

# 유즈넷 서비스 인증에 관한 연구

이달원<sup>\*</sup> · 조인준<sup>\*</sup> · 황일선<sup>\*\*</sup>

<sup>\*</sup>배재대학교 · <sup>\*\*</sup>한국과학기술정보연구원

## On the study of Usenet service authentication

Dal-won Lee<sup>\*</sup> · In-june Jo<sup>\*</sup> · Il-sun Hwang<sup>\*\*</sup>

<sup>\*</sup>Paichai University · <sup>\*\*</sup>Korea Institute of Science and Technology Information

E-mail : munhee@mail.pcu.ac.kr · injune@mail.pcu.ac.kr · his@kreonet2.net

### 요 약

인터넷 서비스 중 다른 곳으로부터 구할 수 없는 전문 지식을 취득할 수 있는 중요한 정보 획득 수단으로서 최신 전문가 그룹과 보조를 맞출 수 있는 유일한 방법은 뉴스 서비스이다. 이러한 목적 때문에 많은 국가에서 뉴스 서비스를 제공하고 있으며 국내에서는 3대 주요 뉴스 서버가 해외의 뉴스 서버들과 연동하여 대량의 뉴스 기사를 입수하여 국내에 배포하고 있으며 기업, 연구소, 대학교 등 많은 기관에서 국내외의 뉴스 기사를 서비스하고 있는 현실이다[1]. 그러나 그 중요성에 비해 뉴스 서비스의 사용자수는 감소하고 있어 현재는 비영리 목적으로 국가 차원에서의 지원과 운영이 요구되고 있으며 기술적 차원의 지원도 미비하여, 특히 보안 기능의 적용은 부분적으로 이루어지고 있어 매우 취약한 상태이며, 서비스 제공자가 필요로 하는 다양한 요구사항을 만족시키지 못하고 있는 상태이다.

본 논문에서는 기존 뉴스 서비스에서 제공해야 될 다양한 보안기능 중 인증에 대한 문제점을 기술하고 뉴스 서비스에서의 안전한 인증방법을 제시하고자 한다.

### ABSTRACT

News service provide professional knowledge which can't be gained from any other internet service and the only way to keep pace with professional group. To get this advantage, many country provide news service and three major korean news server connected with foreign news server provide many articles to korea. A lot of institutes - company, research centers and universities - forward articles to home and abroad. In spite of this important effect, The user of news service and technical supports grow smaller. And now it is necessary for a nation to support and operate by non-profitable business. Especially, partially adapted security weaken entire system safety and can't satisfy service provider of various necessary condition.

In this paper, we will mention troubles in authentication and suggest safety authentication method which must be supported by established news service.

### 키워드

Usenet, Newsgroup, Authentication

### 1. 서 론

뉴스그룹(Newsgroup)은 주요 인터넷 사이트에 특정주제에 관해 짧은 글들을 올려서 서로 토론할 수 있도록 만들어진 인터넷 서비스로서, 전세계적인 뉴스 토론그룹인 유즈넷(Usenet)을 통하여 재배포 된다.

유즈넷은 전세계 사람들이 정보를 공유할 수 있도록 해주는 규모가 크고 비집중화된 컴퓨터 시스템의 집합이다. 이 정보는 각 뉴스그룹이 고

유의 주제를 가지고 있는 토론그룹의 형태로 이루어져 있다. 학술과 기술에 관련된 전문적인 내용에서부터 취미와 오락에 관련된 내용까지 전세계적으로 약 20,000여개 이상의 주제가 설정되어 있으므로 관련 분야에 대한 최신 내용 및 심도 깊은 내용을 구할 수 있다. 또한 특정 주제에 대한 질문과 응답이 가능하므로 정보습득의 좋은 대안은 유즈넷의 사용이 될 수 있다. 이러한 유즈

넷은 Internet News, Netnews, Usenet News, Internet Newsgroup, 토론그룹 등 다양한 이름으로 불리고 있다.

유즈넷을 사용하려면 기사를 수신할 수 있는, 그리고 자신의 의견을 적어서 송신할 수 있는 뉴스서버가 필요하다. 개인적 용도 이외에도 뉴스서버의 주된 임무는 많은 양의 기사를 신속히 입수하여 사용자들에게 제공하는 것이며, 이를 구축하고 관리 및 운영하는 것은 쉬운 일은 아니지만 해당 기관에 관련 분야에 대한 최신 정보를 공급함으로써 그 분야의 전문성을 유지하려면 뉴스서버의 운영은 필수라고 할 수 있다.

뉴스기사의 처리관점에서 살펴보면 뉴스서버의 국내 3대 주요 기간망 서버에 해당하는 연구전산망(news.kreonet.re.kr), 한국통신(usenet.kornet.nm.kr), 데이콤(news.dacom.co.kr)에서 미국과 유럽 그리고 일본의 기간망 서버들로부터 직접 뉴스를 입수하고, 일단 입수한 뉴스를 신속히 다른 뉴스서버들에게 전달함과 동시에 다른 서버가 입수한 뉴스를 수신하여 고가의 해외라인을 효율적으로 사용하고 있는 상태이다[2].

사용자 이용관점에서 살펴보면 지속적인 인기를 유지하고는 있지만 웹 서비스 보다 사용자수가 많지 않고, 유즈넷 서비스의 본래 목적에서 벗어나 바이너리 파일(이미지, 동화상, 프로그램 등)의 서비스 요구가 증가하고 있으며, 서비스에 대한 개선 요구사항이 적기 때문에 사용자와 제공자 모두 유즈넷 서비스를 부가적인 서비스로 인식하고 있을 뿐이어서 보안 서비스 측면에서는 기본적으로 회원인증 서비스만을 제공하고 있는 상태이다.

본 논문에서는 웹 서비스에서는 얻을 수 없는 장점인 특정 주제에 대한 심도 깊은 최신의 정보를 얻을 수 있는 유즈넷 서비스를 사용할때 적용되고 있는 보안 서비스 중 인증에 대한 문제점을 살펴보고 이에 대한 대안을 제시하고자 한다.

## II. 본 론

### 1. 현황

뉴스서버로서 거의 모든 시스템들이 이용될 수 있지만 보편적으로 유닉스 계열 및 리눅스 시스템이 적당한 것으로 알려져 있으며, 주로 사용되는 서버 프로그램에는 INN(InterNetNews), diablo, Cyclone 등이 있다.

국내에서 현재 사용가능한 유즈넷 서비스의 형태를 분류해보면 비영리망을 주축으로 하는 무료 뉴스서버(읽기는 누구나 가능하나 쓰기는 회원전용)와 ISP(Internet Service Provider) 업체를 주축으로 하는 회원전용 뉴스서버(읽기와 쓰기 모두 회원전용) 두가지로 나뉘어지며, 적용되고 있는 인증(Authentication) 방법에는 ID/PW 인증과 IP 인증방법이 있다.

표 2. 국내 주요 유즈넷 서비스 인증방법[3]

제 공	서비스 형태	인증방법
news.kreonet.re.kr (Kreonet)	무료	ID/PW
news.nuri.net (아이네트)	"	"
news.hang.net (한큐넷)	"	IP
news.kornet.net (한국통신)	회원	"
news.hanaset.net (하나포스)	"	"
news.chollian.net (천리안)	"	"
news.unitel.net (유니텔)	"	"
news.netsgo.net (넷즈고)	"	"
news.channeli.net (채널아이)	"	"
news.elim.net (엘림네트)	"	"
newsgroup.korea.com (두루넷)	"	"
news.dreamline.co.kr (드림라인)	"	"
news.hitel.net (하이텔)	"	ID/PW
news.shinbiro.com (신비로)	"	"

### 2. 문제점

인증(Authentication)이란 어떤 사람이나 사물이 실제로 신고된 바로 그 사람(또는 사물)인지를 판단하는 과정이며 개별 또는 인터넷을 포함한 공공 네트워크에서의 인증은 대개 로그인시 암호의 사용을 통해 이루어진다.

본 논문에서 다루고 있는 유즈넷 서비스에서 제공되고 있는 인증방법에는 ID/PW 인증과 IP 인증방법이 사용되고 있는데 이 경우 다음과 같은 문제점들이 발생할 수 있다.

#### 2.1 ID/PW 누출

ID/PW를 이용한 인증방법에서의 일반적인 문제점은 다음과 같다.

- ① 사용자 부주의로 인한 누출
- ② 운영자의 보안 부주의에 의한 누출
- ③ 해커의 패스워드 추측으로 인한 획득 등

#### 2.2 Packet Sniffing

데이터 링크 계층에서 대표적으로 사용되는 Ethernet 프로토콜은 MAC(Medium Access Control)주소를 이용하여 전체 세그먼트에 패킷을 브로드캐스팅하는 통신 방법을 이용한다. 만일 목적지의 MAC주소와 동일한 주소를 가진 호스트라면 패킷을 읽어들이 처리가 가능하게 된다. 이러한 보안 취약점을 이용하여 패킷중 특정 포트만 필터링하여 도청하는 Packet Sniffer 프로그램을 실행하여 정당한 사용자의 ID/PW를 획득하게 된다[4].

### 2.3 IP Spoofing

TCP/IP 프로그램은 매우 유동적이며 사용하기 편리하지만 보안 측면에서는 다음과 같은 취약점을 가지고 있다.

#### 1) 호스트 인증 문제

IP는 호스트의 인증을 IP의 출발지 주소만으로 수행하므로 출발지 호스트의 IP 주소만을 속일 수 있다면 부당한 사용자도 정당한 인증과정을 통하여 사용이 가능하게 된다.

#### 2) 순서번호(sequence number) 문제

일부 TCP/IP 프로그램들에서는 순서번호의 단순한 생성때문에 Packet Sniffer를 이용하지 않더라도 순서번호의 추측만으로 정당한 사용자처럼 위장이 가능하며, 더욱이 패킷의 내용을 볼 수 있다면 순서번호를 알고 있기 때문에 지속적인 연결까지 가능하게 되어 Connection Hijacking을 이용할때 흔히 사용된다[5].

### 2.4 Hijacking

IP Spoofing을 이용하여 Connection Hijacking을 하는 적극적 공격(Active Attack)과 동일한 의미로서 단순히 Packet Sniffer를 이용한 소극적 공격(Passive Attack)과 구별하기 위해 표현하기도 한다. 즉 Packet Sniffing과 IP Spoofing 기술을 복합적으로 사용하여 정당한 사용자처럼 위장하거나 일회용 패스워드나 Kerberos와 같은 티켓 기반 인증 시스템에 의해 제공되는 보안 방법을 우회할 때 사용되는 방법을 말한다[6].

### 2.5 기타

유즈넷 서비스에서 제공되어야 할 보안 서비스로서 사용자에 대한 인증 뿐만이 아니라 사용자가 포스팅(posting)하는 글의 불법변조, 뉴스서버 사이의 기사제공시 서버사이의 인증, 뉴스서버를 해킹경로로 사용되는 문제점들에 대해서도 연구가 되어야 한다.

## 3. 문제점 해결방안

### 3.1 ID/PW 관리

ID/PW에 대한 일반적인 보안 문제점의 해결방안은 사용자와 운영자 그리고 해커에 대비하여 다음과 같은 사항들을 점검해야 한다.

- ① 사용자의 주의깊은 사용 및 보관
- ② 운영자의 보안에 대한 지식습득 및 안전한 운영(패치, 보안도구 적용 등)
- ③ 안전한 패스워드 생성, 패스워드 암호화 후 저장, 패스워드 정보에 대한 접근통제 적용[7] 등

### 3.2 PAM(Pluggable Authentication Modules)적용

ID/PW 인증을 이용하여 접근한 사용자가 올바른 사용자인가를 판단하는 기능을 PAM에서 제공하며 다음과 같은 보안적 특징[8]을 포함하고 있다.

- ① 패스워드 암호화에 비(非) DES(Data Encryption Standard) 방법 적용
- ② 사용자에게 제공되는 시스템 자원량에 제한을 두어 DoS(Denial of Service) 예방
- ③ 패스워드를 쉐도우(shadow) 패스워드로 감춤 제공
- ④ 사용자 사용제한(특정 시간, 장소)기능 제공

### 3.3 SSH(Secure Shell) 이용

SSH는 네트워크의 다른 컴퓨터에 로그인 할 수 있으며 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 프로그램이며 두 호스트간의 통신 암호화와 사용자 인증을 RSA 공개키 암호방식을 사용한다. SSH의 암호화된 패킷 전송을 이용함으로써 IP Spoofing을 방지할 수 있으며 Packet Sniffing으로부터 안전할 수 있다[9].

### 3.4 기타

현재 널리 사용되고 있는 뉴스 서버 프로그램의 하나인 INN 2.3.2 버전의 경우 보안 서비스를 제공하기 위해 SSL(Secure Sockets Layer)과 PGP(Pretty Good privacy)의 적용이 가능하다. SSL은 트랜스포트 레이어에서 작동되며 클라이언트/서버 인증용으로 사용하여 사용자가 포스팅하는 글의 불법변조를 막을 수 있으며, PGP의 전자서명(Digital Signature)를 이용하여 포스팅한 사용자의 신분을 확인할 수 있는 토대를 제공할 수 있다.

## III. 결 론

본 논문에서는 유즈넷 서비스에서 제공하고 있는 인증방법에 대한 일반적인 문제점과 Packet Sniffing, IP Spoofing, Hijacking을 이용한 해킹 방법 그리고 유즈넷 서비스에서 발생가능한 기타 보안 문제점에 대하여 살펴보고 이에 대한 해결방안으로서 ID/PW의 일반적인 관리 중점사항과 PAM 적용, SSH 사용 그리고 특정 뉴스 서버 프로그램에 적용가능한 보안방법에 대하여 살펴보았다.

본 논문에서 나열한 해결방안에 대하여 종합적인 사용을 적용하여 보다 안전한 유즈넷 서비스 제공이 가능하다고 판단된다.

유즈넷 서비스 관점에서의 인증에 대한 문제점과 일반적인 해결방안에 대한 논문이지만 차후에 뉴스서버 프로그램과 뉴스리더(News Reader) 프로그램 자체에 보안 기능이 적용될 수 있도록 연구되어야 할 것이다.

유즈넷 서비스의 본래 목적인 특정 주제에 대한 심도 깊은 최신의 정보를 얻을 수 있는 인터넷 서비스가 될 수 있기를 바란다.

### 참고문헌

- [1] '사용자망 구축 및 관리기술 지침서', 한국 과학기술정보연구원, pp.434, 2002.
- [2] '고성능 News와 FTP서버 관리기술 개발', 배재대학교, pp.16-17, 2001.
- [3] han.rec.humor동우회, '상용뉴스서버 목록', <http://user.chollian.net/~driveway/>
- [4] '네트워크 스니핑 기술 및 방지대책', 한국 정보보호진흥원, 2000.7.
- [5] 'TCP Connection Hijacking 공격 및 대책', 한국정보보호센터, 1999.
- [6] 오태호, 'IP Spoofing 공격', 포항공과대학교 PLUS.
- [7] eric maiwald, '네트워크 보안핸드북', 인포 북, pp.309-310, 2001.
- [8] Peter Hernberg, 'User Authentication HOWTO', <http://kldp.org/HOWTO/html/User-Authentication-HOWTO/index.html>
- [9] 임은재, 'SSH Howto', <http://kdtp.kldp.org/KoreanDoc/html/SSH-KLDP/>, 2002.2.8.