Peer-to-Peer기반 실시간 보안 콘텐츠 공유 시스템 설계

*이광진, *이승하, *방세중, *김양우, **김기홍
*동국대학교 정보통신공학과, **넷시큐어테크놀러지
e-mail: *{ ln3407ss, lesh915, neovega, ywkim }@dongguk.edu,
**lizi@netsecuretech.com

Design of Real-time Security Contents Sharing System based on Peer-to-Peer

*KwangJin Lee, *SeungHa Lee, *SeChung Pang, *YangWoo Kim, **KiHong Kim
*Dept of Computer Information and communication Engineering, Dongguk University
**NetSecure Technology

요 약

기존 정보보호 콘텐츠에 대한 공유는 웹이나 메일 등을 통하여 수동적으로 배포되고, 운영관리자의 판단을 거친 후 보안등급에 맞게 제공되었다. 하지만 사이버 공간의 침해사고는 급속히 확산되어 끊임없이 보안 환경을 위협하는데 그에 대한 확산방지 대응은 즉각적이지 못한 문제점을 가지고 있다. 이러한 침해사고의 빠른 확산을 방지하기 위해서는 실시간 보안 콘텐츠 공유를 통해 각 시스템에서 콘텐츠의 추가 및 변경이 발생할 경우 자동으로 인지 또는 배포할 수 있는 정보보호 시스템을 개발할 필요가 있다. 따라서 본 논문에서는 보안등급에 따른 가상 정보공유 그룹을 구성하기 위해 P2P방식인 JXTA 플랫폼을 적용하였다. 또한 JXTA CMS의 확장을 통해 정보공유 시스템 간 연동할 수 있는 실시간 보안 콘텐츠 공유 시스템을 설계하였다. 이를 통하여 지리적으로 분산된 정보보호 콘텐츠를 실시간 자동인지와 보안등급에 맞는 실시간 공유 방식으로 배포하는 정보보호 시스템을 구현하고자 한다.

1. 서론

정보기술 산업의 발전으로 인하여 발생된 역기능 중 하나인 웜/바이러스 및 취약점을 이용한 사이버 공간의 침해사고가 기하급수적으로 증가하고 있다. 이러한 보안 위협 환경은 시스템의 가용성을 침해하며 정상적인 서비스를 방해하거나 개인정보를 악용하는 등 점점 확대되고 있는 실정이다. 이러한 역기능과 그에 대한 확산은 정보기술의 발전과 더불어 급속히 전 세계로 전파되어 초기 발생지역이 국외라 할지라도 거의 실시간 적으로 악영향을 미치고 있다. 하지만 현재의 정보보호 시스템은 특정지역에서 발생된 위협에 대한 대응방안이 전파되어 인지되기까지 어느 정도의 기간이 필요하다. 사이트마다 관리자들에 의하여 정보보호 콘텐츠가 각각 수동으로 수집/등록/관리 되고 있으며 특정 사이트에 의존적인 정보보호 콘텐츠인 트래픽 분석정보, 위협정도, 공격유형 등은 배포되지 않거나 단순 접근권한 제어 등으로 처리되고 있다. 그렇기 때문에 실시간 적인 상호간의 인지 및 공유가 필요함에도 불구하고 해당 콘텐츠가 별도로 관리되고 있는 문제점을 수반한다. 그러므로 동일 위협에 대한 정보의 신속한 공유를 통하여 해당 위협에 대한 인지 및 대응방안 수립이 필요하다. 그리고 위협에 좀 더 효과적으로 대응할 수 있는 보안 콘텐츠의 실시간 공유가 필요하다. 실시간성이 보장된 보안 메커니즘의 요구에 따라 정보보호 시스템을 보완하기 위해서는 P2P(Peer-to-Peer)[1]를 이용하여 각 시스템에서 추가 또는 변경되는 보안 콘텐츠를 정보보호 그룹 내에서 자동으로 인지하도록 할 수 있다.

P2P는 중앙 집중적 시스템이 아닌 네트워크상의 사용자끼리 직접적으로 서로를 탐색함으로써 유용한 서비스를 결정하고 응용할 수 있는 방식이다. 각각의 피어(Peer)들은 서버와 클라이언트 역할을 모두 수행할 수 있는 정보주체이기 때문에 해당 콘텐츠를 네트워크상에서 사용자간 직접연결을 통해 공유할 수 있다. 하지만 여러 다른 P2P간의 표준 프로토콜이 정립되지 않아 정보공유가 필요한 이기종 시스템 간의 상호호환성 문제가 제기되었다[3].

JXTA는 애플리케이션 간의 상호 호환성과 플랫폼의 독립성을 제공하기 위해 설계된 플랫폼이다. 이를 통하여 기존 P2P의 이기종 시스템 간의 호환성 문제와 시스템 장애를 해결할 수 있게 되었다[2].

한편 정보보호 콘텐츠의 공유를 위해서는 콘텐츠 각각에 대한 관리와 안정적 배포, 동기화를 수행하기 위한 관리가 필요하다. 모든 피어의 공유 콘텐츠를 관리하고 각 피어그룹 간의 공유를 위해서는 JXTA의 CMS(Contents Management System)를 이용하여 애플리케이션이 피어그룹 내의 콘텐츠를 찾고 공유할 수 있도록 할 수 있다.

따라서 본 논문에서는 지역적으로 분리된 정보보호 시스템에서 추가 및 변경되는 보안 콘텐츠의 공유가 필요한

정보보호 시스템에 대하여 P2P기술을 이용하여 정보공유 그룹을 구성하였다. 그리고 정보공유 그룹에 속한 시스템의 CMS를 이용하여 정보공유 시스템 간의 연동을 통해 정보보호 콘텐츠에 대한 배포 및 동기화를 수행하며, 콘텐츠의 동기화 시 보안등급 정책에 맞게 정보보호 시스템에 적용하는 실시간 정보공유 시스템을 설계하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 JXTA와 JXTA CMS를 살펴보고, 3장과 4장에서는 본 논문에서 제안한 실시간 보안 콘텐츠 공유 방법, P2P기반 실시간 보안 콘텐츠 공유 시스템을 제안하였다.

2. 관련연구

2.1 JXTA

JXTA는 SUN Microsystem사에서 오픈 소스 프로젝트의 일환으로 개발을 시작한 P2P플랫폼으로 분산 컴퓨팅을 위한 기반 서비스를 제공하는 동시에 공개(open) 네트워크 컴퓨팅 시스템이다[4][5].

JXTA 프로젝트의 목적은 다음과 같이 3가지 정도로 볼 수 있다.

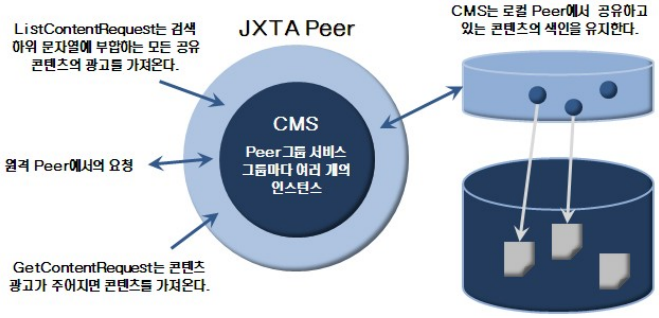
① Inter-operability : 서로 다른 이기종 P2P 서비스 피어들 간에 상호운영이 가능한 환경을 제공한다.

② Platform Independence : 개발 언어, 통신 프로토콜, 시스템 플랫폼에 독립적인 환경을 제공한다.

③ Ubiquity : 네트워크에 접속 가능한 모든 디바이스 상의 구현 가능한 환경을 제공한다. 이기종 언어로 개발된 P2P 서비스라 할지라도 JXTA의 핵심 소스를 적용하여 타 언어로 개발된 JXTA서비스와 연계가 가능하도록 설계한다.

2.2 JXTA CMS (Contents Management System)

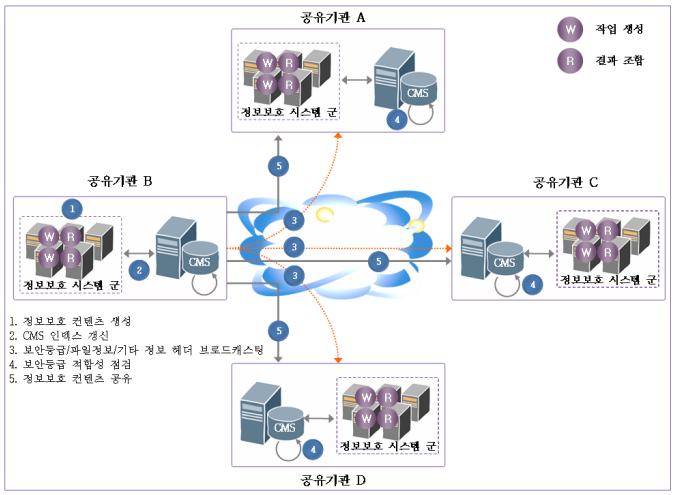
JXTA CMS는 모든 피어의 공유 콘텐츠를 관리하고 피어그룹 곳곳으로 콘텐츠를 공유하는데 쓰이는 JXTA 피어그룹 서비스이다. 그림 1과 같이 CMS는 피어가 공유한 콘텐츠의 로컬 색인을 관리한다. 이 색인은 파일명, 크기, 설명과 함께 콘텐츠를 대표하는 고유 ID를 담고 있다. 공유 파일은 적당한 곳에 두며, CMS는 이 파일을 유지하거나 저장하지 않는다.



(그림1) CMS 작동 원리

3. 실시간 보안 콘텐츠 공유 방법

본 논문에서 제안한 실시간 보안 콘텐츠 공유시스템 구조는 다음과 같다. 먼저 정보보호 콘텐츠의 공유가 필요한 정보보호 시스템들은 각각의 정보공유 그룹으로 설정된다. 이 때 정보공유 그룹은 시스템 내의 보안 정책에 따라 각각에 보안등급이 부여된다. 이 후 정보공유 그룹 간에 허용 된 보안등급에 맞게 시스템의 콘텐츠 중에서 갱신 된 데이터를 선별하도록 한다. 선별된 데이터들을 중심으로 정보보호 시스템이 관리하고 있는 콘텐츠들의 메타정보를 추출한 후, 추출된 메타정보는 CMS를 이용하여 정보공유 그룹 내에 브로드캐스팅 될 메타정보를 생성하도록 하는 정보보호 콘텐츠 공유를 위한 사전작업을 수행한다. 그림 2와 같이 정보보호 콘텐츠의 공유 프로세스는 데이터의 선별 → 선별된 데이터에 대한 메타정보 추출 → 문서 메타정보 생성 → 메타정보 브로드캐스팅 → 보안등급 점검 → 정보공유의 순서로 관리된다.

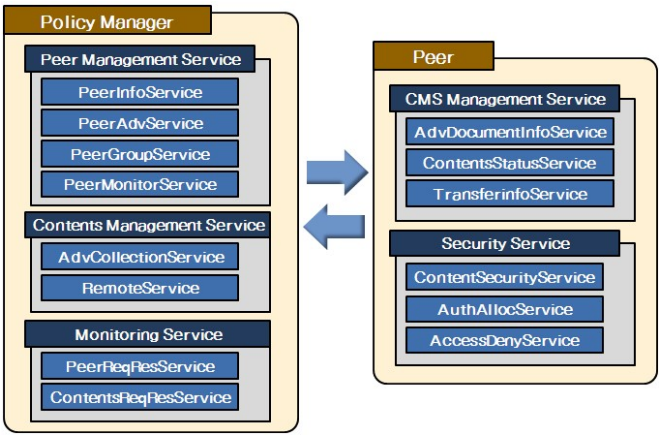


(그림2) 실시간 보안 콘텐츠 공유 방법

4. P2P기반 실시간 보안 콘텐츠 공유 시스템 설계

4.1. P2P기반 보안 콘텐츠 공유 시스템 구조

지역적으로 분리된 곳에 위치한 정보보호 시스템에서 추가 및 변경되는 정보보호 콘텐츠를 실시간으로 공유하기 위해서는 각각의 정보공유 시스템과 피어 간의 동기화가 이루어져야 한다.



(그림3) P2P기반 보안 콘텐츠 공유 시스템 구조

P2P기반 보안 콘텐츠 공유 시스템(Policy Manager) 구조는 그림 3과 같이 크게 3가지의 서비스로 구성되어 있다. 시스템의 기본적인 피어 정보를 관리하는 피어 관리 서비스(Peer Management Service)와 콘텐츠 관리를 위한 콘텐츠 관리 서비스(Contents Management Service), 피어 또는 콘텐츠의 응답이나 요청 등을 관리하는 모니터링 서비스(Monitoring Service)이다. 피어 또한 피어 상의 각각의 CMS를 관리하는 CMS 관리 서비스(CMS Management Service)와 피어와 콘텐츠의 보안등급을 체크하는 보안서비스(Security Service)로 각각 구성된다.

<표1> 보안 콘텐츠 공유 시스템 서비스

서비스	의미
PeerInfoService	피어의 기본적인 정보를 관리
PeerAdvService	피어정보 표시 Advertisement문서 관리
PeerGroupService	같은 작업을 처리 피어들을 그룹연결 관리
PeerMonitorService	현재 피어그룹 상의 피어상태 모니터링
AdvCollectionService	콘텐츠 Advertisement문서를 수집
RemoteService	콘텐츠의 로컬/원격 여부를 판단
PeerReqResService	피어의 응답이나 요청 등을 관리
ContentsReqResService	콘텐츠의 응답이나 요청 등을 관리
AdvDocumentInfoService	콘텐츠 Advertisement문서 정보 관리
ContentsStatusService	콘텐츠 상태를 관리
TransferInfoService	콘텐츠 전송 정보 관리
ContentSecurityService	콘텐츠 문서 보안 관리
AuthAllocService	권한 할당 및 부여
AccessDenyService	Access / Deny 관리

이처럼 보안 콘텐츠 공유 시스템들은 각각의 서비스를 지원하며 각각의 시스템 간, 피어 간 연동을 통하여 정보보호 콘텐츠에 대한 배포 및 동기화를 수행하게 된다.

정보보호 콘텐츠의 공유가 필요한 정보보호 시스템들은 각각의 정보공유 그룹으로 설정되고, 공유 그룹 내에 포함된 시스템들의 콘텐츠를 CMS를 이용하여 메타정보 형태로 관리하게 된다. 콘텐츠의 추가, 변경 등이 발생할 경우는 실시간으로 CMS의 메타정보가 갱신되고, 갱신이 완료된 메타정보는 정보공유 그룹의 시스템들에게 브로드캐스팅 되어 콘텐츠의 변경 또는 추가가 발생되었음을 알린다. 브로드캐스팅 된 메타정보를 전송받은 정보공유 그룹의 시스템들은 각 시스템에 설정되어 있는 보안등급 정책과 메타정보를 비교한 후 보안등급에 준하여 추가하거나 변경된 정보보호 콘텐츠를 공유하게 된다.

4.2. P2P기반 보안 콘텐츠 공유 시스템 설계

본 논문에서는 JXTA상에서 계층화 된 보안등급으로 구성된 공유 그룹 간의 접근과 정보보호 시스템에서 추가 및 변경되는 정보보호 콘텐츠를 실시간으로 공유하기 위하여 콘텐츠 관리 시스템인 CMS를 확장하였다.

그림 4는 본 논문에서 제시한 JXTA CMS상에서 콘텐츠 공유를 보안정책에 따라 자동화하기 위한 콘텐츠 advertisement문서의 한 예이다.

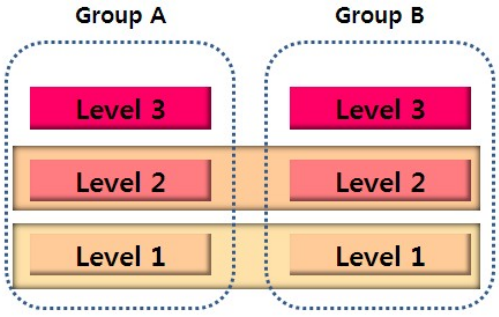
```
<?xml version="1.0">
<!doctype jxta : ExtendedcontentAdvertisement>
<jxta:ExtendedcontentAdvertisement>
    <name>index.html</name>
    <cid>uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6</cid>
    <integrity>md5:1a8baf7ab82c8fee8fe2a2d9e7ecb7a83</integrity>
    <type>text/html</type>
    <length>23983</length>
    <peergroup>
        <groupid_area>seoul</groupid_area>
        <groupid>urn:jxta:uuid-42D52A1F2A.....DJ32D</groupid>
    </peergroup>
    <peer>
        <peerid>urn:jxta:uuid-596162618.....FFC3DSC2</peerid>
        <peerlevel>2</peerlevel>
    </peer>
    <permission>rw</permission>
    <description>Web site index</description>
</jxta:ExtendedcontentAdvertisement>
```

(그림4) 확장된 JXTA CMS 콘텐츠 advertisement

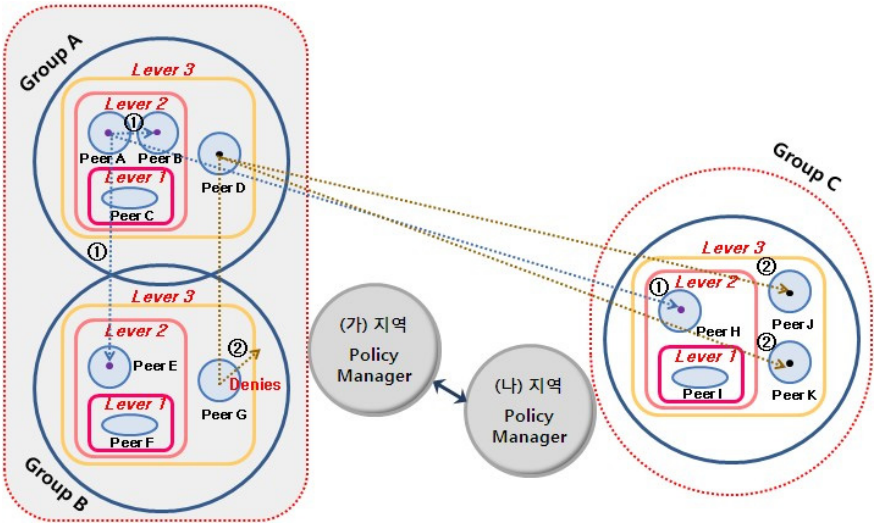
CMS의 확장과 이동성을 확보하기 위하여 콘텐츠 각각의 ID를 뜻하는 cid 필드를 UUID(Universally Unique IDentifier)로 수정하였으며, 콘텐츠 공유 시 무결성을 보장하기 위해 고유한 128비트 MD5 체크섬을 포함한 무결성(integrity) 필드를 추가하였다. 또한 정보공유 그룹인 피어그룹(peergroup)과 피어(peer), 권한(permission)필드를 추가하였다. 피어그룹 필드는 위치, ID 등 피어그룹에 대한 정보를 담고 있으며, 피어필드에서는 정보공유 시스템 상의 보안정책에 따른 피어 접근레벨과 ID를 담고 있다. 권한필드는 피어 접근레벨에 따른 보안등급 내의 갱신된 콘텐츠 공유 여부를 읽기(r), 쓰기(w)로 나누어 정의하였다.

이러한 CMS의 콘텐츠 메타정보는 각각의 정보공유 시스템이 관리한다. 원격간의 콘텐츠 정보공유는 정보공유 시스템간의 연동으로 피어정보 교류를 통해 이루어진다.

한편 각 정보공유 그룹은 보안등급에 따라 가상의 정보공유 그룹을 구축하게 된다. 가상의 정보 공유 그룹을 통해 원격지의 정보공유 그룹과 배포 및 동기화를 수행하는데 그림 5는 보안등급에 따른 가상의 정보공유 그룹을 구축한 예이다.



(그림5) 보안등급에 따른 가상 그룹 구축



(그림6) 실시간 정보보호 콘텐츠 공유시스템 동작원리

보안등급 1과 2는 정보 공유가 가능하도록 설정된 하위 접근레벨로 설정되었으며, 지리적으로 분리된 정보공유 그룹 A와 B를 가상의 정보공유 그룹으로 묶어 피어 및 콘텐츠의 정보를 상호 공유하게 된다. 또한 보안등급 3은 최고 접근레벨로 설정되어 가상의 정보공유 그룹을 구축하지 않고 상호 독립적으로 관리/운영된다.

4.3 실시간 보안 콘텐츠 공유 시스템 동작원리

본 논문에서 제안한 실시간 보안 콘텐츠 공유시스템 동작원리는 다음과 같다. 그림 6과 같이 정보공유 시스템들은 각각의 정보공유 그룹으로 구성되어지며, 피어는 각 접근레벨에 따라 최고 접근레벨인 Level 3부터 1까지 계층화 되어 구분 관리된다. 최고 접근레벨인 Level 3은 해당 정보공유 그룹만의 기밀문서이기 때문에 상호 공유가 되지 않는 것을 원칙으로 할 수 있다.

(가)지역은 정보공유 그룹 A와 B로 구성되며, 지리적으로 분리된 (나)지역의 정보공유 그룹 C는 (가)지역의 정보공유 그룹 A와 같은 성격을 가진 그룹이라 가정한다.

- 시나리오 ① : (가)지역의 정보공유 그룹 A의 피어 A에 해당 콘텐츠가 갱신되었다. 실시간으로 CMS의 메타정보가 갱신되고, 갱신이 완료된 메타정보는 각 정보공유 시스템에게 브로드캐스팅 되어 콘텐츠의 변경 또는 추가가 발생되었음을 알린다. 각 시스템에 설정되어 있는 보안등급 정책과 메타정보를 비교한 후 보안등급에 준하는 가상의 정보공유 그룹을 구축하여 해당 콘텐츠를 배포하게 된다.
- 시나리오 ② : (가)지역의 정보공유 그룹 A의 피어 D의 콘텐츠가 갱신되었다. 시나리오 ①과 같이 각 정보공유 시스템에게 CMS 메타정보가 브로드캐스팅된다. 하지만 갱신된 콘텐츠는 상호 독립적으로 관리/운영되는 최고 접근레벨 3에서 갱신된 기밀문서이기 때문에 정보공유 그룹 B에는 공유되지 않지만 같은 성격을 가진 정보공유 그룹 C의 피어들에게는 해당 콘텐츠가 배포된다.

5. 결론 및 향후연구

기존의 정보보호 콘텐츠에 대한 공유방식은 웹이나 메일 등을 통하여 수동적으로 배포되어 운영관리자의 판단을 거친 후 보안등급에 맞게 제공되어왔다. 그러나 실시간 정보공유의 경우 정보공유 그룹에 포함된 각 시스템에서 콘텐츠의 추가 또는 변경이 발생할 경우 자동으로 변경내용을 인식하여 사전에 정의된 보안등급 정책에 준하여 정보보호 콘텐츠를 제공할 수 있다. 그러므로 본 논문에서는 정보보호 콘텐츠의 공유가 필요한 정보보호 시스템에 대하여 P2P기술을 이용하여 정보공유 그룹을 구성하고, 정보공유 그룹에 속한 각 시스템의 CMS를 이용하여 각각의 정보보호 시스템을 보안등급 정책에 맞게 가상의 정보공유 그룹으로 구축하였다. 이에 상호 연동을 통해 콘텐츠의 동기화가 이루어 질 경우 정보보호 시스템에 적용하는 실시간 정보공유 시스템을 설계하였다.

향후 연구 방향으로는 SSL프로토콜을 적용하여 인증과 암호화를 통해 데이터의 안정성을 높이도록 하고, 허가되지 않은 접근이나 변경으로부터 자원을 보호하기 위해 자원에 대한 모든 사용자 및 프로세스의 접근을 중재하는 참조 모니터를 통해 시스템의 보안성을 높일 예정이다.

참고문헌

[1] Andy Oram, "PEER-to-PEER", O'Relly, 2001.

[2] Li Gong, "JXTA : a network programming environment", IEEE Internet Computing, Volume : 5 Issue : 3, May-June 2001 Page(s) : 88-95

[3] 이구연, 이용, 김화종, 정충교, 이동은, "보안성과 유연성을 갖춘 Peer-to-Peer 데이터 공유 기법의 설계 및 구현", 정보보호학회논문지, 제15권, 제4호, 2005.08.

[4] Juan Carlos Soto, "Project : Content Management System", www.jxta.org

[5] JXTA v2.0 Protocols Specification, Sun Microsystems Inc.,http://spec.jxta.org/nonav/v1.0/docbook/JXTAProtocols.pdf