전자상거래 서비스를 위한 통합 관리 시스템의 보안 에이전트

서대희[†] · 이임영[††]

요 약

최근 인터넷의 급속한 보급으로 인터넷을 이용한 사회 활동이 증가하고 이에 따라 전자상거래 분야에 대한 관심이 높아지고 있다. 실세계에서의 상거래를 가상 공간인 인터넷으로 그대로 옮긴 전자상거래는 암호화된 기반 구조와 안전한 프로토콜을 통해 온라인으로 연결되어야 하며 이러한 상거래 환경에서는 정보의 보안성, 개별 거래에 대한 인증체계, 전자 지불 수단 및 관련 체계 등의 기본 조건이 만족해야 한다. 따라서 현재 많은 전자상거래 시스템들이 구축되어 서비스되고 각 시스템 별로 별도의 관리자를 두어 상호간의 정보를 교환하여 서로의 시스템을 보안에 관한 정보를 서로 상호 보안적인 관계를 유지하면서 시스템을 보안하고 있다. 본 논문에서는 관리자의 개입 없이도 많은 정보와 작업을 관리하여 전자상거래에서 많은 연구가 진행중인 에이전트를 이용하여 사용자에게 안전한 전자상거래 서비스를 제공하기 위한 보안된 시스템 관리를 제시함으로써 보다 안전하고 편리한 전자상거래 서비스를 위한 보안 기법을 제안한다.

A Secure Agent of Integrated Administration System for the Electronic Commerce

Dae-Hee Seo[†] and Im-Yeong Lee[††]

ABSTRACT

Nowadays economic and commercial businesses have been increased because of the Internet. As a result of this, electronic commerce is becoming one of the most interesting topic of discussion. Electronic commerce is equal to a real market, only the place of business is the imaginary space supported by the Internet. There are a few conditions to consider, making electronic commerce work safely. The electronic commerce should be connected by a substantial system and an on-line protocol. There are some conditions needed for information security, authentication, and payment by electronic currency, etc. Although there are many kinds of existing systems, which create services successfully, further research for security is required. Therefore, this paper suggests an authenticated Agent management, which offers more convenience and security than before. Also, this paper shows many authenticated methods for a management system. An Agent that is one of interesting things to study can handle information problems and works related to electronic commerce.

Key words: E-Commerce, Mobile 에이전트, 통합 관리 시스템

1. 서 론

최근 인터넷의 급속한 보급으로 인터넷을 활용한 사회 활동이 급증하면서, 전자상거래 분야에 대한 관심도 고조되고 있다. 전자상거래에서 제공되는 E-mail이나 웹과 같은 정보 스트림으로 제공되는 정보의 양은 엄청나며, 그 종류도 뉴스정보, 상품 카탈로그, 영화 스케줄 등 매우 다양하다. 하지만 이처럼 웹을 통해 접근 가능한 테라바이트 수준의 정보량에 비해 실제 사용자 개개인이 필요로 하는 정보는 극히 일부분이며, 이러한 현상을 정보과다(Information

[†] 준회원, 순천향대학교 전산학과 석사과정
[††] 종신회원, 순천향대학교 정보기술공학부 부교수

Overload)라고 표현할 수 있다. 이 정보과다로 인해 생산성 증대, 교육적 이득, 오락적 가치 등 인터넷을 이용한 이점이 위협받을 수 있다. 이렇게 인터넷의 정보 홍수 속에서 원하는 정보를 정확하게 제시간에 얻기란 쉬운 일이 아니며, 따라서 이러한 작업을 대신해 주는 에이전트의 역할이 점점 커지고 있다.

또한 전자상거래에서 제공해야 하는 서비스와 새로운 요구 기능의 출현 주기가 점점 짧아질 뿐만 아니라, 서비스와 요구 기능 자체의 다양성도 점차 증가하고 있다. 따라서 전자상거래에서 이들 서비스 및 요구 기능을 시기 적절하게 지원하기 위해서는 네트워크 구조가 유연(Flexible)하고 환경 변화에 쉽게 대응할 수 있는 적합성(Adaptive)을 가지는 구조로 변화되어야 한다.

따라서 본 논문의 2장에서는 통합 관리 시스템에 대해서 알아보고 통합 관리 시스템에 에이전트를 적용하기 위한 보안적인 요구사항을 제시한다. 3장에서는 기존 관리 시스템인 ISMS(Integrated Security Management System)와 네트워크에 적용된 에이전트에 대한 취약성 분석을 통해 4장에서 에이전트를 이용한 새로운 보안 기법을 제안하고자 한다. 5장에서는 제안 방식과 기존 방식을 2장에서 제시한 보안적인 요구사항을 기반으로 분석한 뒤 6장에서 결론을 맺고자 한다.

2. 통합 관리 시스템

전자상거래에서는 다수의 시스템이 설치되었을 경우 각 시스템 별로 별도의 관리자를 두어 상호간의 정보를 교환하여 서로의 시스템을 보안하고 있다. 그러나 잘못된 정보에 의해 상호 교환된 정보는 시스템에 치명적인 취약점을 만들 수 있다. 따라서 최근에 이러한 문제점을 보안하기 위해 통합 관리 시스템을 통해 관리자가 이기종으로 구성된 보안 제품들을 통합 관리할 수 있기 때문에 관리의 편의성을 제공 받으며, 보안위협에 빠르고 정확하게 대처할 수 있다는 장점을 가지고 있다.

통합 관리 시스템이 중앙에서 각 시스템들의 보안 정책 및 관리에 필요한 정보를 관리해 줌으로써 통합된 인터페이스를 제공해 주어 전반적으로 통합된 보안 정책을 수립할 수 있으며 시스템들을 전체적으로 점검하여 문제가 발생할 수 있는 정책의 유무와 정책 수정에 따른 결과를 예측할 수 있다[1,2,5,6].

따라서 전자상거래에서 활용할 수 있는 통합 관리 시스템에 에이전트를 적용하기 위해서는 다음과 같은 보안 요구사항을 만족해야 한다[3-5,7].

- ***신뢰성*** : 에이전트가 정보를 수집하여 전달할 경우 객관적인 판단 능력을 가진 객체를 통하여 이에 대한 결정이 이루어져야 한다.
- ***무결성***: 에이전트가 노드에서 악의적인 공격으로부터 무결성 유지를 위한 보안적 서비스가 이루어져야 한다.
- ***기밀성***: 에이전트가 수행하고자 하는 코드들에 기밀성을 유지해야 한다.
- ***기밀연산***: 에이전트는 원격지에서 초기 비밀키를 노출시키지 않고 수행해야 한다.
- ***인증***: 에이전트 및 모든 객체들의 상호 인증을 통해 정당한 객체간에 통신을 보장해야 한다.
- ***상호 운용성***: 시스템간의 상호 운용성을 보장해야 한다.
- ***시간적인 지연***: 공격자에 의한 공격시 이에 대한 대비와 그에 상응하는 대응이 신속히 이루어져야 하며 수집된 정보를 시간 지연 없이 전송해야 한다.
- ***객체공격***: 에이전트와 관계된 네트워크 객체들의 공격에 대한 보안대책이 있어야 한다.
- ***우선순위***: TTP의 특정 정책에 의한 에이전트의 우선 순위가 배제 되어야 한다.
- ***정책***: 새로운 에이전트에 대한 객관적인 판단으로 시스템 관리자가 중심이 되는 정책이 이루어져야 한다.
- ***명령어 제약***: 에이전트 수행에 대한 제약이 이루어져서는 안된다.
- ***Overhead***: 해당 모든 객체들간의 Overhead를 최소화 하여야 한다.
- ***TTP 의존도***: TTP의 의존도를 최소화 하여야 한다.

3. 기존 방식 분석

3.1 ISMS(Integrated Security Management System)

ISMS는 네트워크에 산재되어 설치된 각 보안 시스템들을 관리하는 보안 시스템 관리 전담 에이전트와 전체적인 관리 동작을 수행하는 하나의 통합 서버 그리고 웹 인터페이스를 제공하는 Manager로 구성

되어 있다.

기능적으로는 보안 시스템에 대해 제한되지 않고 폭넓은 이기종 보안 시스템 및 운영 플랫폼을 지원하며 가상 보안 도메인을 설정하고 도메인 내의 보안관리에 일관성을 부여하며 통합보안관리 서버에서 자동화된 보안정책의 일관성을 검사하거나 관리자 인터페이스를 통합 관리한다[5].

ISMS는 기술된 3-tire Broker Model 구조를 가지며 네트워크에 산재되어 설치되어 있는 각 보안 시스템들은 보안 시스템 관리 전담 Agent와 전체적인 관리 동작을 수행하는 하나의 통합관리 서버, 그리고 웹 인터페이스를 제공하는 매니저로 구성되어 있다. ISMS는 통합 보안관리를 위해서 망관리 표준 프로토콜인 SNMP를 사용하면 시스템 공통의 MIB를 정의해야 하고 이를 사용하는 Agent 기능을 추가로 구현하거나 해당 보안관리 시스템과 전담 Agent 사이의 표준화된 API를 정의해야 한다[1,2].

그러나 ISMS는 다음과 같은 문제점을 가지고 있다[5,12].

- ***신뢰성*** : 관리자가 생성한 에이전트가 정보를 수집하여 관리자가 이를 판단하는 형식으로 인해 관리자의 주관적인 판단이 개입될 우려가 있다.
- ***무결성*** : 에이전트가 목표 시스템에서 정보 수집 작업을 완전히 마치고 다시 되돌아올 때까지 악의적인 공격으로부터 무결성 유지를 위한 보안적 서비스가 없다.
- ***기밀성*** : 에이전트가 수행하고자 하는 코드들에 안전한 기밀성을 유지하지 못한다.
- ***기밀연산*** : 에이전트는 원격지에서 초기 비밀키를 노출시키지 않고 수행하지 못한다.
- ***인증*** : 현재의 SNMP(Simple Network Management Protocol) 프로토콜에는 상호 인증 기능이 없다.
- ***상호 운용성*** : 현재의 ISMS에서는 보안 시스템 간의 상호 운용성이 부족하다.
- ***시간 지연성*** : 관리자가 모든 정보를 통합하여 보안 정책 및 방화벽의 재구성으로 인한 시간적인 지연을 통해 공격자에 대한 대응이 지연된다.

3.2 기존 네트워크에서의 에이전트 보안 방식

가. 대리서명을 이용한 방식

본 방식은 대리서명 기법을 이용하여 안전한 에이전트의 패러다임을 구현하고자 하는 방법으로써 사용자 비밀키의 노출 없이 에이전트의 계산을 호스트에서 수행하도록 하는 방식이다.

대리서명 방식은 에이전트가 서명 함수를 전달하지 않고도 공개 가능한 데이터의 전송으로 사용자의 비밀키의 안전성을 보장하고 사용자를 대신한 서명을 생성하여 서버와의 인증을 통해 안전한 통신을 하고자 하는 방식이다[9].

대리서명이 방식의 경우 에이전트의 서명에 대한 유효값을 계산하는 것이 가능하게 되므로 주문 정보간의 우선순위 정책을 두어 분쟁을 최소화 하고자 하였으며, 악의를 가진 호스트가 취할 수 있는 취약점을 보안하고자 하였으나 다음과 같은 문제점을 가지고 있다[9,12].

- ***인증*** : 호스트와 에이전트 사이의 인증이 호스트가 에이전트를 인증하는 일방향 인증으로 악성 호스트에 대한 에이전트의 보안 대책이 없다.
- ***객체공격*** : 에이전트나 호스트가 공격자로부터 공격을 받았을 경우 쉽게 객체에 대한 정보의 취득이 가능하여 위장할 수 있는 문제점이 있다.
- ***우선순위*** : 일정한 필요 정보에 대한 우선 순위를 결정하고 시행함에 따라 TTP(Trusted Third Party)나 신뢰기관의 참여가 불가피하다.

나. 등급부여를 통한 방식

본 방식은 에이전트에 등급을 부여하여 등급에 따라 집합을 정의함으로써 에이전트를 제어하는 방법이다.

등급 부여 방식이 경우 사람을 대신하는 에이전트의 침입시 불법적인 행위에 따른 감시 및 행동에 대한 침입탐지 시스템에 대해 설계하고 실험의 대상으로 한 조직내에서 각기 다른 역할을 수행하는 에이전트를 가정하고 소속된 에이전트가 서버에 접속할 경우 사람에게 주어지는 등급과 달리 그 사람에게 소속된 에이전트에게 등급을 부여함으로써 현재 많이 이용되어지고 있는 에이전트를 제어하고 서버를 보호하고자 하는 방식이다[10].

그러나 이 방식은 다음과 같은 문제점을 가지고 있다[3,7].

- ***인증*** : 임의의 새로운 에이전트의 인증 단계에서 에이전트가 가져야할 보안적 요구사항 중 기밀성을 중심으로한 인증을 통하여 서버가 공격당했을 경

우 공격자에 의해 계속된 악성 에이전트 인증이 가능하다.

• ***명령어 제약*** : 에이전트의 명령어에 대한 제약이 이루어지는 가운데 에이전트간에 상호 인증 명령어 역시 제약되므로 상호 인증이 불가능하다.

다. 정책 프로토콜을 이용한 방식

본 방식은 안전한 통신 설정을 위해 특정 정책을 기반으로 이루어진 보안 프로토콜로써 서로 다른 보안 영역간의 에이전트의 협상에 대하여 보안 모델을 제시하였다.

SPS는 호스트와 보안 게이트웨이에게 안전한 통신 설정을 위해 필요한 보안 정책정보를 제공하는 분산시스템이다. 보안 영역의 호스트, 서브넷, 망의 보안정책 정보를 발견, 접근 처리하기 위해 필요한 매커니즘을 제공한다. 특히 SPP(Security Policy Protocol)을 사용해서 정책 클라이언트와 서버들은 정보를 교환한다. 이 프로토콜은 클라이언트와 서버에 의해 정책 정보가 어떻게 교환, 처리 및 보호되는지를 정의한다[11].

그러나 이 방식은 다음과 같은 문제점을 가지고 있다[3,5,9,13].

• ***Overhead*** : 각각의 에이전트, 서버간에 통신 Overhead가 커진다.

• ***인증*** : 각 서버와 서버, 에이전트와 에이전트간에 이루어지는 정보의 교환에서 자료의 무결성에 대한 입증이 안된다는 단점이 있으며 객체간에 상호인증 없이 객체인증을 통한 악성 에이전트 또는 서버에 대한 부정이 발생할 수 있다.

• ***정책*** : 정책설정만을 통한 에이전트의 인증으로 정책 서버가 공격당했을 경우 에이전트에 대한 모든 인증이 위협을 받게 된다.

4. 새로운 에이전트 보안 기법 제안

본 제안 방식은 인터넷 환경에서 많은 전자상거래 시스템을 운영할 경우 각 시스템간의 일관된 보안 정책을 통해 사용자에게 안전하고 신뢰성 있는 서비스를 제공하기 위해 에이전트를 이용한 관리 기법을 제안한다. 제안 방식의 구성 객체는 관리서버, TTP, 에이전트, 전자상거래 서비스 시스템으로 구성된다.

4.1 구성 요소

본 논문에서 제안한 통합 관리를 위한 보안 에이전트 방식을 구성하는 객체는 다음과 같다.

• ***관리 서버*** : 관리 서버는 임의의 네트워크를 담당하여 네트워크 안에 위치한 모든 전자상거래 서비스 시스템들의 보안적인 관리를 실시한다. 관리 서버는 에이전트를 이용하여 각 시스템들의 정보를 수집하고 이를 기반으로 적절한 보안 정책을 수립하여 통합적인 보안 관리 시스템으로써의 역할을 수행한다.

• ***TTP*** : TTP는 에이전트의 생성 및 관리를 담당하는 신뢰 기관으로써 관리 서버와는 독립적으로 운영되며, 관리 서버의 요구가 있을 경우 관리 서버의 요구에 맞는 에이전트를 생성 후 에이전트를 관리한다. 또한 에이전트가 수집한 정보를 수집하여 관리 서버에게 이를 통보하며, 관리서버와 전자상거래 서비스 시스템들의 상호인증을 통한 안전한 통신을 보장한다.

• ***에이전트*** : 관리 서버의 요구에 의해 생성된 에이전트는 전자상거래 서비스 시스템들의 보안적인 정보를 수집하고 공격으로 의심되는 보안 침해 요소나 침해당한 시스템의 정보들에 관하여 모든 해당 정보들을 수집하여 TTP에 이를 전송한다.

• ***전자상거래 서비스 시스템*** : 관리 서버가 관할하고 있는 임의의 네트워크 구성 요소로서 독립적인 보안 정책을 가지고 사용자에게 전자상거래 서비스를 하는 객체이다.

4.2 제안방식 시나리오

본 논문에서 제안한 새로운 에이전트 보안 기법은 구성 객체들간의 프로토콜은 다음과 같이 3개의 단계로 이루어진다.

단계 1 : 초기화 설정 단계

관리 서버는 전자상거래 서비스를 제공하는 여러 시스템들에 대한 보안 설정 및 정책 수립을 위하여 TTP에 에이전트의 생성을 요구한다. TTP는 에이전트 생성 요구에 따라 에이전트를 생성하고 에이전트만이 가지는 고유 비밀 정보를 생성하고 관리 서버에게 이를 전송한다.

단계 2 : 전자상거래 서비스 시스템과의 상호 인증

및 통신 단계

관리 서버는 전자상거래 서비스 시스템으로부터 보안에 대한 정보를 수집하고자 에이전트를 활성화 시킨다. 활성화된 에이전트는 관리서버가 관리하는 모든 전자상거래 서비스 시스템의 현재 보안정책 및 보안 수준에 대한 정보를 수집하고 이를 TTP에게 전송한다.

에이전트가 정보를 수집하고자 할 때 각각의 전자상거래 서비스 시스템과는 TTP를 통한 상호인증으로 안전한 통신을 보장한다.

단계 3 : 검증 및 공표

TTP는 에이전트가 전송한 정보에 관하여 무결성 및 기밀성을 검증하고 초기 생성했을 때 비밀 정보와 비교했을 때 정당성이 입증될 경우 전송 받은 정보를 저장하고 관리 서버의 요구가 있을 경우 이를 해당 게시판에 공고한다.

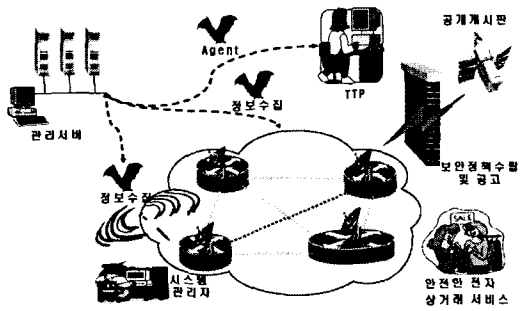


그림 1. 제안방식 시나리오

4.3 시스템 계수

다음은 새로운 방식의 에이전트 보안 기법을 제안하는데 필요한 시스템 계수를 기술한다.

* : 관리서버 : D, TTP : T, 에이전트 : A, 시스템 : S

α_* : *가 생성한 소수 ($512bit \le Length \le 1024bit$, $2^{L-1} < \alpha_* < 2^L$을 만족하는 소수)

β_* : $\beta_* | (\alpha_* - 1)$

x_*, y_* : 공개키 암호 알고리즘 E를 기반으로 한 *의 개인키, 공개키

E : 공개키 암호 알고리즘

T_* : *가 생성한 Time Stamp

$S_*\_@$: *에서 @로 전송되는 공개키 서명값

Sig_* : *의 개인키를 이용한 공개키 서명 알고리즘

R_A, S_A : 에이전트가 갖는 고유 서명값

r_* : *에 의해 생성한 랜덤 수

Y_* : 상호인증 검증값

g, n : 모든 객체에 공개된 시스템 계수

ID_* : 객체 *의 정보

M_* : *의 정보 요구 메시지 (시스템의 이름, 현재 진행중인 보안 프로세스 ID, 의심되는 시스템 로그가 있을 경우 로그를 남긴 Time Stamp, 해당 시스템의 이름, 에이전트 ID, 정보 수집때의 Time Stamp)

$h@\_*$: @에서 *로 전송되는 안전한 해쉬 값

H : 안전한 해쉬 함수

M_{res_*} : *의 정보 요구 메시지에 대한 응답 메시지

J_* : 에이전트를 제외한 모든 객체들의 검증 값

$V*\_@$: *에서 @로 전송되는 암호화된 값

4.4 프로토콜

제안 방식의 프로토콜은 임의의 네트워크의 전자상거래 시스템들의 보안적인 관리를 위해 에이전트를 활성화하여 전자상거래 시스템들의 보안 정책을 유지 및 관리를 위한 통합 보안 관리 시스템의 프로토콜로서 초기 설정 단계, 에이전트와 전자상거래 서비스 시스템간의 상호 인증 단계, 프로토콜 단계로 이루어진다.

가. 초기 설정 단계

관리 서버는 TTP에 관리 서버의 정보 (서명자 이름, ID, 소속, 기타)를 제공하여 에이전트 생성을 요구한다.

1) TTP는 관리 서버의 확인이 끝난 후 정당한 요구일 경우 R_A, S_A를 고유값으로 갖는 에이전트를 생성한다.

$K_T = g^{r_T} \bmod n$

$R_A = K_T \bmod \beta_T$

$S_A = r_A(H(ID_A) + \beta_T R_A) \bmod \beta_T$

$Y_A = (g \times K_T)^{(r_A \times r_T)} \bmod n$

Y_A는 TTP에서 에이전트 활성화 후 임의 네트워

크에서 동작하여 에이전트의 인증을 요구 받을 경우 에이전트의 인증을 위해 임시 저장하고, 생성된 고유값과 K_T, T_T를 연접하여 자신의 공개키 서명을 취한 값인 ST_A, Y_A, ID_A를 에이전트에 전송한다.

$ST\_A = Sig_T(K_T||R_A||S_A||T_T)$

2) 에이전트는 TTP의 공개키 서명을 확인 한 뒤 ST_A, Y_A, ID_A를 고유 코드로 하여 관리 서버에 할당되며, TTP는 에이전트 생성을 요구한 관리 서버에 에이전트를 대신하여 다음의 내용을 전송한다.

$VT\_D = E_D\{(ST\_A ||ID_A||Y_A||r_T)\}$

3) 관리 서버는 자신의 비밀키로 VT_D를 복호화 한 뒤 ST_A를 TTP의 공개키로 복호화 하여 에이전트의 서명을 확인하고 자신이 요청한 정보가 맞는 에이전트가 생성 되었는지 확인하고 r_T, Y_A, K_T를 저장한 뒤 이벤트 종결 메시지를 송신한다.

나. 에이전트와 전자상거래 서비스 시스템간의 상호 인증 단계

다음의 단계는 관리 서버가 여러 전자상거래 서비스 시스템에 대한 현재 보안 정책 및 보안 사항에 관한 정보를 수집의 위해 에이전트와 전자상거래 서비스 시스템간의 상호 인증 단계이다.

1) 보안 정책 및 보안 사항에 대한 정보를 수집하기 위하여 에이전트는 전자상거래 서비스 시스템에 접속을 요구하는 요청 메시지를 송신하며 이를 인지한 전자상거래 서비스 시스템은 TTP에 에이전트의 접속 요구에 대한 메시지를 전송한다.

2) TTP는 접속 요구 에이전트에게 ST_A, ID_A, Y_A의 정보를 요청하며, 전자상거래 서비스 시스템에게는 VS_T를 요청한다.

3) 에이전트는 자신의 고유 코드인 ST_A, ID_A, Y_A를 TTP에서 전송하며, 전자상거래 서비스 시스템은 VS_T를 계산하여 TTP에 이를 전송한다.

$K_S = g^{r_S} \bmod n$

$Y_S = (g \times K_S)^{r_S} \bmod n$

$VS\_T = E_T(Y_S||r_S||T_S)$

4) TTP는 에이전트의 초기값 Y_A의 검증을 통해 정당한 에이전트인지를 확인한 뒤 다음을 계산하여 hT_A를 에이전트에게 전송한다.

$K_T = g^{r_A} \bmod n$

$Y_T = (g \times K_T \times K_A \times K_S)^{r_T} \bmod n$

$hT\_A = H(Y_T||T_T)$

5) TTP는 VS_T를 복호화 한 뒤 VT_S를 계산하여 전자상거래 서비스 시스템에 VT_S,를 전송한다.

$K_T = g^{r_T} \bmod n$

$Y_T = (g \times K_T \times K_A \times K_S)^{r_T} \bmod n$

$hT\_S = H(Y_T||T_T)$

$VT\_S = E_S(Y_T||hT\_S)$

6) 전자상거래 서비스 시스템은 VT_S를 자신의 개인키로 복호화 한 뒤 Y_T와 hT_S를 임시 저장한다.

7) 에이전트는 TTP에서 전송받은 hT_A를 자신의 고유값과 함께 전자상거래 서비스 시스템에게 ($ST\_A||hT\_A$)를 전송한다.

8) 전자상거래 서비스 시스템은 TTP에게서 전송받은 Y_T와 hT_S를 이용해 안전한 해쉬 값을 생성한 뒤 hS_A를 에이전트에 전송한다.

$hS\_A = H(Y_T||hT\_S)$

9) 에이전트와 전자상거래 서비스 시스템은 전송된 해쉬값을 비교함으로써 Y_T에 대한 무결성을 검증하고 상호인증 이벤트 종결 메시지를 TTP에 전송한다.

다. 프로토콜 진행 단계

1) 관리 서버는 다음을 계산한 뒤 VD_A, M_D를 에이전트에 전송한다.

$J_D = (H(M_D) \oplus H(K_D||K_T)) \bmod n$

$VD\_A = E_S(K_D||J_D||T_D||M_D)$

2) 에이전트는 VD_A에 자신의 고유값과 함께 ($VD\_A||ST\_A$), hA_S를 전자상거래 서비스 시스템에 전송한다.

$hA\_S = H(ST\_A||T_A)$

3) 전자상거래 서비스 시스템은 전송된 hA_S에

서 ST_A의 무결성을 확인하고 VD_A에서 K_L, S_L를 확인 후 다음을 계산하여 VS_A를 에이전트에게 전송한다.

$$J_S = (H(M_{res_s}) \oplus H(K_S \| K_T)) \mod n$$

$$VS\_A = E_{S_i}(J_S \| T_S \| M_{res_s} \| K_S)$$

4) 에이전트는 VS_A에 자신의 고유값과 함께 $(VS\_A \| ST\_A)$, hA_D를 TTP에 전송한다.

$$hA\_D = H(ST\_A \| T_A)$$

다. 검증 단계

관리서버와 시스템에서는 다음과 같은 과정을 통해 그 유효성을 입증할 수 있다.

관리서버 : $H(M_{res_s}) \oplus H(K_T \| K_S) = J_S \mod n$

시스템 : $H(M_D) \oplus H(K_T \| K_D) = J_D \mod n$

관리서버와 시스템은 J_*의 검증을 통해 전송된 정보의 기밀성과 무결성을 확인하고 이에 대한 프로토콜 종결 메시지를 에이전트에게 전송한다.

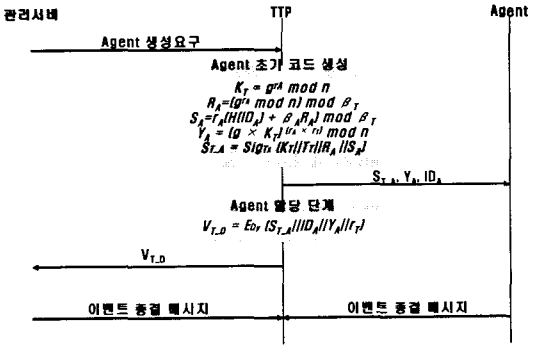


그림 2. 초기 생성 단계

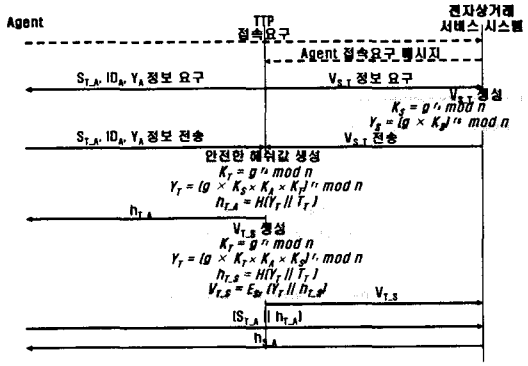


그림 3. 상호인증 단계

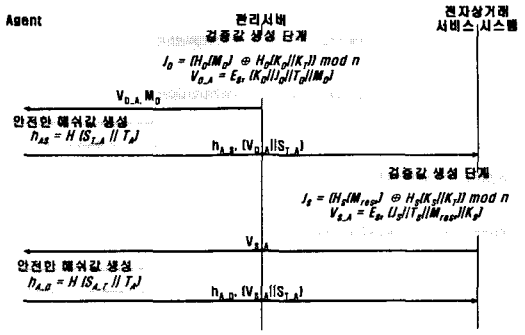


그림 4. 프로토콜 단계

에이전트는 해당 정보를 TTP에 전송하고 TTP는 에이전트 수집한 정보를 저장한다.

정보를 전달한 에이전트는 최종 목표 시스템까지 이동하는 동안의 중간 시스템들을 대상으로 ***가~다*** 까지의 프로토콜을 수행하여 TTP에 이를 제공함으로써 정보 수집 및 사용자 추적을 실시한다(그림 2-4 참조).

5. 제안 방식 분석

기존의 에이전트와 통합관리시스템을 고려할 경우, 본 방식은 다음과 같은 특징을 보유하고 있다.

- ***무결성*** : 에이전트는 자신의 서명값과 안전한 해쉬값을 이용하여 관리자와 모든 시스템간의 정보를 전송함으로써 무결성 유지가 가능하다.
- ***기밀성*** : 에이전트가 코드 수행시 TTP에서 계산된 비밀값이 에이전트에 포함되므로 기밀성을 유지할 수 있다.
- ***기밀연산*** : 에이전트는 원격지에서 TTP의 초기 비밀 값을 노출시키지 않고 J_*으로 메시지의 유효성을 검증함으로써 기밀연산 수행이 가능하다.
- ***정책*** : 제안 방식은 에이전트에 대한 특정 정책이 없는 환경에서 적용이 가능하다.
- ***TTP의 의존도*** : TTP가 모든 객체를 인증함으로써 TTP의 의존도가 높다.
- ***인증*** : 프로토콜을 이루는 해당 객체는 디지털 서명과 검증값을 이용해 상호 인증이 가능하다.
- ***신뢰성*** : 관리자의 요구에 의해 TTP가 에이전트를 생성하고 그에 대한 정보를 관리하여 관리자의

표 1. 제안방식 분석

	대리서명	등급부여	프로토콜 방식	통합보안관리 시스템	제안방식
무결성	×	×	×	△	○
기밀성	○	○	×	×	○
기밀 연산	×	×	×	×	○
정책	×	○	○	○	○
TTP 의존도	높다	높다	높다	낮다	높다
신뢰성	△	○	△	△	○
상호 운용성	×	×	×	△	○
시간 요소	×	×	×	×	○
인증	객체 인증	객체 인증	객체 인증	상호 인증	상호 인증
객체공격	×	△	△	×	○
우선 순위	×	△	△	×	○
명령어 제약	△	×	△	×	○
Overhead	△	△	×	△	△

[× : 위험, △ : 취약, ○ : 안전]

주관적인 판단이 배제된 에이전트 관리가 가능하다.

• ***상호 운용성*** : 상호 시스템간의 TTP의 정보 공유에 따른 상호 운용성이 향상된다.

• ***시간적인 지연*** : 최종 시스템까지 정보를 수집하여 공개하는 것이 아닌 목표 시스템까지 이동하는 중간 시스템들에 대한 정보들을 수집하여 공개하는 방식을 통한 시간적인 지연을 최소화하였다.

• ***객체공격*** : 제안 방식은 전체 시스템에서 하나의 침해 시스템이 발생했을 경우 이를 위한 정보와 추적이 동시에 이루어지며, 수집된 정보를 바탕으로 관리자의 보안 정책을 통해 객체 공격의 안전성을 유지할 수 있다.

• ***우선순위*** : TTP의 특정 정책에 의한 에이전트의 우선 순위를 지정하지 않는다.

• ***명령어 제약*** : 제안 방식은 에이전트의 명령어 제한이 이루어지지 않는다.

• ***Overhead*** : 각 해당 객체를 TTP를 중심으로 상호 인증이 진행되고 각 시스템의 정보를 독립적으로 처리하므로 Overhead는 크다고 할 수 있다.

다음의 표 1은 기존의 방식과 제안 방식을 비교 분석한 결과이다.

6. 결 론

정보화 시대가 급격하게 발전함에 따라 보안에 대한 중요성이 확산되고, 정보전 해킹 등 보안의 역기능에 따른 내부정보의 보호를 위해 많은 보안 시스템이 도입되고 있다. 그러나 이러한 보안 시스템이 구축되는 과정에서 관리자는 서로 다른 사용자 인터페이스에 따른 관리의 부담이 가중되고 효과적인 관리가 어려워지면서 통합 보안관리 시스템의 필요성이 대두되었다. 이와 더불어 전자상거래 서비스의 활성화에 따른 정보보호제품의 기능과 역할도 중요하지만 이들을 통해 사용자에게 일관된 정책과 통합관리를 실현하는 것 역시 매우 중요한 초점이 되고 있다.

따라서 본 논문에서는 전자상거래 서비스 시스템에 적용한 통합 보안 관리 시스템에 대해 고찰하였다. 본 논문에서 제안한 방식은 에이전트가 가져야 되는 안전성 뿐만 아니라 기존 통합 관리 시스템이 제공하지 못했던 보안 사항까지 제공하였다. 이는 현재 전자상거래 서비스를 보다 안전하고 효율적으로 확대하는데 중요한 연구 분야이며, 향후 무선 전자상거래 서비스까지를 고려하였을 경우 지속적인 연구가 필요한 분야라 할 수 있다.

참 고 문 헌

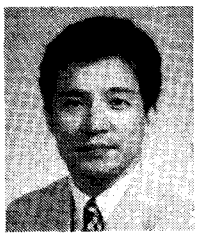
[1] Modori Asaka, "Information Gatehering with mobile Agents for an intrusion Detection System," System and Computers in Japan.

Vol.30, No.2, 1999.
[2] Dan Sterne, "Active Network intrusion Detection and Response (AN-IDR)", Boeing and NAI Lab., DARPA FTN PI Meeting, Jul. 20, 2000.
[3] Tomas Sander, Christian F. Tschudin, "Towards Mobile Cryptography," Proceedings of the IEEE Symposium on Security and Privacy, 1998
[4] 신원, "안전한 이동 에이전트 시스템의 설계와 응용", 전자계산학과 박사학위논문, 부경대학교, 2001.
[5] ETRI 네트워크 보안 연구부, "차세대 인터넷을 위한 능동 보안 기술 백서", 한국전자통신연구원, 2001.
[6] 한국정보처리학회, "Active Network와 Security 기술 기반", Sigcomm Review, Vol.1 No.1, 2000.
[7] 박종열, 신욱, 이동익, "이동코드와 보안문제", 정보처리학회학회지, Vol 7 No.2, 2000.
[8] 장병탁, 이종우, 서용우, "학습 에이전트", 정보과학회지 제 18권 5호, p26, 서울대학교, 2000.
[9] 김희선, 백준상, 이병천, 김광조, "대리서명을 이용한 모바일 에이전트의 안전성 강화 방법 (Enhancing Security of Mobile Agent using Proxy Signature)", KIISC 종합학술발표회 (CISC2000), 종합 학술발표 논문집 Vol. 10 No. 1, pp.424~437, 성균관대학교, 2000.
[10] 임용성, 장덕성, 정홍 "명령어 등급 부여를 통한 에이전트의 불법행위 방지에 관한 연구", 정보처리학회 논문집 Vol.7 No. 8S, pp.2641~2649, 2000.
[11] 김영덕, 신동명, 최용락 "SPS를 기반으로한 보안영역간 이동 에이전트 인증 협상 모델", 한국통신정보보호학회 충청지부, pp.241~254, 대전대학교, 2000.
[12] 서대희, 박희운, 이임영 "Active Network에 적용 가능한 에이전트 보안에 관한 연구", 한국정보보호학회 충청지부 종합학술발표회논문집, pp317~329, 2001.
[13] 서대희, 박희운, 이임영 "상호인증이 가능한 Mobile 에이전트 보안기법에 관한 연구", 한국멀티미디어학회 춘계학술발표논문집 제 4권 제 1호, pp477~480, 2001.
[14] 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신 보안", 도서출판 그린, 2000.
[15] 이임영 "전자상거래 보안입문", 생능출판사, 2001.8.
[16] Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996.

서 대 희

2001년 2월 동신대학교 전자공학과 졸업
2001년 3월~현재 순천향대학교 전산학과 석사과정

관심분야 : 암호이론, 정보이론, 컴퓨터 보안



이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학 전공 석사
1989년 3월 오사카대학 통신공학 전공 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안