Network Vulnerability Analysis), 네트워크 보안(Network Security)

1. 서 론

특정 네트워크 시스템을 공격하기 위해 미리 해당 시스템에 관한 취약점 정보를 수집하는 과정을 침입시도 공격이라 한다[2]. 침입시도 공격은 합법적으로 정보를 수집하는 foot printing 공격, 어떠한 시스템이 작동중인지 어떠한 시스템을 접근할 수 있는지 그들이 제공하는 서비스는 무엇인지를 탐지하는 스캐닝 공격, 시스템으로부터 노출되는 자원의 이름이나 유효한 계정을 추출하는 enumerating 공격으로 나눌 수 있으며 최근에 mscan, sscan, nmap 등과 같은 강력한 공격도구들의 공개로 인해 그 발생빈도가 급증하고 있는 실정이다[4-6].

이러한 네트워크 침입시도 공격에 대응하기 위하여 scanlogd, snort, RTSD(Real Time Scan Detector), DS-NVSA (Detection System of Network Vulnerability Scan Attack), SDMS-RTIR(Scan Detection Management System with Real Time Incidence Response) 등 다양한 도구들이 개발되었다[1-4].

특히, 한국정보보호진흥원에서 개발된 RTSD는 1차적으로 에이전트에서 공격을 탐지하고 2차적으로 탐지된 공격이 메일을 통해 중앙 관리서버에 보고되도록 함으로써 scanlogd와 snort같이 에이전트 수준이상의 계층적 대응을 하지 못하는 단독(stand-alone) 탐지 구조의 한계를 개선하였다[4]. 그러나 RTSD는 메일을 통해 에이전트와 관리서버간의 상호연동을 지원하기 때문에 중앙 관리서버 상에서 실시간

† 정 회 원 : (주)인터넷시큐리티 선임연구원
†† 정 회 원 : 한국정보보호진흥원 연구원
논문접수 : 2003년 2월 27일, 심사완료 : 2003년 8월 28일

으로 자동화된 종합 탐지 및 계층적인 대응을 하지 못하는 문제점을 갖는다[2, 4]. 이러한 문제점을 해결하기 위해 한국정보보호진흥원에서는 실시간으로 에이전트들이 관리서버에게 공격을 보고하고 이를 근거로 계층적인 탐지 및 대응을 수행하는 SDMS-RTIR을 개발하였다[1]. SDMS-RTIR에서 중앙 관리서버는 에이전트들로부터 보고된 탐지 정보를 실시간으로 수집 및 분석하는 동시에 공격이 탐지되면 whois 서비스를 이용하여 공격자를 검색하고 해당 공격자에게 경고 메일을 전송함으로써 대규모로 발생한 공격에 대응한다. 또한, SDMS-RTIR은 탐지 메시지의 규격으로서 IETF(Internet Engineering Task Force)의 작업그룹 IDWG(Intrusion Detection Working Group)가 제안한 IDMEF(Intrusion Detection Message Exchange Format)를 채택 및 확장하여 이기종의 침입(시도)탐지 시스템들과의 상호연동을 가능하도록 하였다. 그러나 SDMS-RTIR은 탐지 메시지 규격에만 표준안을 적용하였기 때문에 이기종의 침입(시도) 탐지 시스템들과 프로토콜 수준의 실시간 상호연동을 지원하지 못하며 또한 서버와 에이전트들 사이의 정보공유 과정에서 발생할 수 있는 거짓 탐지 보고와 거짓 침입 대응, 탐지 메시지 변조, 메시지 전송 부인 등의 보안위협에 취약한 문제점을 갖고 있다.

본 논문에서는 이러한 SDMS-RTIR의 문제점을 개선하기 위해 IDWG가 침입탐지 메시지 교환 프로토콜로 제안하였던 IAP(Intrusion Alert Protocol)를 기반으로 이기종의 에이전트들과 중앙 관리서버 사이에 실시간 상호연동을 지원하며 각종 보안위협에 안전한 침입탐지 메시지 교환 프로토콜 라이브러리 IDMEPL(Intrusion Detection Message Exchange Protocol Library)을 구현한다.

본 논문의 구성은 다음과 같다. 2장에서는 이기종의 침입(시도)탐지 시스템들 사이의 상호연동을 위한 IDWG 프레임워크를 기술하고, 3장에서는 IDMEPL의 기반이 되는 IAP 프로토콜을 기술한다. 4장에서는 SDMS-RTIR의 에이전트들과 중앙 관리서버 사이의 안전한 침입탐지 메시지 교환 절차를 설계하고, 5장에서는 이를 바탕으로 IDMEPL을 구현한다. 6장에서는 결론을 맺고 향후 연구 과제를 제시한다.

2. IDWG(Intrusion Detection Exchange Format) 프레임워크

IETF의 IDWG는 침입(시도)탐지 및 대응, 관리 시스템 사이에서 전송되는 메시지 형식과 메시지 교환절차의 표준화를 위해 구성되었다[16].

IDWG는 침입탐지 메시지 규격과 메시지 교환 절차(IDP : IDMEF transport Protocol)의 요구사항을 정의한 후, 침입탐지 메시지 규격으로서 IDMEF를 제안하였고, IDP의 요구사항을 만족하는 침입탐지 메시지 교환절차로서 IAP와 IDXP(Intrusion Detection eXchange Protocol)를 제안하였다[7-9, 13, 16]. IAP와 IDXP는 IDP의 요구사항 중 보안에 관련된 항목을 완벽히 지원하기 위해서 TLS(Transport Layer Security) 프로토콜 적용을 전제로 한다[7-8, 19].

비록 최근에 IDXP가 RFC 후보로서 유력하지만 복잡한 구조 및 TLS 프로파일의 검증과 다중채널 지원, configuration interface 개선 등의 구현상 문제점을 갖기 때문에 SDMS-RTIR에 적용할 수 없었다[7, 15]. 따라서 본 논문에서는 구조가 단순하고 이미 구현되어 적용사례를 갖는 IAP를 SDMS-RTIR의 침입탐지 메시지 교환 프로토콜로서 채택하였으며[8, 16], 향후 IDXP 프로토콜 적용을 위해 IDMEPL 설계에 있어서 유연성 있는 메시지 교환 프로토콜 선택을 중요한 요구사항으로 정의하였다.

3. IAP(Intrusion Alert Protocol)

본 장에서는 IDWG가 제안한 침입탐지 메시지 교환 프로토콜 중 하나인 IAP를 기술한다.

3.1 통신 모델

IAP는 설정 단계와 데이터 전송 단계로 구성되며 TCP 계층 위에서 요청-응답(request-response) 방식으로 진행된다[15].

3.1.1 IAP 설정 단계

IAP 설정 단계는 TCP 연결이 설정된 후의 첫 번째 단계로서 TCP 설정, 보안(Security) 설정, 채널 설정 3단계로 구성되며 각각의 단계를 통해 프로토콜의 환경 값들이 설정된다.

TCP 설정 단계는 SA(Sensor/Analyzer)와 M(Manager : 관리자) 사이에 TCP 연결이 설정되는 단계이다. 이 단계에서 SA는 iap-connect-request 메시지를 전송하여 연결을 요청하며 M은 연결승인 혹은 연결거부를 나타내는 iap-response 메시지를 통해 응답한다.

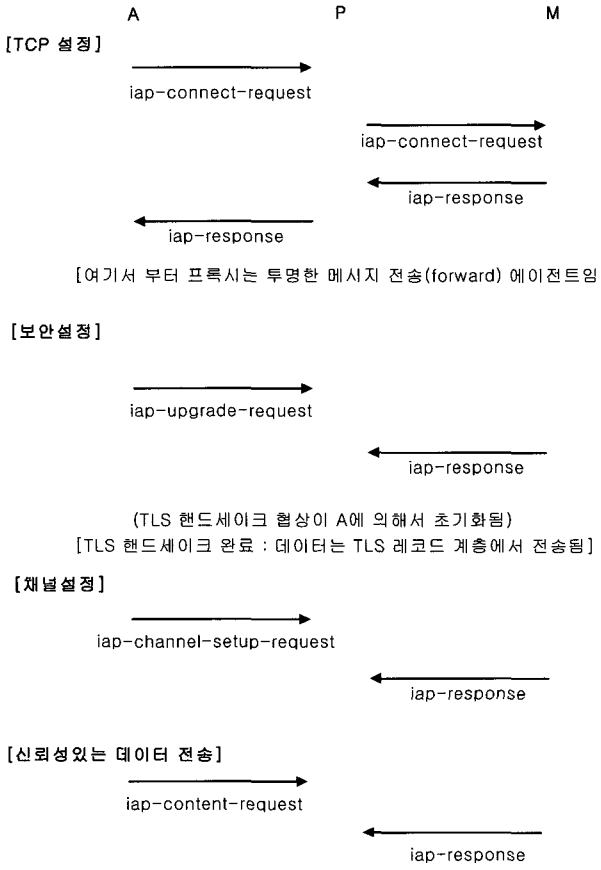
보안 설정 단계는 통신의 보안 환경을 설정하는 단계이며 이 단계 이후에 SA와 M은 TLS 1.0의 핸드세이크 프로토콜을 진행한다[8]. TLS 핸드세이크 프로토콜이 완료되면 SA와 M은 TLS 레코드 프로토콜을 통해서 채널 설정 단계를 진행한다.

채널 설정 단계는 IAP의 버전과 SA와 M의 역할을 결정하는 단계이다. SA가 iap-channel-setup-request 메시지를 보내면 M은 이 메시지에 대해서 프로토콜 설정 단계 동안 받았던 데이터들을 비교하여 버전 정보를 검증하고 SA에게 혹은 SA로부터 요청을 전송하거나 수신할 수 있는지를 검토한다. 그리고 iap-response를 SA에게 전송하여 SA가 설정한 프로토콜 변수들에 대해 동의 여부를 명시한다.

3.1.2 신뢰성 있는 데이터 전송(Secured Data Transport)

신뢰성 있는 데이터 전송 단계는 프로토콜의 핵심 부분

으로 IDMEF 메시지가 TLS 레코드 상에서 M에게 전송되는 단계이다.



(그림 1) IAP 프로토콜 진행 과정

3.1.3 종료

통신의 종료는 TLS close-notify alert 메시지를 통하여 SA나 혹은 M에 의해 초기화될 수 있으며 메시지를 받은 객체는 *close-notify alert* 메시지를 통하여 응답하고 연결을 종료한다.

(그림 1)은 프로토콜 진행 과정을 나타낸다. 여기서 A는 에이전트, P는 프록시, M은 관리서버를 의미한다.

```
iap-message = ( iap-request | iap-response )

iap-request    = iap-request-start-line
                 *(message-header CRLF)
                 CRLF
                 [ message-body ]

iap-response   = iap-response-start-line
                 *(message-header CRLF)
                 CRLF
                 [ message-body ]

iap-version = "IAP/0.5"
```

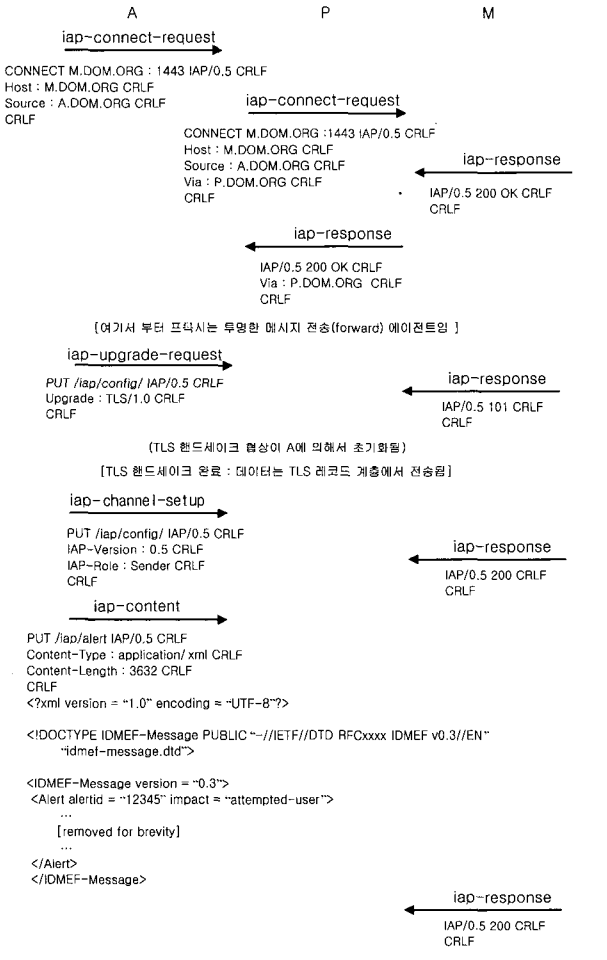
(그림 2) IAP 구문

3.2 IAP 프로토콜 메시지

IAP의 구문은 HTTP/1.1과 유사하며 (그림 2)와 같다[15]. IAP는 HTTP/1.1과 같은 요청-응답 프로토콜로서 IAP의 각 객체는 요청이나 응답중 하나의 메시지를 주고받는다. (그림 3)은 각 단계별 프로토콜 메시지를 보여주며 (그림 4)는 A.DOM.ORG가 M.DOM.ORG에게 IDMEF 형식의 침입탐지 메시지를 전송하는 프로토콜 메시지의 예를 보여준다.

```
iap-request-start-line =
        ( iap-connect-request |
          iap-upgrade-request |
          iap-channel-setup-request |
          iap-content-request )
```

(그림 3) IAP의 각 단계별 프로토콜 메시지



(그림 4) IAP 프로토콜 메시지의 예

4. 안전한 침입탐지 메시지 교환 절차 설계

본 장에서는 SDMS-RTIR을 위한 침입탐지 메시지 교환 절차의 요구사항을 정의한 후, 이를 기반으로 SDMS-RTIR의 안전한 침입탐지 메시지 교환 절차를 설계한다.

4.1 침입탐지 메시지 교환 절차의 요구사항

4.1.1 실시간 수준의 상호연동성

SDMS-RTIR은 침입시도 공격에 관한 국가적인 대응 체계를 확립하기 위해 개발되었다. 따라서 SDMS-RTIR은 대규모의 네트워크 환경에 존재하는 이기종의 다양한 침입(시도)탐지 시스템과 실시간 수준의 상호연동을 해야 하며 이를 위해서 IDWG에서 제안한 표준 메시지 교환절차와 표준 메시지 규격을 지원해야 한다[1, 4]. 또한, SDMS-RTIR은 침입탐지 메시지 교환 프로토콜을 위해 IAP와 더불어 IDXP 혹은 기타 표준 프로토콜을 선택할 수 있는 유연성을 제공해야 한다.

4.1.2 보안성

SDMS-RTIR은 메시지 교환과정에서 발생할 수 있는 각종 보안위협에 안전해야 한다. 이를 위해 IDP에서 제시하였던 신뢰성 있는 메시지의 전송, 네트워크 환경의 보안체계 유지, 상호인증, 기밀성, 무결성, 부인봉쇄, 서비스 거부 공격 대응, 유해한 메시지 복사 방지와 같은 보안 요구사항이 만족되어야 한다[13]. IDWG에서 제안한 IAP와 IDXP는 X.509 v3 인증서를 통한 상호인증 옵션이 선택된 TLS 프로토콜과 함께 적용될 때, IDP의 요구사항을 모두 만족시킬 수 있다[7-8, 13, 19].

따라서 SDMS-RTIR은 X.509 v3 인증서를 통한 상호인증 옵션이 선택된 TLS 프로토콜을 지원해야 하며, 아울러 이러한 상호인증이 불가능하거나 TLS 프로토콜 자체를 선택할 수 없는 네트워크 환경도 지원할 수 있어야 한다.

4.2 침입탐지 메시지 교환 절차

침입탐지 메시지 교환 절차는 프로토콜 선택, 프로토콜 설정, 메시지 전송의 3단계로 구성된다.

프로토콜 선택 단계는 에이전트와 관리서버가 상호 메시지 교환을 하기 위해 IAP와 IDXP 등의 표준 프로토콜 중 적절한 프로토콜을 선택하는 단계이다. 이 단계를 통해 SDMS-RTIR은 IAP와 IDXP 또는 기타 침입탐지 메시지 교환 프로토콜들을 적용할 수 있다.

프로토콜 설정 단계는 프로토콜 환경변수 설정, 채널설정, 보안설정 등 메시지 전송을 위한 초기화 단계이며 메시지 전송 단계는 실질적으로 메시지가 전송되는 단계이다.

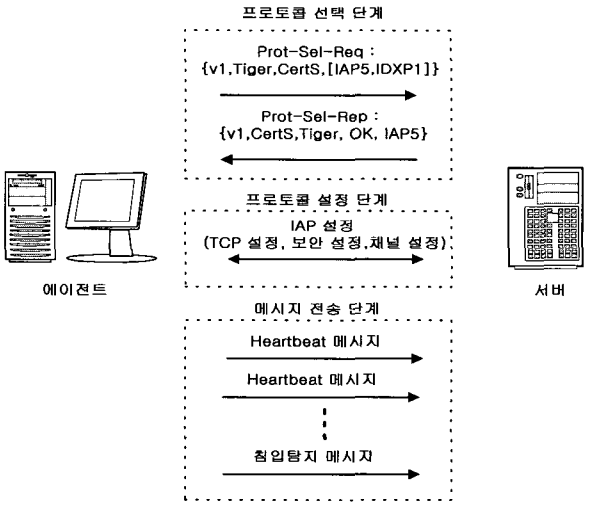
프로토콜 선택 단계를 통해 침입탐지 메시지 교환 프로토콜이 선택되면 선택된 프로토콜의 고유절차에 따라 프로토콜 설정과 메시지 전송 단계가 진행된다.

(그림 5)는 프로토콜 선택 단계의 메시지 규격을 보여주며 (그림 6)은 침입탐지 메시지 교환 절차의 예를 보여준다.

```
Prot-Sel-Req = {Ver, S, R, PL}
Prot-Sel-Req = {Ver, S, R, sts, P}

Ver : 프로토콜 버전 (defalt v1)
S : 메시지 송신자
R : 메시지 수신자
PL : 프로토콜 목록 [IAP5, IDXP1, etc]
P : 선택된 프로토콜
sts : 응답상태
```

(그림 5) 프로토콜 선택 메시지 규격



(그림 6) 침입탐지 메시지 교환 절차의 예

침입탐지 메시지 교환을 위해 초기 네트워크 연결이 시작될 때, (그림 6)에서처럼 에이전트는 에이전트가 적용할 수 있는 프로토콜 목록이 포함된 Prot-Sel-Req 메시지를 서버에게 전송한다. (그림 6)의 경우, 에이전트는 IAP와 IDXP를 모두 적용할 수 있다. 서버가 Prot-Sel-Req 메시지를 받으면 Prot-Sel-Req 메시지의 프로토콜 목록 중에서 적절한 프로토콜을 선택하고 Prot-Sel-Rep 메시지를 에이전트에게 전송한다. (그림 6)에서는 IAP가 침입탐지 메시지 교환 프로토콜로 선택되었다. IAP 선택 이후, IAP의 고유한 프로토콜 설정 단계인 TCP 설정, 보안설정, 채널설정이 진행되며 프로토콜의 설정단계가 완료되면 IAP와 TLS 프로토콜 상에서 실제 메시지가 전송되는 메시지 전송 단계가 진행된다.

4.3 사용자 인증 및 암호화 통신 프로토콜

SDMS-RTIR이 IDP의 보안 요구사항을 완전히 만족하기 위해서는 TLS 프로토콜에서 X.509 v3 인증서에 의한 상호인증이 적용되어야 한다. 그러나 이는 공개키 기반 환경의 복잡성 및 관리비용, 개인키 보관 문제 등으로 인해 인증서 기반의 사용자 인증 혹은 TLS 프로토콜 자체의 적용이 어려운 네트워크 환경에 대해서 대안을 제시하지 못한다.

본 절에서는 이를 위해 단독으로 혹은 TLS 프로토콜과 함께 사용될 수 있는 패스워드 기반의 사용자 인증 프로토콜을 제안하고 IAP를 확장한다.

4.3.1 패스워드 기반의 사용자 인증 프로토콜

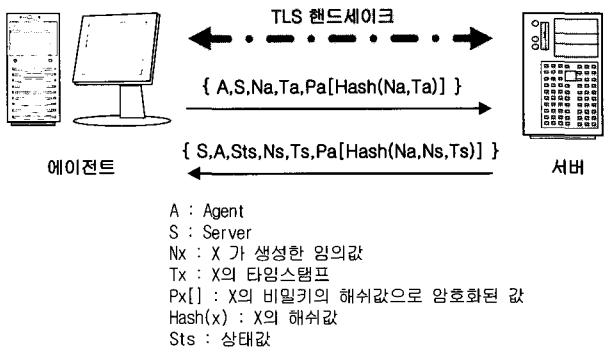
패스워드 기반의 사용자 인증 프로토콜은 (그림 7)과 같

이 정의된다.

제안된 인증 프로토콜은 특수한 경우를 제외하고 TLS 프로토콜의 데이터 전송단계에서 진행되는 것을 가정한다. 제안 프로토콜은 임의의 생성값 Na, Ns의 암호화를 통해 에이전트와 서버 사이의 상호인증을 지원하며 타임스탬프를 적용함으로써 재전송 공격에 대비하였다. 또한, TLS 프로토콜이 제공하는 암호화 통신에서 상호인증이 진행되기 때문에 공유 비밀키에 대한 오프라인 사전 공격(dictionary attack)에 취약하지 않다.

재전송 공격에 대응하기 위해 적용되는 타임스탬프는 침입탐지 메시지를 생성하기 위해 서버와 에이전트 사이의 시간 동기화가 필수적이므로 오버헤드가 되지 않는다.

제안 프로토콜은 TLS 프로토콜을 적용할 수 없는 환경에서 단독으로 적용될 수 있으나 이 경우, 서버와 에이전트 사이의 공유 비밀키에 대한 오프라인 사전 공격에 취약하며 <표 1>과 같이 상호인증을 제외하고 무결성, 기밀성, 부인봉쇄 등의 보안 요구 사항을 만족시킬 수 없다.

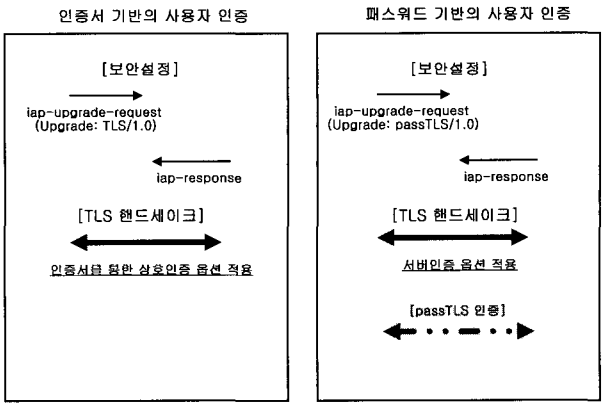


(그림 7) 패스워드 기반의 상호인증 프로토콜

4.3.2 IAP 확장

IAP는 오직 TLS/1.0만을 적용하기 때문에 제안된 사용자 인증 프로토콜이 적용되기 위해서 Upgrade Request가 확장되어야 한다.

이를 위해 Upgrade Request의 "Upgrade : TLS/1.0" CRLF 헤더는 그 내용이 TLS/1.0으로 고정되지 않고 "Upgrade : protocol" CRLF로 변경되며 패스워드 기반의 암호화 프로토콜을 위해 passOnly/1.0, passTLS/1.0이 추가되었다. passOnly/1.0은 TLS 프로토콜이 적용되지 않는 패스워드 기반의 암호화 프로토콜을 나타내며 passTLS/1.0 프로토콜은 TLS 프로토콜이 적용되는 패스워드 기반의 암호화 프로토콜을 나타낸다. (그림 8)은 IAP에서 TLS 프로토콜을 적용한 인증서 기반의 사용자 인증과 패스워드 기반의 사용자 인증 과정을 보여준다. <표 1>은 passOnly/1.0 및 passTLS/1.0, TLS/1.0을 비교 분석하였다. passOnly/1.0과 passTLS/1.0, TLS/1.0을 통해 사용자는 네트워크 환경에 따라 적절한 암호화 프로토콜을 선택할 수 있다.

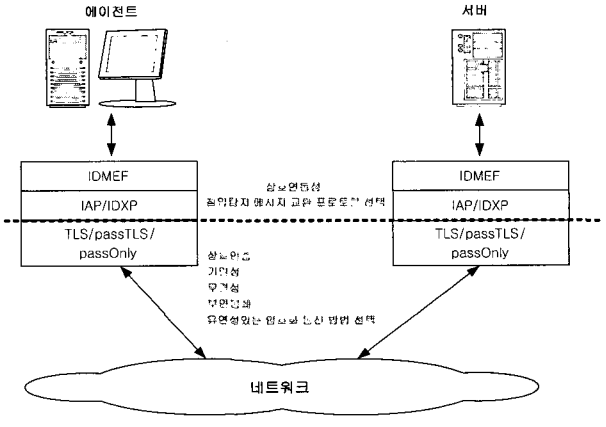


(그림 8) TLS 프로토콜 기반의 IAP 사용자 인증 과정

〈표 1〉 IAP의 암호화 통신 프로토콜 비교

비교 항목	passOnly/1.0	passTLS/1.0	TLS/1.0
인증 방식	패스워드 기반	패스워드 기반	인증서 기반
TLS 적용	×	서버인증 옵션	상호인증 옵션
구현 비용	최 소	중 간	최 고
관리 비용	최 소	중 간	최 고
연산 비용	최 소	중 간	최 고
상호 인증	○	○	○
무 결 성	×	○	○
기 밀 성	×	○	○
부인 봉쇄	×	×	△
유해한 메시지 복사	×	○	○
서비스 거부 공격 대응	×	○	○

(그림 9)는 본 장에서 설계된 안전한 침입탐지 메시지 교환절차의 전체 구성도를 보여준다. 침입탐지 메시지 교환절차는 IDMEF와 IAP 및 IDXP를 통해 SDMS-RTIR과 이기종의 침입(시도) 탐지 에이전트들 사이의 실시간 수준의 상호연동을 지원하며 TLS와 passTLS, passOnly 프로토콜들을 통해 안전한 메시지 교환을 지원한다.



(그림 9) 안전한 침입탐지 메시지 교환 절차 구성도

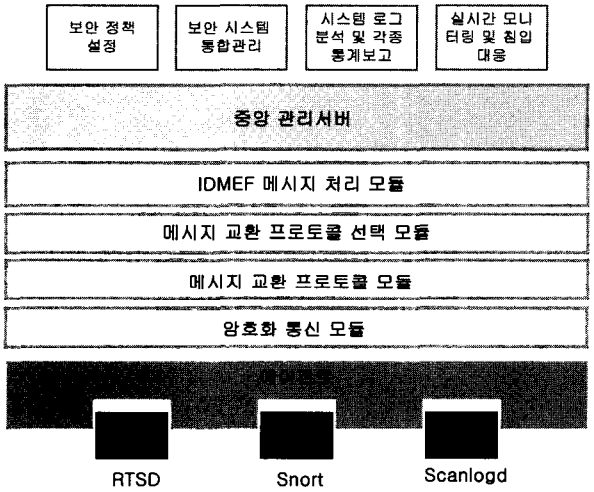
4.3.3 IDXP(Intrusion Detection eXchange Protocol) 적용

제안 절차에 대한 IDXP의 적용은 어렵지 않다. IDXP는 BEEP(Block Extensible Exchange Protocol) 프레임워크를 기반으로 구현되었기 때문에 오직 TLS 프로토콜을 전제로 하는 IAP와 달리 암호화 통신 방법 선택의 유연성을 지원한다. 따라서 별도의 확장 없이 IDXP를 본 논문의 제안 프로토콜에 적용할 수 있다. 단 passTLS/1.0과 passOnly/1.0의 적용을 위해서는 프로파일을 정의하여 등록해야 한다[7].

5. IDMEPL(Intrusion Detection Message Exchange Protocol Library) 구현

본 장에서는 4장에서 제안된 안전한 침입탐지 메시지 교환절차를 기반으로 침입탐지 메시지 교환 프로토콜 라이브러리 IDMEPL을 구현한다.

IDMEPL은 (그림 10)과 같이 IDMEF 메시지 처리 모듈과 메시지 교환 프로토콜 선택 모듈, 메시지 교환 프로토콜 모듈, 암호화 통신 모듈로 구성된다.



(그림 10) IDMEPL의 구조

본 논문에서는 IDMEPL의 IDMEF 메시지 처리 모듈을 위해 libxml 2.4.16과 libidmef 0.6.3 라이브러리를 적용하였고 암호화 통신 모듈을 위해 TLS 1.0을 지원하는 OpenSSL 0.9.7 라이브러리를 적용하였다[10-11, 14].

〈표 2〉 IDMEPL 구성 라이브러리

IDMEPL 모듈	구현 라이브러리
IDMEF 메시지 처리 모듈	libxml 2.4.16/libidmef 0.6.3 적용
메시지 교환 프로토콜 선택 모듈	libprotsel 1.0 구현
메시지 교환 프로토콜 모듈	libiap 1.0 구현
암호화 통신 모듈	OpenSSL 0.9.7 적용
	libpassauth 1.0 구현

또한, 이들 모듈 외에 메시지 교환 프로토콜 선택 모듈과 메시지 교환 프로토콜 모듈, 패스워드 기반 사용자 인증 프로토콜 모듈은 각각 API를 설계하고 직접 구현하였다.

<표 2>는 IDMEPL을 구성하는 라이브러리를 나타낸다.

5.1 메시지 교환 프로토콜 선택 모듈

IDMEPL의 메시지 교환 프로토콜 선택 모듈 libprotsel은 4장에서 제안된 메시지 규격과 절차에 따라 (그림 11)과 같이 구현되었다.

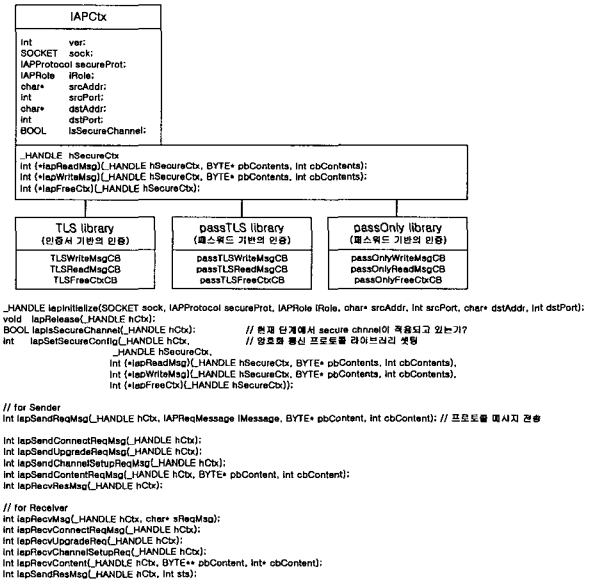
```
SelProtCtx
    // version : default 1 ;
int ver ;
    // socket handle
int sock ;
    // 역할 0 : secder, 1 : receiver
int role ;
    // 프로토콜 목록
int protlist [MAX_PROTOCOL] ;
    // 프로토콜 목록 크기
int protnum ;

// 역할
# define roleSender 0
# define roleReceiver 1

// 프로토콜 정의
# define IAP05 0
# define IDXP1 1

_HANDLE selpInit(int socket, int role, int* protlist, int protnum) ;
void selpRelease(_HANDLE h) ;
int selpSendReqMsg(_HANDLE h, const char* strDestAddr, int port) ;
int selpReceiveReqMsg(_HANDLE h) ;
```

(그림 11) libprotsel 모듈



(그림 12) libiap 모듈

selpInit에서 지정하는 프로토콜 목록은 통신객체의 역할에 따라 그 의미가 달라진다. 즉 역할이 송신자(roleSender)일 경우, 목록의 의미는 통신객체가 지원할 수 있는 프로토콜 목록을 나타내며 역할이 수신자(roleReceiver)일 경우, 통신객체가 허용할 수 있는 프로토콜 목록을 나타낸다. 만일 송신자가 적용할 수 있는 프로토콜이 2개 이상이고 그

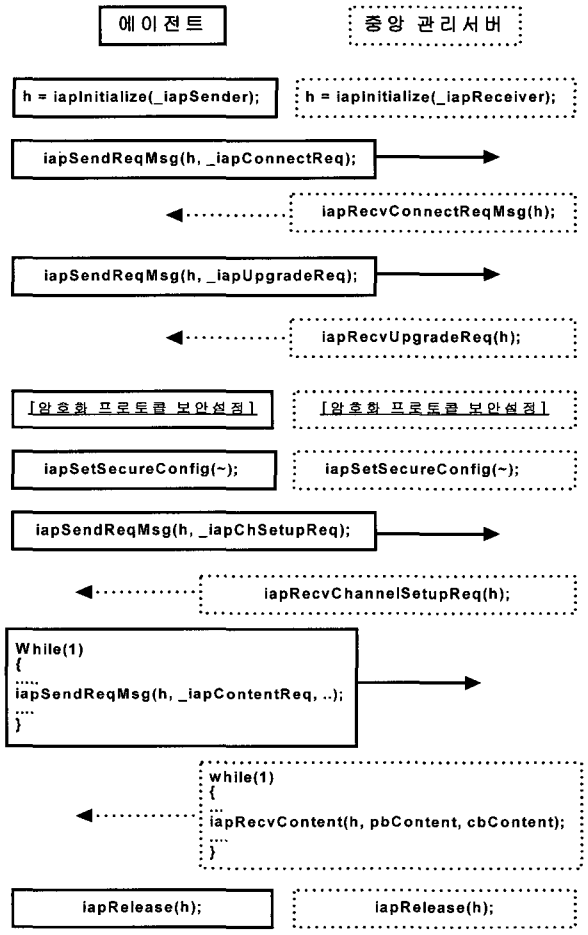
중 2개 이상이 수신자의 프로토콜 목록에 존재한다면 수신자의 프로토콜 목록에서 가장 우선 순위가 높은 프로토콜이 선택된다.

5.2 메시지 교환 프로토콜 모듈

IDMEPL의 메시지 교환 프로토콜 모듈 libiap는 3장에서 기술된 IAP를 기반으로 구현되었다.

libiap는 (그림 12)와 같이 IAPCtx 구조체와 그 구조체의 인스턴스를 통해 접근 할 수 있는 API 함수들로 구성되며, 특히 IAPCtx 구조체의 hSecureCtx, iapReadMsg, iapWriteMsg, iapFreeCtx를 통해 passOnly/1.0과 passTLS/1.0, TLS/1.0과 같은 암호화 통신 방법이 지정될 수 있도록 하였다.

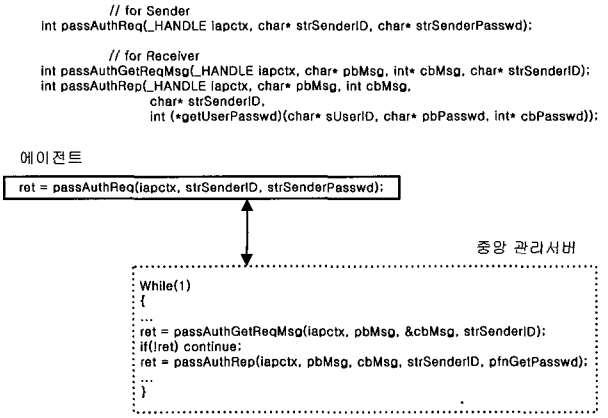
(그림 13)은 libiap API의 적용 과정을 보여준다.



(그림 13) libiap의 API 적용과정

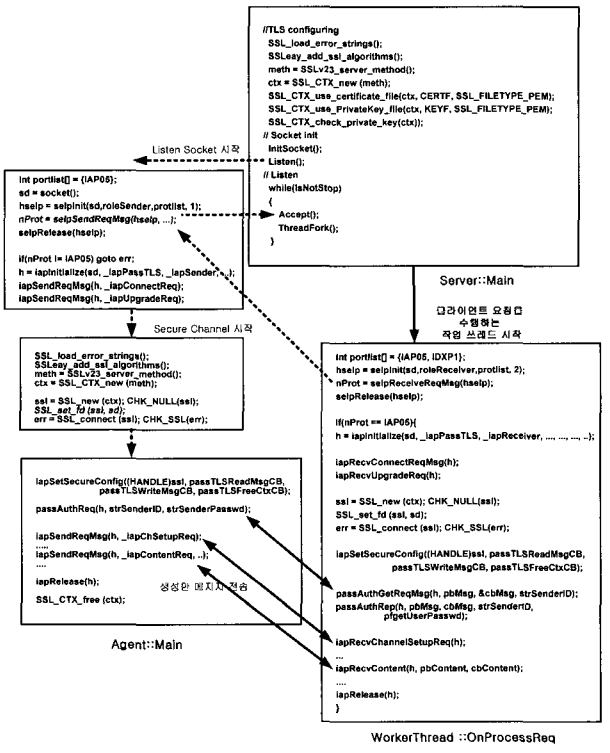
5.3 암호화 통신 모듈

본 논문에서는 암호화 통신 passTLS/1.0과 TLS/1.0, passOnly/1.0을 지원하기 위해 (그림 12)에서 처럼 TLS 라이브러리와 passTLS 라이브러리, passOnly 라이브러리를 구현하였다. 이들 라이브러리의 각 함수는 iapSetSecureConfig 함수를 통해 IAPCtx 구조체의 iapReadMsg, iapWriteMsg, iapFreeCtx에 설정되어서 이후에 IAP 함수들에 의해 호출된다. 패스워드 기반의 사용자 인증을 지원하는 passTLS/1.0과 passOnly/1.0은 4.3.1에서 제안된 인증 프로토콜을 기반으로 (그림 14)와 같이 구현되었다.



(그림 14) 패스워드 기반의 사용자 인증 모듈 API

(그림 14)에서 처럼 passAuthReq와 passAuthRep 함수는 IAPCtx 유형의 핸들 iapctx를 인수로 받아서 사용자 인증을 위해 교환되는 프로토콜 메시지를 passTLS 라이브러리나 혹은 passOnly 라이브러리의 ***WriteMsgCB/***ReadMsgCB 함수를 통해 전송한다. 또한, passAuthRep 함수는 콜백함수로서 getUserPasswd를 인수로 받아 다양한 사용자 패스워드 획득방식을 지원할 수 있다.



(그림 15) IDMEPL 적용 예

5.4 IDMEPL 적용 예

(그림 15)는 IDMEPL의 API를 적용한 예를 보인다. 프로토콜 선택단계에서 에이전트는 프로토콜 목록 protlist에 IAP05를 추가하여 서버에게 프로토콜 선택요청을 하였고 서버는 자신이 지원 가능한 프로토콜들의 목록 중에 IAP가 있는지 확인한 후, 승인여부를 결정한다. 만일 IAP가 승인되면 두 객체는 IAP 상에서 프로토콜 설정단계를 진행할 수 있다. (그림 15)의 예에서 IAP의 암호화 통신을 위해 passTLS/1.0이 선택되었고, 두 통신 객체는 보안설정 과정에서 TLS 핸드세이크와 패스워드 기반의 사용자 인증 과정을 거친다.

5.5 IDMEPL 분석

<표 3>에서처럼 IDMEPL은 4.1절에서 정의된 침입탐지 메시지 교환 절차의 요구사항을 만족한다. 즉 IDMEPL은 이기종의 다양한 침입(시도)탐지 에이전트들이 SDMS-RTIR과 실시간으로 상호연동을 할 수 있게 하며 자신이 속한 네트워크 환경에 상호인증 수준 이상의 적절한 암호화 통신 방법을 선택하도록 한다.

〈표 3〉 침입탐지 메시지 교환 절차 요구사항과 IDMEPL

요 구 사 항		IDMEPL
상 호 연동성	IDMEF 지원	libxml 2.4.16 및 libidmef 0.6.3 적용
	실시간 수준의 상호연동	IAP 프로토콜 구현 (libiap 1.0)
	추후 IDXP 지원 고려	libprotsel 1.0 구현
보안성	IDP 요구수준의 암호화 프로토콜 지원	OpenSSL 0.9.7 적용
	IDP 요구수준의 암호화 프로토콜 적용이 어려운 환경 지원	OpenSSL 0.9.7 적용/ libpassauth 1.0 구현

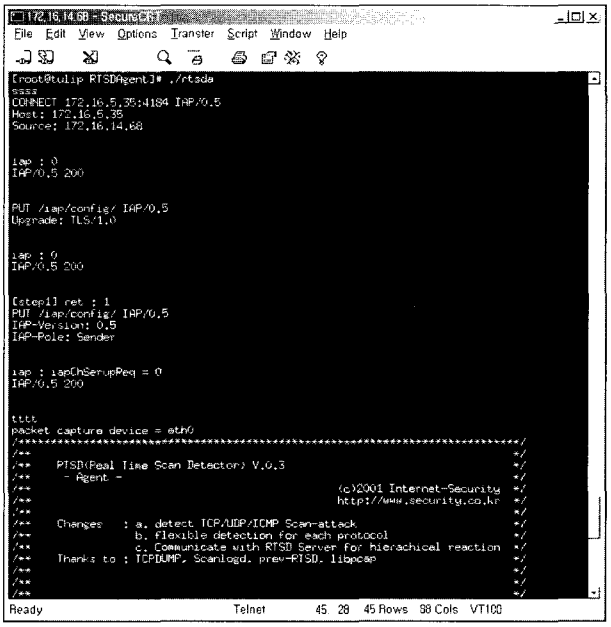
<표 4>는 기존 메시지 교환 라이브러리를 적용한 SDMS-RTIR과 IDMEF XML 플러그인을 탑재한 Snort, 최근에 제안된 IDXP를 지원하는 SIDI와 IDMEPL을 적용한 SDMS-RTIR의 비교분석을 나타낸다.

〈표 4〉 기존 구현들과의 비교

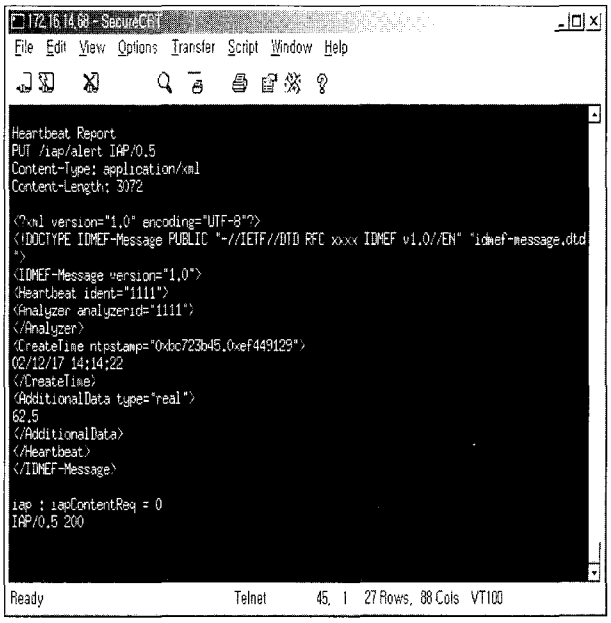
비 교 항 목		①	②	③	④
상 호 연동성	메시지 포맷	IDMEF	IDMEF	IDMEF	IDMEF
	메시지 교환 프로토콜	IAP	×	×	IDXP
	실시간 상호연동성	○	×	×	○
	유연성 있는 메시지 교환 프로토콜 선택 기능	○	×	×	×
보안성	TLS 1.0 지원	○	×	×	○
	IDP 요구수준의 암호화 프로토콜 지원	○	×	×	○
	네트워크 환경에 따른 유연성 있는 암호화 프로토콜 선택 기능	○	×	×	×

① 제안 SDMS-RTIR ② 기존 SDMS-RTIR ③ Snort ④ SIDI

Snort와 기존의 SDMS-RTIR이 단지 IDMEF만을 지원하는 것과 달리 IDMEPL이 탑재된 SDMS-RTIR과 SIDI는 각각 IAP와 IDXP를 지원한다. 비록 SIDI가 유력한 RFC 후보인 IDXP를 지원하고 있지만 SIDI는 유연성 있는 프로토콜 선택 구조를 지원하지 않기 때문에 IDXP 이외에 IAP 혹은 다른 메시지 교환 프로토콜을 갖는 이기종의 시스템들을 지원하기 어려운 단점이 있다. 반면 IDMEPL은 IAP 이외에 IDXP 혹은 다른 메시지 교환 프로토콜을 동시에 지원할 수 있는 구조를 제시하고 있다. 또한 IDMEPL은 TLS 1.0 이외에 패스워드 기반의 passTLS 1.0과 passOnly 1.0



(그림 16) RTSD 에이전트 시작 화면



(그림 17) Heartbeat 메시지 보고 절차

같은 암호화 프로토콜을 제공함으로써 다양한 환경과 네트워크에 대한 적용이 용이하도록 하였다. 이러한 IDMEPL 구조는 다양한 환경과 구조의 침입(시도)탐지 시스템들로부터 광범위한 침입(시도)탐지 메시지를 실시간으로 접수하고 분석해야 하는 대규모 침입(시도)탐지 및 대응 체계에 적합한 구조이다.

(그림 16)과 (그림 17)은 각각 SDMS-RTIR의 에이전트 RTSD의 첫 시작 화면과 Hearbeat 메시지의 보고 절차를 보여준다.

6. 결론 및 향후 연구 과제

본 논문에서는 SDMS-RTIR과 이기종의 침입(시도)탐지 에이전트들 사이에 실시간 수준의 상호연동을 지원하며 각종 보안위협에 안전한 침입탐지 메시지 교환 프로토콜 라이브러리 IDMEPL을 구현하였다.

IDMEPL 구현에 앞서 설계된 침입탐지 메시지 교환 절차는 프로토콜 선택, 프로토콜 설정, 메시지 전송의 3단계로 구성되며, 특히 프로토콜 선택과정을 통해 IAP와 IDXP와 같은 프로토콜 선택에 있어서 유연성 및 확장성을 지원하고 선택된 프로토콜을 통해 실시간 수준의 상호연동을 지원한다.

또한, 침입탐지 메시지 교환 절차에서 인증서 기반의 상호인증 옵션을 갖는 TLS 프로토콜을 지원할 수 없거나 TLS 프로토콜 자체를 지원할 수 없는 경우를 위해 패스워드 기반의 상호인증 프로토콜이 제안되었다.

IDMEPL은 설계된 침입탐지 메시지 교환 절차를 기반으로 구현되었으며 침입탐지 메시지 교환 절차의 요구사항인 상호연동성과 보안성을 만족함을 보였다.

IDMEPL의 적용을 통해 SDMS-RTIR은 이기종의 다양한 침입(시도)탐지 에이전트들로부터 광범위한 침입(시도)탐지 사고를 실시간으로 접수하고 분석할 수 있으며 이를 통해 국가적 공격대응 체계 확립에 기여할 수 있다.

또한, IDMEPL은 기존 시스템의 재사용과 탐지 영역 확대를 통한 기업내 통합 보안환경(ESM : Enterprise Security Management) 시스템의 프레임워크로 적용될 수 있다.

향후 연구 과제로서 IDMEPL을 위한 IDXP의 구현과 이기종의 침입(시도)탐지 에이전트들의 IDMEPL 적용 및 운영사례 분석이 요구된다.

참 고 문 헌

[1] 박수진, 박명찬, 이새롬, 최용락, "실시간 e-mail 대응 침입시도탐지 관리시스템의 설계 및 구현", 정보처리학회논문지C, 제9-C권 제3호, 2002.

[2] 유일선, 조경산, "네트워크 취약점 검색 공격에 대한 개선된 탐지 시스템", 정보처리학회논문지C, 제8-C권 제5호, 2001.

[3] 유일선, 김종은, 조경산, "네트워크 취약점 검색공격 탐지 시스템을 위한 보안성 있는 통신 프레임워크 설계", 정보처리학회논문지C, 제10-C권 제1호, 2003.

[4] 이현우외 4인, "대규모 네트워크취약점 검색공격 패턴분석 및 탐지도구", http://www.certcc.or.kr, 1999.

[5] 한국정보보호진흥원, "Hacking 통계자료", http://www.certcc.or.kr, 2001.

[6] 한국정보보호진흥원, "RTSD 2001년 통계자료", http://www.certcc.or.kr, 2001.

[7] B. Feinstein, G. Matthews, J. White, "The Intrusion Detection Exchange Protocol (IDXP)," <draft-ietf-idwg-beep-idxp-07>, 2002.

[8] D. Gupta, "IAP : Intrusion Alert Protocol," <draft-ietf-idwg-iap-05.txt>, 2001.

[9] D. Curry, H. Debar, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition," <draft-ietf-idwg-idmef-xml-10.txt>, 2003.

[10] libidmef 0.6.3, http://www.silicondefense.com/idwg/libidmef/.

[11] libxml 2.4.16, http://www.xmlsoft.org/.

[12] M. Jahnke, "SIDI - AN IMPLEMENTATION OF A SURVIVABLE INTRUSION DETECTION INFRASTRUCTURE," http://www.fgan.de/~jahnke/sidi/sidi.html, 2003.

[13] M. Wood, M. Erlinger, "Intrusion Detection Mesage Exchange Requirements," <draft-ietf-idwg-requirements-10.txt>, 2002.

[14] OpenSSL 0.9.7, http://www.openssl.org/.

[15] R. Fielding외 6인, "Hypertext Transfer Protocol - HTTP/1.1," RFC 2616, 1999.

[16] R. Pollock외 6인, "Implementing the Intrusion Detection Exchange Protocol," 17th Annual Computer Security Applications Conference, 2001.

[17] Silicon Defense, "IDMEF XML plugin for the Snort IDS," http://www.silicondefense.com/idwg/snort-idmef/.

[18] Snort, http://www.snort.org/.

[19] T. Dierks, C. Allen, "The TLS Protocol Version 1.0," RFC 2246, 1999.

유 일 선

e-mail : qjemfahr@security.co.kr

1995년 단국대학교 전산통계학과(이학사)

1997년 단국대학교 일반대학원 전산통계학과(이학석사)

2002년 단국대학교 일반대학원 전산통계학과(이학박사)

1997년~2000년 (주)한조엔지니어링 연구원

2000년~현재 (주)인터넷시큐리티 선임연구원

관심분야 : 침입탐지, 네트워크보안, 사용자 인증 및 접근통제

이 동 련

e-mail : ryuni@cert.certcc.or.kr
1999년 순천향대학교 전산학과(공학사)
1991년 순천향대학교 일반대학원 전산학과 (공학석사)
2000년~현재 한국정보보호진흥원 연구원
관심분야 : 침입탐지, 네트워크보안, 사용자 인증 및 접근통제

오 은 숙

e-mail : esoh@cert.certcc.or.kr
1999년 순천향대학교 전산학과(공학사)
1991년 순천향대학교 일반대학원 전산학과 (공학석사)
2000년~현재 한국정보보호진흥원 연구원
관심분야 : 침입탐지, 네트워크보안