2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

Web security 기능을 위한 Anonymiser 구축 방안에 대한 연구

최영림*, 장혁수*
*명지대학교 정보통신공학과
e-mail : quarry@mju.ac.kr

An Anonymiser Development for Web Security

Young-Lim Choi*, Hyuk-Soo, Jang*
*Dept. of Information Communication Engineering, Myong-Ji University

요 약

Web Security 를 위한 방법으로서 anonymity 에 대한 개념에 대해서 살펴보고, 멀티캐스트 그룹환경에서 web 보안을 위해 익명 서비스를 제공하는 anonymiser 를 사용하여 보다 효율적인 web 보안과 익명 서비스를 적용할 수 있는 방안을 제안 한다.

1. 서론

인터넷 사용자 수의 급격한 증가로 인해 인터넷은 다양한 문제들을 갖고 있다. 인터넷 사용에 있어서 여러 가지 보안상의 문제점과 네트워크 자원을 공유하기 때문에 생기는 QoS 의 불만족과 트래픽의 문제는 심각하게 받아들이고 있다. 또한 네트워크를 통한 자료의 공유 또한 보편화되고 활성화됨에 따라 네트워크 확장의 문제와 그 비용의 문제도 크게 대두되고 있다. 그 중에서 보안의 심각성은 ISP 와 같은 서비스를 제공하는 업체뿐만 아니라 일반 사용자들도 그 문제가 심각한 현상으로 받아들여지고 있다. 현 PC 시대의 보안 위협은 엄연한 현실이다. 예를 들어 전자메일은 바이러스가 유포될 수 있는 가장 손쉬운 방법중의 하나이다. 아웃룩이나 윈도우 스트립팅 호스트와 같은 전자메일 프로그램을 운영한다면, 러브 버그(Love Bug)와 같은 바이러스에 감염되기 쉽다. 주소록에 있는 정보를 보고 메일을 발송하기 때문에 이러한 바이러스는 베이스 네트워크에 전이 시킬 수도 있다. 이러한 바이러스는 물론 크래커의 침입으로 인해 사용자 및 관리자들은 항상 보안의 문제를 항상 염려해 두고 있어야 한다. 자치 잘못하면 모든 데이터의 손실 및 Server Down 등의 현상이 발생하기 때문이다. 게다가 현재 관심을 갖고 있는 분산 응용 분야인 멀티미디어 회의, 컴퓨터를 이용한 공동 작업, 의료분야에서의 원격 진단 및 자문 등의 활성화와 같은 다수가 참여하는 멀티캐스트에서도 그 보안의 심각성과 해결방안은 큰 관심의 대상이 되고 있다.

정보통신망에 제공되는 기본적인 정보보호 서비스로 인증, 접근통제, 비밀보장, 무결성, 부인방지 등이 있고 이를 위한 보호 메커니즘으로 암호화, 인증, 데이터 무결성, 트래픽 패딩, 경로제어 등이 있는데 이러한 기술들을 복합적으로 적용하여 보안의 문제에 대처하고 있고, 연구 개발 중에 있다.[8]

이에 본 연구는 정보보호 서비스를 제공하는 방법으로 멀티캐스트 환경에서 anonymity 에 대해서 살펴보고, Web security 기능을 위한 anonymiser 구축 방안에 대하여 살펴보고자 한다. 먼저 2 절에서는 anonymity 에 대해서 살펴보고, 3 절에서는 anonymiser

를 이용한 송신자와 수신자의 anonymity 와 anonymiser 의 구축방안에 관해서 살펴보고, 4 절에서 결론을 맺었다.

2. Anonymity

지금까지 멀티캐스트의 환경에서는 익명 서비스에 관해 거의 고려하지 않고 있었다. 하지만 traditional point-to-point communication 에서는 예전부터 익명성을 제공하고 있었으며, 인터넷 특히 WorldWideWeb 에서 많은 작업들이 익명성 서비스를 이용하고 있었다.[1]

인터넷 사용자들이 다양한 정보 접근과 여러 가지 서비스를 제공 받음으로써 노출될 수 있는 정보(client 의 IP address, 최근 접속한 web server address, e-mail address 등) 보호를 위해 이 anonymisation service(익명성 서비스)를 제공하고자 하는 것이다. 특히 전자상거래를 통한 거래 중에 개인의 이름과 주소, 은행 계좌 정보 및 신용카드 번호 등, 개인의 중요한 정보가 유출되거나 해킹 당할 수 있기 때문에 이러한 익명성 서비스를 제공함으로써 사용자들을 보호하고자 하는 것이다.

David Chaum 은 'Mix'로 불리는 anonymity 의 일반적인 개념에 대해서 표현했다. Mix 는 Proxy 와 같은 중간 스테이션 단계로서 패킷을 대신 수신하고 송신하는 기능을 한다.[2]

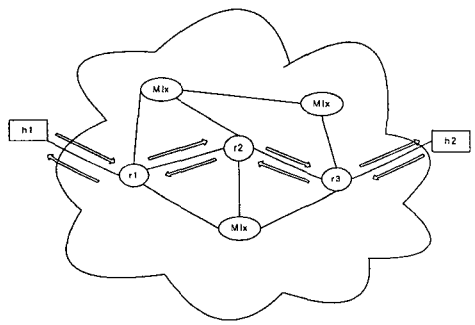

그림 1. Chaum's Mix Concept

그림 1 에서 세 Mix(r1, r2, r3)가 사용되고 있다. 캡슐화와 암호화 된 content 는 캡슐화를 풀거나 복호화 없이 그대로 전송된다. 각 Mix 들은 단지 all next hop neighbors 의 identity 만을 알고 있으면 되기 때문에 각 Mix 들의 상호 협동을 통해 host h1 과 h2 사이의 통신을 수행하는 것이다. 이 기본 아이디어 형태는 web anonymity 를 위한 여러 가지로 가능한 새로운 서비스의 기본이 되고 있다. *Onion-Routing*[3], *Anonymizer*, *janus/Rewebber*[4] 등은 web browser 와 proxy service 형태를 사용하여 이용가능 하다. [1] 이들은 web server 에 접속해서 client 의 요구된 정보를 가져오는 것이다. 그러므로 각 서버들은 demanding host 로서 anonymiser 만 구별하면 되기 때문에 client 를 알 필요가 없는 것이다. 이와는 다른 개념으로 Crowds[5]가 있다. 이것은 host 의 큰 그룹을 형성하여 described proxy service 를 제공하는 것이다.

다음 절에서는 익명성을 이용한 송신자와 수신자의 서비스에 대해서 살펴보고자 한다.

3. 익명성 서비스

3.1 송신자 서비스

먼저 여기서 전제로 두고 있는 멀티캐스트 서비스라 함은 사전에 미리 보안 기능을 하고자 하는 임의의 그룹에서 암호화와 복호화에 관한 규약이 선행되어야 하며 여기서 제공한다는 멀티캐스트는 일대일 통신이 아닌 여러 호스트들에게 보내는 똑같은 정보를 말하는 것이다. 다시 말하자면, 임의의 한 회사에서 여러 지역에 퍼져 있는 자사 직원들에게 회사의 비밀 정보나 대외비 등의 정보 등을 보내고자 할 때 자사의 허가 받은 자만이 암호화된 정보를 찾아 볼 수 있게 하는 것이다. 이에 대한 암호/복호 기능을 각 호스트에서 하는 것이 아니라 익명 서비스를 제공하는 anonymiser 를 설치하거나 기존의 웹 캐쉬 서버에서 모듈을 추가하여 멀티캐스트 서비스를 제공하는 것이다. 여기서 웹 캐쉬 서버를 두는 이유는 목적지의 캐쉬의 적중률을 높여 원거리에 있는 원래 웹 서버까지 가야 할 확률을 줄여서 네트워크의 트래픽을 줄일 수 있기 때문이다.[6][7] 여기에 proxy 서버와 같은 기능으로서 anonymisation service 를 제공함으로써 보안의 기능을 추가한 것이다. 그림 2 에서 보면 anonymiser A 가 송신자의 익명성 서비스를 제공하고 있다.

물론 한 proxy 서버를 사용함으로써 그에 대한 경로 수 증가와 트래픽의 congestion 문제가 발생할 수 있다. 하지만 이에 대한 해결방안으로 cache location 문제[7]를 적용하여, 적정 캐쉬의 수를 계산하여 위치시킴으로써 문제를 해결해 보려는 것이다.

이렇게 암호화된 정보는 어느 일정 노드까지 유니캐스트 방식으로 전송 된 후 멀티캐스트 방식으로 전송 될 것이다. anonymisation service 를 제공하는 서버나 모듈은 암호화를 원하는 정보만 암호화 하기 때문에 그 이외의 데이터는 기존의 서버로 직접 보내면 되기 때문에 추가적인 부하나 트래픽이 적으리라 판단된다. 하지만 여기서 발생할 수 있는 문제는 어느 침입자가 그 중간노드를 거치지 않은 다른 길로 들어 온다면 그 침입에 대응하지 못 하는 것이다. 왜냐하면 그 중간노드까지는 암호화 되지 않은 메시지를 보내고 있기 때문이다.

여기에서 이 문제를 해결하려면 원 소스를 보내는 최초 그룹 내에 proxy 서버를 두어 메시지를 암호화 하고 대신 중간 노드까지의 트리를 계산, 경로를 추정하여 정보를 갖고 보낸다면 위에서 제기한 문제를 해결할 수 있다. 다만 여기서 생기는 추가적인 네트워크의 경로를 캐쉬 위치 알고리즘을 적용하여 그 해당 위치를 찾는 것이다.

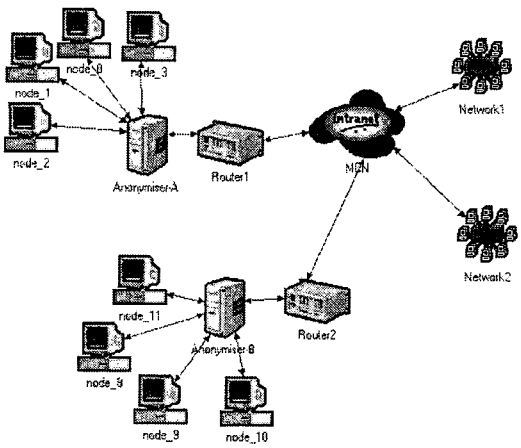

그림 2. Anonymiser

3.2 수신자 서비스

송신자가 보낸 암호화 된 정보는 어는 일정 노드까지 전송 된다. 여기서 주안을 두는 것은 송신자가 보낸 정보는 end-user 인 호스트까지 보내는 것이 아니라 라우터와 같은 일정 노드까지 전송한다는 것이다. 그림 2 에서 살펴보면, anonymiser B 까지 전송하는 것이다.

익명성 서비스를 받고자 하는 각 Host 는 여기 anonymiser 에 접속하여 자신이 원하는 서비스를 받아가는 것이다. 수신자 또한 자신이 누구라는 것을 밝히지 않고 서로 사전에 약속된 정보로 그 서비스를 받아가는 것이다. 만일 anonymiser B 에 속한 그룹이 여러 개가 존재한다면, 그 소규모 그룹까지 다시 전송되어진다. 즉, 멀티캐스트 data 를 이 노드까지 유니캐스트로 보내면 이 라우터에 속해 있는 각 호스트(사전에 허락받은 사용자)는 이 노드에서 암호된 data 를 풀지 않고 자신이 속한 소규모 그룹까지 가져가는 것이다.

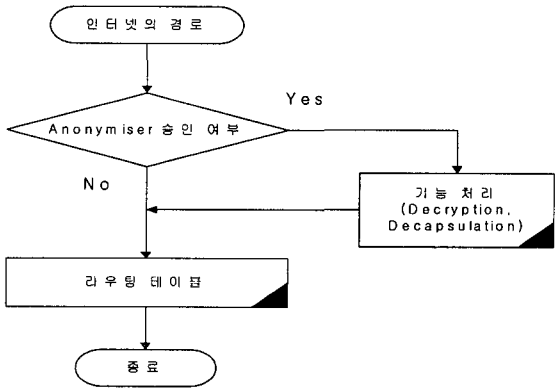

그림 3. Anonymiser 처리 과정

그런 다음에 자신이 속한 말단의 라우터에 속한 서버에서 복호화 하여 암호를 푼 다음, 정보를 가져가는 것이다. 복호화의 간단한 알고리즘은 그림 3 에서 보듯이 anonymiser 사용여부에 따라, 그 기능이 있는 것은 해당 모듈로 보내어 처리한 다음에 다시 보내면 되는 것이다. anonymiser 를 사용하지 않은 메시지는 그냥 통과시키면 되기 때문에 많은 트래픽을 요구하지 않고 그 기능을 처리 할 수 있다고 본다.

여기에서 생각해 볼 문제는 만일 소규모 기관의 호스트 수가 많다면 그 정보를 가져오는 노드까지의 거리와 실제 암호화 데이터를 가져오는 사용자의 참가율을 적용하여 여러 대의 캐쉬 서버를 적용한다는 것이다. 그러면 추가된 네트워트 경로에 대한 트래픽을 감소할 수 있다. 여기서 말하는 감소란 단순히 한 서비스(한 번의 통신)만 놓고 본다면 그 이득을 가져올 수 없겠지만 일정 수준 이상의 호스트 수와 그 암호 데이터를 송,수신하는 그룹 수가 크다면 충분히 그 이득을 볼 수 있다.

4. 결론

인터넷의 확장에 따라 네트워크를 통한 외부 침입 가능성은 더욱 커졌고, 이로 인하여 발생할 수 있는 문제는 걷잡을 수 없을 정도이다. 이에 대한 대체 방안으로서, 본 연구는 익명성 서비스에 대해서 살펴보았다. 멀티캐스트 환경에서 송신자와 서비스를 보호하기 위해, 익명성을 제공함으로서 송신자와 수신자를 보호하고자 하는 것이다. 그리고 익명성을 제공하는 anonymiser 의 구축 방안으로서 기존의 web-server 나 라우터에서 그 처리를 함으로써 부가적인 부하를 줄이려고 하였다. 또한 기존의 web cache server 가 anonymiser 기능을 수행으로서 추가적인 트래픽에 능동적으로 대체할 수 있는 방안을 제시하였다. 앞으로 멀티캐스트 환경에서 anonymiser 를 위한 다양한 서비스를 제공할 수 있는 멀티캐스트 그룹에서의 구축 방안과 트래픽 제어에 관해 연구 할 예정이다.

참고문헌

[1] Christian Grosch, " Anonymisation Services for IP *Multicast*", IEEE, 2000

[2] David Chaum, "Untraceable electronic mail, returnaddress, and digital pseudonyms", Communications of the ACM, 1981

[3] David Goldschlag, Michael Reed, and Paul Syverson, "Onion routing for anonymous and private internet connection", Communications of the ACM, 1999

[4] Andress Rieke and Thomas Demuth, "Janus: Server-anonymitat im world wide web", In Horster, Patrick: Sichereisinfrastrukturen, 1999

[5] Michael Reiter and Aviel Rubin, "Crowds: Anonymity for web transactions", DIMACS Technical Report, 1997

[6]민경훈, 장혁수, "네트워크 경로에 기초한 웹 캐슁 알고리즘", 정보처리학회, 2000.7

[7]P. Krishnan, Danny Raz, "The Cache Location Problem", IEEE, 2000. 10.

[8]권현조. 김학범, 홍기용, "네트워크 보안 기술 동향", 한국정보보호학회, 1998. 6.