TTSSH와 PuTTY의 비교 분석

강민정* · 강민수* · 박연식**

*경상대학교 · **경상대학교 해양산업연구소

A comparision of TTSSH and PuTTY

Min-jung Kang* · Min-su Kang* · Yeoun-sik Park**

*Gyeong-sang National University · **GSNU-TOMI

E-mail : lundi@opentown.net, mikisoo@hitel.net, parkys@nongae.gsnu.ac.kr

요 약

리눅스를 포함한 유닉스 기반의 서버가 꾸준히 늘어나면서 MS군 사용자가 이러한 서버에 원격 접속하는 일이 많아졌다. 그동안은 telnet을 통한 접속이 많았으나 최근 secure shell(SSH)의 등장으로 무료로 사용 가능한 TTSSH나 PuTTY를 통한 접속이 점점 증가하고 있다. 본 논문에서는 이들의 특징과 사용법을 비교 분석하여 MS군 사용자를 위한 보다 효율적인 원격접속 툴을 제안한다.

ABSTRACT

As Unix based server including Linux are increased steadily, MS group users who want to connect these servers are increased. There were lots of connection using telnet for a while, but there are increased connection using "TTSSH or PuTTY" which get used free since "secure shell"(SSH) appeared recently. This paper compare TTSSH & PuTTY's characters and using method, and propose remote-access tool which improve TTSSH.

키워드

SSH, TTSSH, PuTTY, secure shell

Ⅰ. 서 론

ftp, pop, telnet 등과 같은 전통적인 네트워크 서비스들은 효율적이고 합리적이라 많은 사람들에 의해 사용되어져 오고 있지만, 원래 안전하지 못한 프로그램들이어서 네트워크를 통하여 전송되어지는 평문(plaintext) 형식의 사용자 패스워드와 데이터는 초보 해커에게도 쉽게 공격당할 수 있다.

그러나 SSH를 사용함으로써 이러한 문제점을 해결할 수 있다. SSH는 BSD의 r*명령어 사용법에 보안기능을 추가한 툴로써, 원격 작업을 하는데 있어서 보안을 유지하려는 노력의 일환으로 Tatu Ylönen에 의해 개발되었다.[1]

SSH는 패스워드를 포함하여 모든 통신을 암호화할 수 있는 쉘(shell)로써, 안심하고 원격접속 · 파일복사 등의 작업을 수행할 수 있다. 그래서 telnet을 대신할 수 있을 뿐 아니라 ftp, pop, ppp와 같은 tunnel 서비스도 제공한다.

SSH는 Tatu Ylönen에 의해 개발되어 현재는 대부분 운영체제에서 실행될 수 있도록 다양한 SSH 프로그램들이 출시되고 있다. 리눅스의 경우엔 OpenBSD에서 특허와 관련된 코드를 제거한 후 각종 기능을 추가한 free software인 OpenSSH를 사용한다. 물론 MS군 사용자를 위한 SSH 제품도 출시되어 있다. 표1은 MS군 기반 SSH 클라이언트 소프트웨어들로써, MS군 사용자들이 가장 많이 이용하는 프로그램은 무료로 사용 가능한 TTSSH와 PuTTY이다.[2][3]

본 논문에서는 OpenSSH 서버에 현재 MS군 사용자에 의해 가장 많이 이용되어지고 있는 TTSSH와 PuTTY를 비교 · 분석하여, MS군 사용자를 위한 개선된 TTSSH 클라이언트용 툴을 제안한다.

표 1. MS군 기반 SSH 클라이언트 소프트웨어

종 류	특 징
PuTTY	• SSH1과 SSH2 모두 지원 • 무료사용 • PSCP/PSFTP/Plink/Pageant 등 독립적인 SSH 툴 제공.
TTSSH	• SSH1만 지원 • 무료사용 • Teraterm Pro의 확장된 DLL 기능 이용 • 독립적인 툴 제공 안함.
Cygwin	• SSH1과 SSH2 모두 지원 • 무료사용 • 커맨드 라인 환경과 X윈도우 환경 모두 적합
MSSH	• SSH1만 지원 • 무료사용 • Metropolitan State College 개발
FreeSSH	• SSH1과 SSH2 모두 지원 • 무료사용 • 16bit 윈도우 시스템에서도 실행
SecureCRT	• SSH1과 SSH2 모두 지원 • 유료사용 • 안전한 로그인, 안전한 채널을 통한 파일 전송
MindTerm	• SSH1.5까지만 지원 • 유료사용 • 자바로 개발
Secure iXplorer	• PuTTY의 PSCP를 비롯한 모든 기능을 시각적 방식으로 구현 • 유료 사용
Winscp	• scp 기능을 쉽게 사용할 수 있도록 시각적 방식으로 제공(PuTTY와 유사) • 무료사용

II. TTSSH와 PuTTY의 비교

2.1 TTSSH

TTSSH는 1998년 Robert O'Callahan에 의해 만들어진 MS군 사용자를 위한 무료 SSH 클라이언트 프로그램이다. 이는 Teraterm Pro의 확장된 DLL 기능을 이용하여 실행되는데, Teraterm Pro의 기능 손실 없이 SSH 기능이 추가되었다.[4]

가장 최신 버전은 2001년 3월 21일 발표된 버전 1.5.4로 다음과 같은 특징을 가진다.

• SSH 버전 1.5와 양립된다.

• 사용 가능한 암호 알고리즘 : 3DES, Blowfish, DES

• ssh_known_hosts 파일을 이용한 서버 인증을 한다.

• 압축을 지원한다.

• forwarding 연결(X connection forwarding 포함) 기능을 제공한다.

• 독립적인 SSH 툴(scp, ssh-keygen, ssh-agent 등)을 전혀 포함하지 않는다.

• Teraterm에 종속되어 있기 때문에 쌍방간의 사용만 가능하다.

TTSSH는 자체적인 키 생성 능력이 없으므로, 서버에서 키를 생성하여 비밀키(보통 identity)는 클라이언트 컴퓨터에 복사하고 공개키(authorized_keys)는 서버에 저장하는 번거러운 과정으로 인하여 보안상 문제가 발생할 수 있다. 그 과정은 다음과 같다.

```
[lundi@inforcom lundi]$ssh-keygen
Generating public/private rsa1 key pair.
Enter file in which to save the key
(/home/lundi/.ssh/identity) :
Created directory '/home/lundi/.ssh'.
Enter passphrase (empty for no passphrase) :
Enter same passphrase again :
Your identification has been saved in
/home/lundi/.ssh/identity.
Your public key has been saved in
/home/lundi/.ssh/identity.pub.
The key fingerprint is :
d4:75:5d:63:c7:5c:da:d5:9c:b5:4c:96:02:3e:2f:f0
lundi@inforcom.gsnu.ac.kr
[lundi@inforcom lundi]$cd .ssh
[lundi@inforcom .ssh]$ls
identity identity.pub
[lundi@inforcom .ssh]$mv identity.pub
authorized_keys
[lundi@inforcom .ssh]$chmod 700 .
[lundi@inforcom .ssh]$chmod 600 authorized_keys
[lundi@inforcom lundi]$cd .ssh
```

TTSSH는 네가지 인증방법이 있다.

첫 번째 인증방법은 "Use plain password to log in" 방식이다. 이는 passphrase 박스에 패스워드를 입력하여 서버에게 직접 전송한다. telnet과 다른 점은 패스워드가 암호화된 채널을 통하여 전송되므로 단순한 공격으로는 암호를 훔쳐낼 수 없다는 것이다. 그러나 암호가 노출된다면 SSH도 telnet과 다를바 없게 된다.

두 번째 인증방법은 "Use RSA key to log in" 방식이다. RSA private key인 identity를 선택함으로써 인증되는 방법으로, 이 파일은 ssh-keygen 명령에 의해 생성되어진다. 대부분 이 파일은 passphrase에 의해 보호되고 있으므로 passphrase box에 키 생성시 입력했던 passphrase를 기입한다. 채널을 통하여 패스워드를 직접 전송하는 것 보다 더 안전하고 비교적 쉬운 사용법 때문에 가장 많이 이용되고 있는 방법이다.

세 번째 인증방법은 "Use rhosts to log in" 방식이다. 리모트(remote) 컴퓨터가 인식할 수 있는 로컬

(local) 컴퓨터의 이름을 입력하면 패스워드 입력 없이 인증이 이루어지는 방식이다. 만약 RSA키를 사용하는 서버에 로컬 컴퓨터를 인증시키고 싶다면 호스트의 private key 파일을 선택해야 한다. passphrase는 RSA와 마찬가지로 이 키에 접근하기 위하여 사용된다. 그러나 TTSSH가 1024이하의 포트를 자동 할당하기 때문에 firewall를 사용하는 사용자들은 이 인증방법을 사용할 수 없다. 그래서 이 방법은 기본값으로 활성화되어 있지 않으므로 다음과 같은 옵션을 덧붙여서 컴파일하여야 한다.

"--with-rsh=PATH"

네 번째 인증방법은 "Use challenge/response [TIS] to log in" 방식이다. 패스워드 없이 서버가 먼저 challenge 메시지를 전송하면 클라이언트가 response 하는 방식으로 인증이 이루어진다. 기본값으로 활성화되어 있지 않기 때문에 다음과 같은 옵션을 덧붙여 설치해야 한다.

"--with-skey=PATH"

그리고 이 옵션을 사용하고자 한다면 먼저 "s/key libraries"를 별도로 다운 받아 설치해야만 한다. S/key는 컴퓨터에 접근하는 것을 인증하기 위하여 "one-time password"를 사용한다. 이는 MD4, MD5, SHA1, RIPEMD-160과 같은 알고리즘에 의해 전송되어지는 정보(64bit)를 사용하는데, 안전한 컴퓨터에 의해 생성되어지는 여섯자리 영단어 형식으로 구성되어진다.

공개키를 이용한 TTSSH 인증과정은 그림 1과 같다.

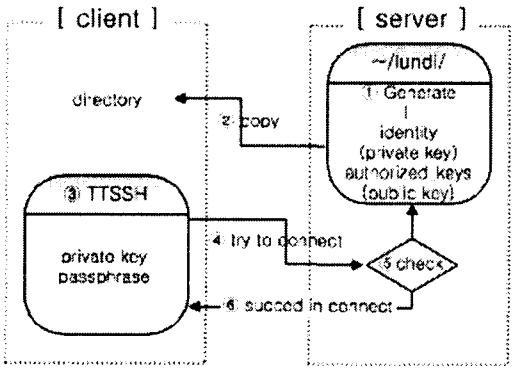

그림 1. 공개키를 이용한 TTSSH 인증과정

2.2 PuTTY

PuTTY는 1998년에 Simon Tatham에 의해 만들어진 win32 플랫폼 윈도 사용자를 위한 무료 SSH 프로그램으로 xterm 터미널 에뮬레이터를 기반으로 사용한다.[5]

가장 최신 버전은 2002년 1월 14일 발표된 버전 beta 0.52로 다음과 같은 특징을 가진다.

- 버전 0.50부터 SSH2를 제공한다.
- 사용 가능한 암호 알고리즘 : 3DES, Blowfish, DES, AES
- RSA,DSA 모두 SSH2에서 공개키로 제공된다.
- 독립적인 SSH 툴을 가진다. (PSCP, PSFTP, PuTTYtel, Pageant, PuTTYgen)
- port forwarding과 X11 forwarding 가능하다.
- full-screen 모드를 제공한다.

PuTTY는 독립적인 여섯 개의 툴을 가지는데. 각각 다음과 같은 용도로 사용된다.

① PuTTY : 텔넷과 SSH 모두 사용 가능한 클라이언트
② PSCP : command-line형식의 SCP 클라이언트
③ PSFTP : SFTP 클라이언트
④ PuTTYtel : 텔넷 사용만 가능한 클라이언트
⑤ Pageant : PuTTY와 PSCP 그리고 Plink를 위한 SSH 인증 에이전트
⑥ PuTTYgen : 사용자의 비밀키와 공개키를 생성하는 유틸리티

PuTTY는 PuTTYgen이라는 툴을 이용하여 공개키와 비밀키를 생성한다. 새로운 키를 생성하기 위해서는 먼저 생성하고자 하는 키 형태와 키 길이를 선택해야 한다. PuTTYgen에서 제공하는 키 형태는 SSH1 프로토콜에 대한 RSA와 SSH2 프로토콜에 대한 RSA, DSA 세가지이다. 키 형태와 키 길이 선택이 끝나면 실제적인 키 생성을 위하여 "Generate" 버튼을 누른다. key 박스에 진행막대가 표시되고, 임의성(randomness) 확보를 위하여 마우스를 key 박스 주위로 움직여야 한다. 충분한 임의성을 모으게 되면 진행막대 표시가 점차 채워지고 진행 막대가 끝에 도달하는 순간 키가 생성될 것이다. PuTTYgen이 생성한 공개키는 서버에 복사한다. 서버가 유저의 신분을 확인하고자 할 때 PuTTY는 유저의 비밀키를 이용하여 signature를 생성한다. 서버는 signature를 검증하고 로그인을 허락한다. 이때 서버가 해킹을 당했거나 spoofing된 경우, 공격자는 유저의 비밀키나 패스워드 대신 재사용이 불가능한 signature만 얻게 되므로 안전하다고 할 수 있다. 하지만 비밀키가 유출될 경우를 대비하여 반드시 패스프레이즈로 비밀키를 암호화하도록 한다.

그림 2는 PuTTY 인증과정을 그림으로 나타낸 것이다.

이상에서 살펴 본 TTSSH와 PuTTY의 차이점을 정리하면 표 2와 같다.

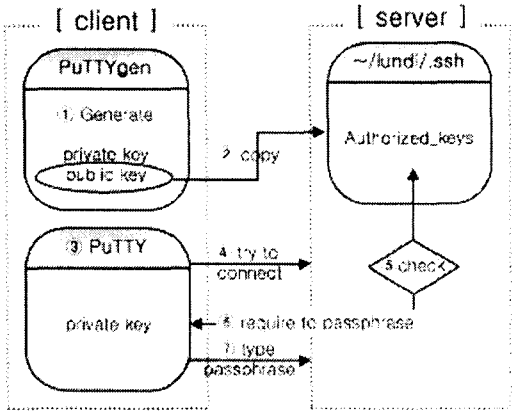

그림 2. PuTTY 인증과정

표 2. TTSSH와 PuTTY의 차이 비교

항목	TTSSH	PuTTY
SSH 지원	SSH 1.5	SSH1, SSH2
키 생성 능력	자체 생성 불가능 (ssh-keygen 이용)	자체 생성 가능 (PuTTYgen 이용)
사용 가능한 대칭키 알고리즘	DES, blowfish, Triple DES	DES, blowfish, Triple DES, AES
공개키 지원	RSA1	RSA1, RSA2, DSA
인증방법	4가지	1가지(공개키 인증)
비밀키와 공개키	identity(변경가능), identity.pub→authorized_keys	정해져 있지 않음. 단, 공개키명 변경 →autyorized_keys
독립적인 툴 보유	독립적인 툴 없음	6개의 독립적인 툴 있음

III. 개선된 TTSSH 원격접속 툴 제안

현재 TTSSH의 가장 큰 문제는 SSH 버전2를 제공하지 않는다는 것과 공개키 인증방식의 안전성 결여다. 그래서 본 논문에서는 SSH 버전2 지원과 자체 키 생성 능력을 부여하여 TTSSH를 개선하고자 한다. TTSSH의 인증방식 중 "Use challenge/ response [TIS] to log in" 을 이용한 방법이 있다. 이는 s/key 일회용 패스워드 기법을 적용한 것으로, 현재의 TTSSH로서는 공개키 사용법 보다 더 안전한 방법이다. 그러나 사용하기 위한 절차가 까다롭고 자동으로 일회용 패스워드가 생성되지 않아서 사용하기도 힘들다. 그래서 공개키를 이용한 인증방법의 문제점을 해결함으로써 TTSSH의 안전성을 향상시키고자 한다. 그림3은 SSH 버전2를 추가시킨 TTSSH의 메인 화면이다.

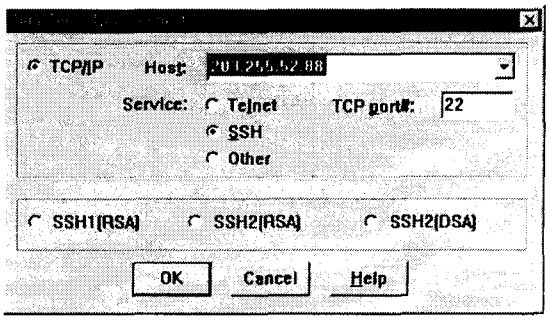

그림 3. SSH 버전2가 추가된 TTSSH

공개키 생성능력을 TTSSH 프로그램에 추가시키기엔 너무 많은 시간이 필요하고 프로그램이 복잡해진다. 그래서 PuTTYgen을 그대로 사용하여 공개키를 생성하고 사용할 것을 추천한다. 본 논문에서는 PuTTYgen을 이용하여 TTSSHgen을 새로 생성하였다.

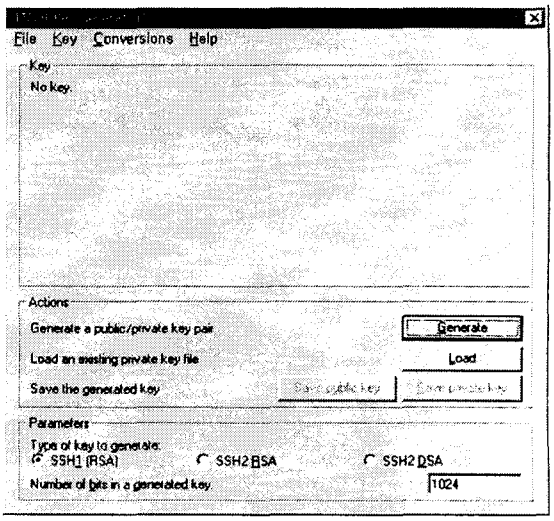

그림 4. TTSSHgen

IV. 결 론

정확한 수치는 알 수 없으나 우리나라는 PuTTY 사용률보다 TTSSH 사용률이 훨씬 높다. 그러나 TTSSH는 PuTTY와 비교・분석하여 본 결과 안전성이 낮은 편이다. 먼저 SSH 버전2가 지원되지 않으며, 둘째 자체적인 키 생성능력이 없음으로 공개키 인증방법을 사용할 경우 서버에서 공개키 쌍을 생성하여 유저 컴퓨터로 옮겨야 한다. 이러한 문제점 해결을 위하여 PuTTY 소스를 이용하여 SSH 버전2와 자체적 키 생성기인 TTSSHgen을 추가하였다. 그러나 scp와 sftp의 기능을 제공하는 독립적인 툴이 없으므로 여전히 PuTTY보다 기능이 부족하다. 따라서 앞으로 계속

이러한 툴에 대한 연구가 있어야 할 것이다.

참고문헌

[1] http://www.ssh.com
[2] 리눅스매거진편집부, SSH, Linux magazine 7월호, P78, 2001
[3] http://www.jfitz.com/tips/ssh_for_windows. html
[4] Robert O'Callahan, TTSSH : An SSH Extension to Terterm Version 1.5, http://www.xipworld.com.au/~roca/ttssh.html
[5] Simon Tatham, PuTTY : A Free Win32 Telnet/SSH Client, http://www.chiark.greenend.org.uk/~sgtatham/putty