ISBN 978-89-6211-016-6 98560

공개키를 이용한 OpenSSH 접속 방법

일 자: 2007년 12월 21일
부 서: 고성능연구망사업단
제출자: 이길재, 권윤주, 석우진, 곽재승
{giljael, yulli, wjseok, jskwak}@kisti.re.kr

한국과학기술정보연구원
305-806 대전광역시 유성구 어은동 52번지
TEL (042)869-0676 / FAX (042)869-0679
www.kisti.re.kr

공개키를 이용한 OpenSSH 접속 방법

Secure Shell (SSH) 공개키 인증은 클라이언트가 서버에 접속할 때 사용될 수 있는 방법이다. 본 문서는 공개키를 이용하여 OpenSSH 접속을 수행하는 방법을 설명한다. 아래에서 설명하는 방법은 kerboros나 OpenAFS와는 동작하지 않는다.

우선, 이해를 돕기 위해서 공개키를 이용한 OpenSSH 접속 방법을 간략한 예를 들어서 설명을 하기로 한다. 공개키는 자물쇠, 비밀키는 열쇠, 그리고 SSH의 버전은 자물쇠와 열쇠를 만드는 공장에 비유할 수 있다. SSH의 버전이 다른 상태에서 생성한 자물쇠와 열쇠는 함께 동작할 수 없다. 또한, 내가 가지고 있는 열쇠는 같은 자물쇠면 어디든지 열 수가 있다. 이를 바탕으로 공개키와 비밀키를 이용한 인증과정을 설명하면 다음과 같다.

- 클라이언트에서 서버로 접속을 원할 경우 자신의 자물쇠(공개키)를 서버 쪽에 보낸다.
- 클라이언트에 저장되어 있는 자신의 열쇠(비밀키)는 남에게 노출하면 안된다. 따라서 파일 권한 설정 작업이 필요하다.
- 자신의 열쇠와 맞는 자물쇠로 잠금되어 있는 서버에는 언제든지 로그인할 수 있다.
- 서버->클라이언트 접속을 원할 경우도 클라이언트->서버로 접속할 경우와 마찬가지이다. 클라이언트 쪽에 자신의 열쇠와 맞는 자물쇠만 있으면 된다.
- 이때, 새로운 자물쇠와 열쇠를 만들 필요는 없다. 자신이 가지고 있는 자물쇠를 클라이언트 시스템에 복사하고 클라이언트 시스템에 있던 자신의 열쇠를 서버에 복사해 놓으면 역시 접속이 가능한 것이다.

용어정의:

클라이언트 시스템 : 특정 서버에 SSH접속을 시도하는 랩탑 또는 데스크탑 컴퓨터

서버 : 클라이언트 시스템으로부터 접속되는 컴퓨터. 처음 접속되는 서버를 통해서 다시 연결되는 다른 컴퓨터도 해당

1. OpenSSH 버전 확인

먼저, 서버와 클라이언트 시스템에 설치된 SSH 소프트웨어가 OpneSSH 인지 확인한다. 일반적으로 Linux Fedora Core 시리즈에는 OpenSSH가 설치되어 있다. 키 생성은 SSH의 구현에 따라서 다양할 수 있다. ssh -V 명령을 실행했을 때 아래와 같이 OpenSSH로 시작하는 결과를 얻으면 되며 반드시 일치할 필요는 없다.

```
[giljael@proxy1 ~]$ ssh -V
OpenSSH_4.2p1, OpenSSL 0.9.7f 22 Mar 2005
```

2. 키 생성

A. Linux 시스템

RSA키 쌍 (공개키, 비공개키)를 생성해야 하며 클라이언트 시스템에서 생성한다고 가정한다. 키 쌍중 공개키 부분은 접속되는 서버에 옮겨 놓을 것이다. 개인키 부분은 클라이언트 시스템의 안전한 장소에 보관되어야 하는데 디폴트 디렉토리는 [개인홈]/.ssh/이다. 클라이언트 시스템에서 다음의 명령을 수행한다.

```
[giljael@proxy1 ~]$ mkdir ~/.ssh
[giljael@proxy1 ~]$ chmod 700 ~/.ssh
[giljael@proxy1 ~]$ /usr/bin/ssh-keygen -q -t rsa
Enter file in which to save the key (/home/giljael/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

주의: passphrase를 입력할 경우 시스템 계정과 같은 password나 empty passphrase는 사용하지 않는다.

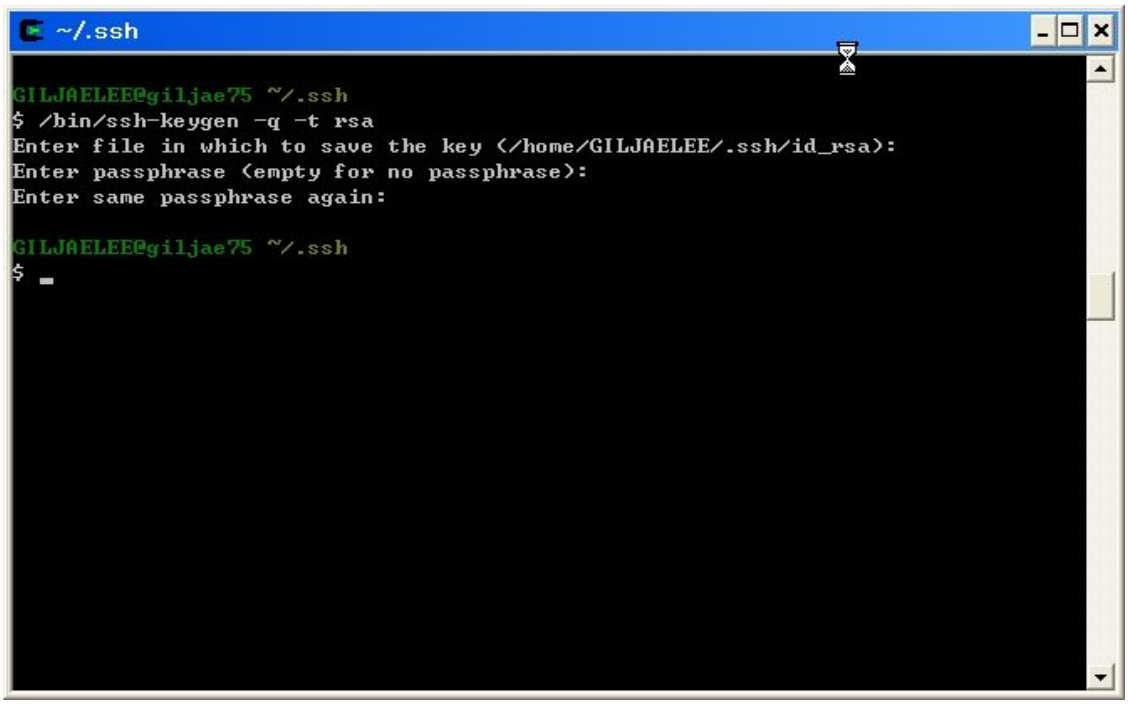
생성된 키 쌍은 반드시 다른 유저가 읽을 수 없도록 제한을 두어야 한다. OpenSSH는 버전에 따라서 파일 권한이 제대로 설정되어 있지 않으면 공개키 인증을 거부할 수도 있다. 아래의 명령을 꼭 실행한다.

```
[giljael@proxy1 ~]$ chmod go-w ~/
[giljael@proxy1 ~]$ chmod 700 ~/.ssh
[giljael@proxy1 ~]$ chmod go-rwx ~/.ssh/*
[giljael@proxy1 ~]$
```

B. Windows 시스템 (Cygwin, Xmanager, putty)

a. cygwin

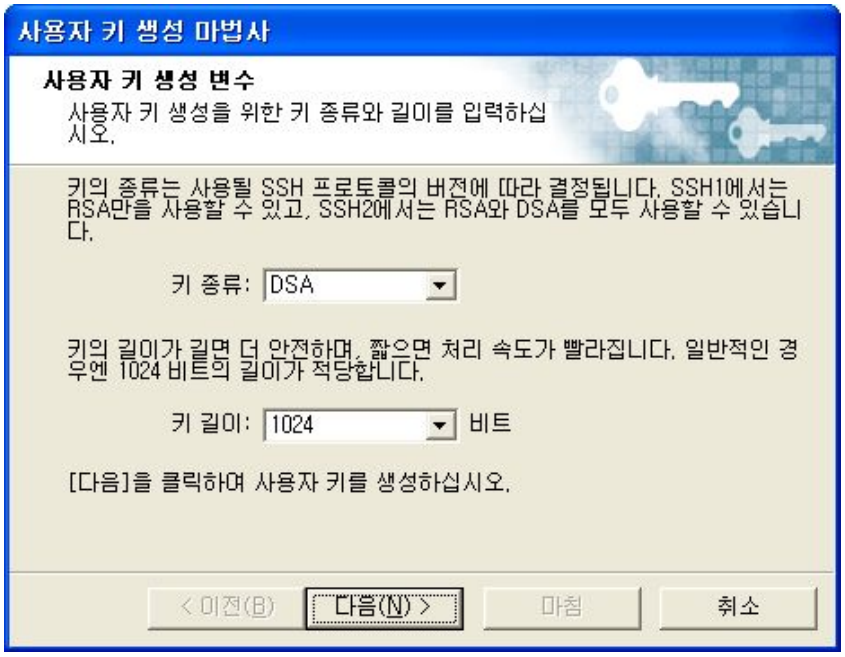
RSA키 쌍 (공개키, 비공개키)를 생성해야 하며 클라이언트 시스템에서 생성한다고 가정한다. 키 쌍중 공개키 부분은 접속되는 서버에 옮겨 놓을 것이다. 개인키 부분은 클라이언트 시스템의 안전한 장소에 보관되어야 하는데 디폴트 디렉토리는 [개인홈]/.ssh/이다. 클라이언트 시스템에서 다음의 명령을 수행한다. linux 시스템의 경우와 동일하다.



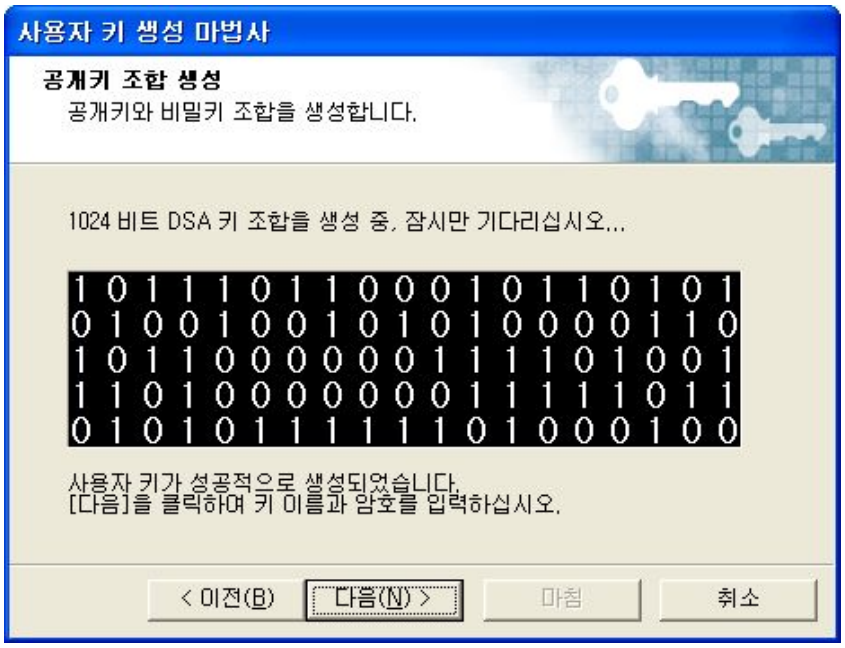
b. Xmanager

Xmanager에서 사용할 수 있는 공개키를 생성하기 위해서는 Xshell이라는 프로그램을 사용하거나 Cygwin 등을 이용해서 공개키를 생성하는 두 가지 방법이 있다. 본 절에서는 Xshell이라는 상용 프로그램을 이용해서 공개키를 생성하는 과정을 설명한다.[6]

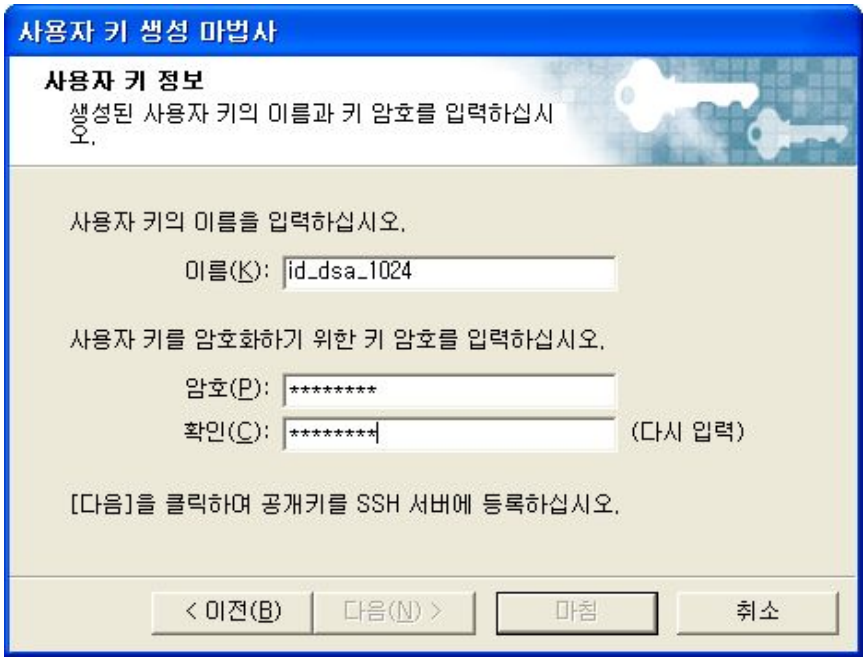
먼저, Xshell을 실행시키고 [도구] 메뉴에서, [사용자 키 생성 마법사]를 선택한다.



키 종류 리스트에서 DSA 또는 RSA를 선택한다. SSH1 프로토콜은 RSA 키 만을 지원하며 SSH2 프로토콜은 RSA 와 DSA 모두를 지원한다. 원격 서버가 지원하는 키 종류를 선택해야 한다. 키 길이 리스트에서 키 길이를 선택한다. 키 길이가 길면 보다 안전하고, 짧으면 처리 속도가 빨라진다. 일반적인 경우 1024 비트가 적당하다. [다음]을 선택하여 키 생성 단계로 진행한다.



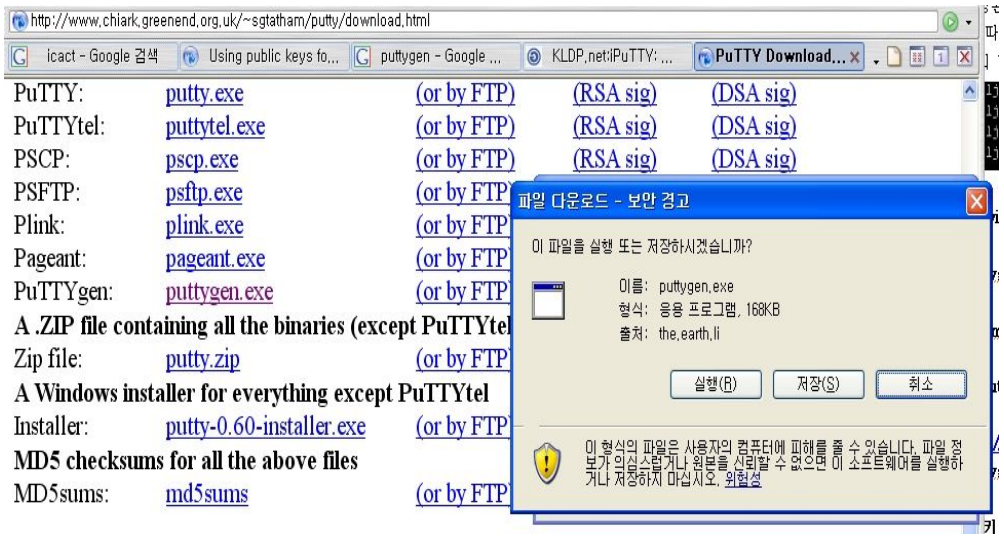
키 생성이 성공적으로 끝나고 나면, [다음]을 선택하여 사용자 키 정보 입력 화면으로 진행한다.



[이름]에는 생성된 키의 이름을 입력한다. 임의로 설정하면 된다. 사용자 키는 파일로 저장되므로 키 이름은 파일명으로 유효한 문자로 이루어져야 한다. [암호]에는 사용자 키의 암호를 입력한다. 키를 사용할 때 마다 필요하므로 꼭 기억해 두어야 한다. [확인]에는 위에서 입력한 암호를 다시 한번 입력하고 [다음]을 선택하여 다음 공개키 등록 단계로 진행한다.

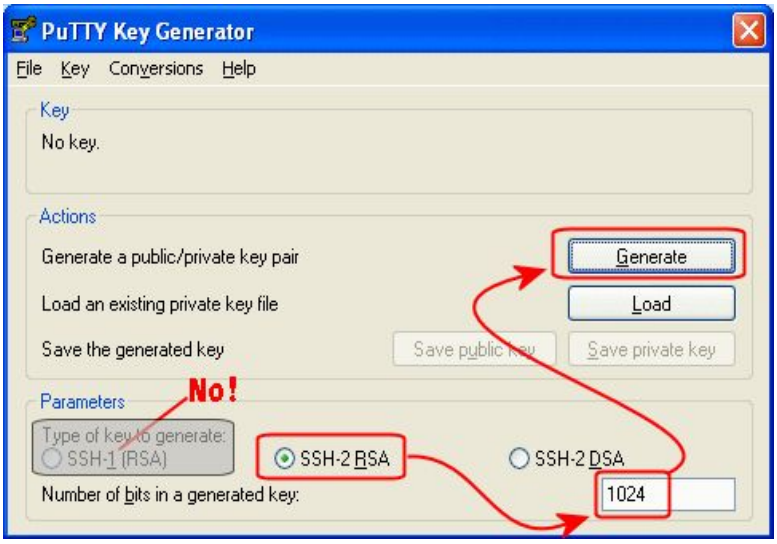
c. putty

공개 ssh 터미널인 putty를 사용한다면 key를 생성하기 위해서 먼저 http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html 사이트에서 puttygen.exe 를 다운로드 받는다.



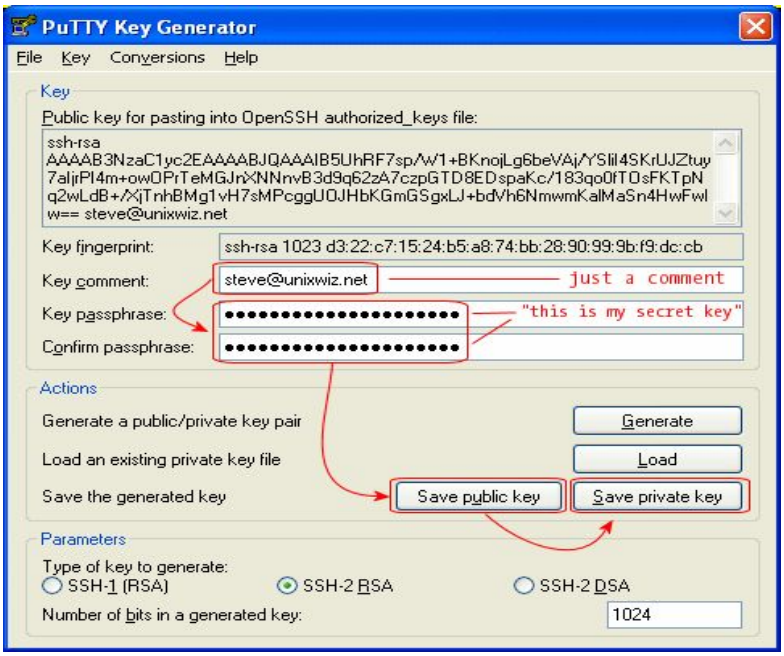
puttygen.exe를 실행시키고 key type과 key size를 선택한다. 우리는 RSA key를 이용하

며 SSH 2 protocol을 사용할 것이다. 또한, key size는 기본 값인 1024 bits를 사용해도 무방하다. 설정이 끝나면 "Generate" 버튼을 눌러서 RSA키 쌍을 생성한다. 생성하는 중에 마우스를 계속 움직여 주면 생성되는 키의 임의성을 증가시킬 수 있으며 키 생성도 빨리 진행됨을 명심해야 한다.



"Key fingerprint" 상자에 생성된 키의 핑거프리트 값이 보여진다. 이 값은 공개 키 값을 암호화해서 보여주는 것이므로 보안을 유지할 필요는 없다. putty는 사용자가 하나의 시스템에 여러 개의 키를 가질 수 있도록 각 키에 대해서 설명 값을 설정할 수 있다. 생성된 key에 대해서 적당한 설명 값을 "Key comment" 항목에 추가하면 된다.

생성된 비밀키에 대한 암호를 설정한다. 이때 생성된 키에 대해서 암호를 설정하지 않으면 컴퓨터에 저장된 키 값은 위험에 노출된다. 키가 생성되고 해당 설정이 마무리되면 이제 "Save private key"버튼과 "Save public key"버튼을 이용해서 원하는 위치에 비밀키와 공개키를 저장한다.



3. 키 분배

A. Linux 시스템

RSA 키 쌍의 공개키 부분은 클라이언트 시스템이 접속하려고 하는 서버에 복사되어야 한다. 복사되는 공개키 정보는 클라이언트 시스템의 ~/.ssh/id_rsa.pub 파일이다. 본 고에서는 모든 서버를 OpenSSH 기반으로 가정한다. 모든 공개키 정보는 서버의 ~/.ssh/authorized_keys 파일에 추가되어야 한다. 아래는 **서버측**에서 수행되어야 할 일련의 과정을 나타낸다.

```
[giljael@proxy1 ~]$ scp ~/.ssh/id_rsa.pub 134.75.110.130:
giljael@134.75.110.130's password:
id_rsa.pub                                    100%  396     0.4KB/s   00:00
[giljael@proxy1 ~]$ ssh giljael@134.75.110.130
giljael@134.75.110.130's password:
Last login: Fri Jun 29 10:56:05 2007 from 134.75.21.100
[giljael@proxy2 ~]$ mkdir ~/.ssh
[giljael@proxy2 ~]$ cat ~/id_rsa.pub >> ~/.ssh/authorized_keys
[giljael@proxy2 ~]$ chmod 600 ~/.ssh/authorized_keys
[giljael@proxy2 ~]$ rm ~/id_rsa.pub
[giljael@proxy2 ~]$
```

주의: 새로운 공개키 정보는 authorized_keys 파일에 추가되어야 하며, 각 공개키 정보는 서로 다른 라인에 추가되어야 한다.

여러 가지 이유로 인하여 공개키 기반 인증이 동작하지 않을 수 있으니 서버로의 접속이 잘 되는지 다음과 같은 방법으로 확인하면 된다.

```
[giljael@proxy2 ~]$ ssh -o PreferredAuthentications=publickey 134.75.21.100
Enter passphrase for key '/home/giljael/.ssh/id_rsa':
Last login: Mon Jul  2 10:04:21 2007 from 134.75.110.130
[giljael@proxy1 ~]$
```

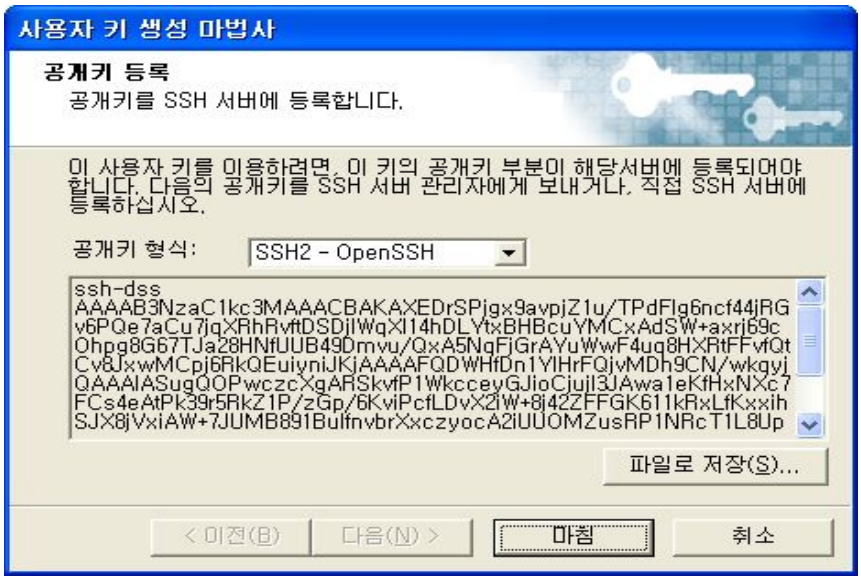
B. Windows 시스템 (Cygwin, Xmanager, putty)

a. cygwin

공개키는 한 라인으로 구성되어 있어야 하므로 authorized_keys 파일에 저장할 경우 주의해야 한다. 나머지 부분은 linux 시스템의 경우와 동일하다.

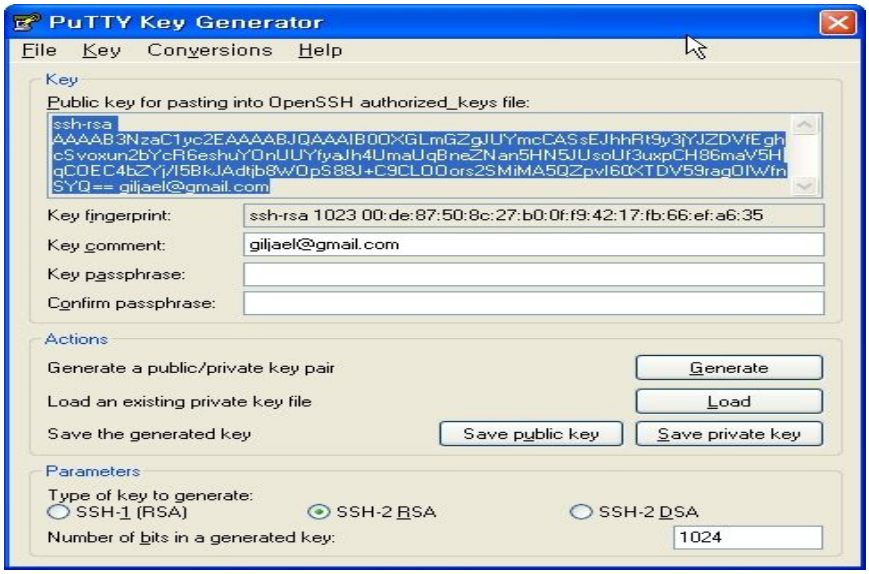
b. Xmanager

Xshell 프로그램을 이용해서 생성한 사용자 키의 공개키 부분을 원격 서버에 등록한다. 사용자 키는 Xshell의 사용자 키 데이터베이스에 저장됩니다. [공개키 형식] 리스트에서 SSH1, SSH2 - OpenSSH, 그리고 SSH2 - IETF SECSH 중 하나를 선택한다. 아래쪽 텍스트 상자에는 선택된 형식의 공개키가 나타날 것인데 나타난 공개키를 복사하거나 파일로 저장하여 원격 서버에 등록하면 된다. 나머지 부분은 linux 시스템의 경우와 동일하다.



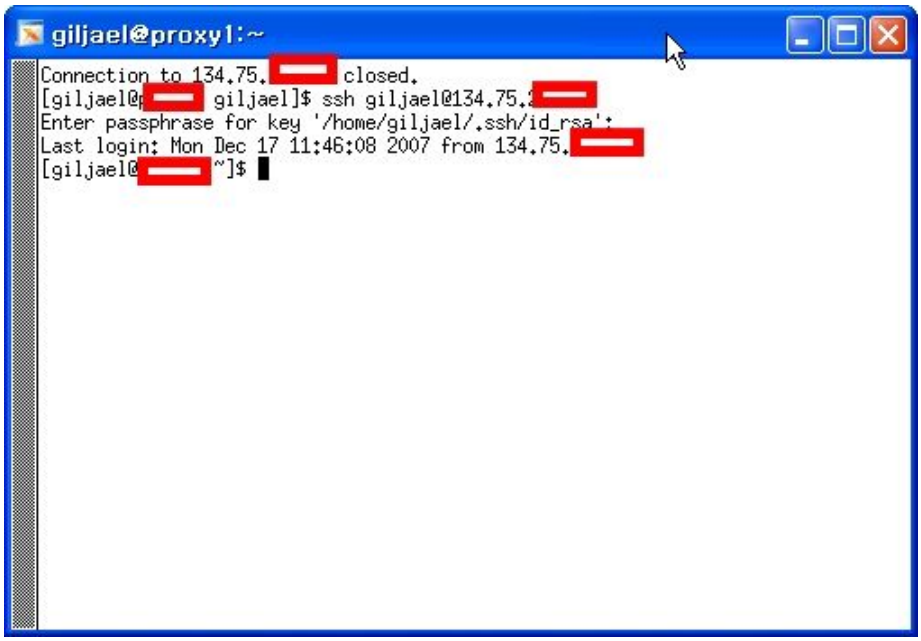
c. putty

puttygen에서 생성된 공개키는 "Public key for pasting into OpenSSH authorized_keys file" 항목에 있는 내용이다. 이 부분을 접속하고자 하는 시스템의 [개인계정]/.ssh/authorized_keys에 추가한다. 자세한 절차는 키 분배의 linux 시스템 부분을 따르면 된다. 공개키는 한 라인으로 구성되어 있어야 하므로 authorized_keys 파일에 저장할 경우 주의해야 한다.



4. SSH 접속

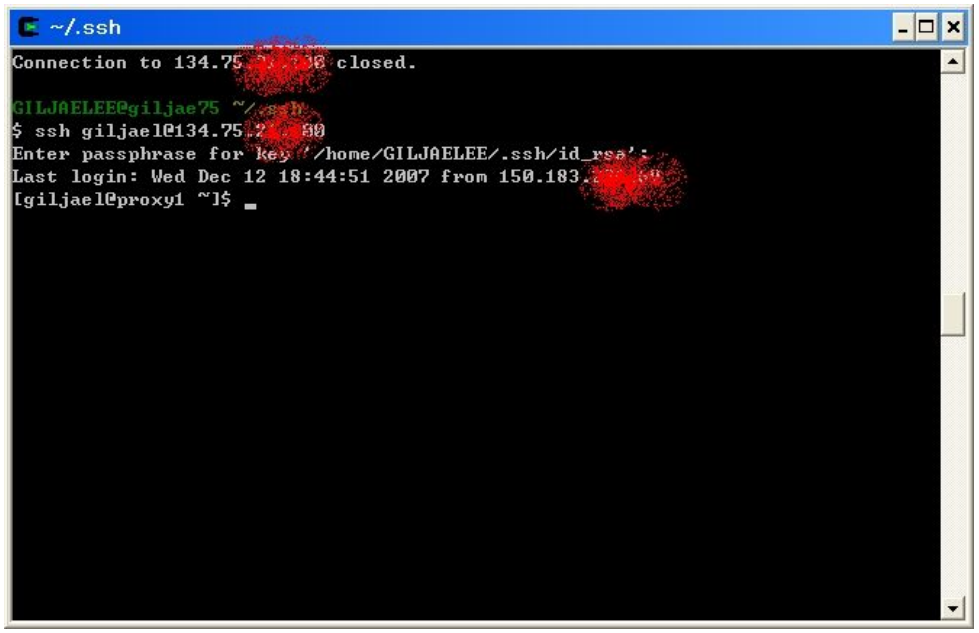
A. Linux 시스템



B. Windows 시스템 (Cygwin, Xmanager, putty)

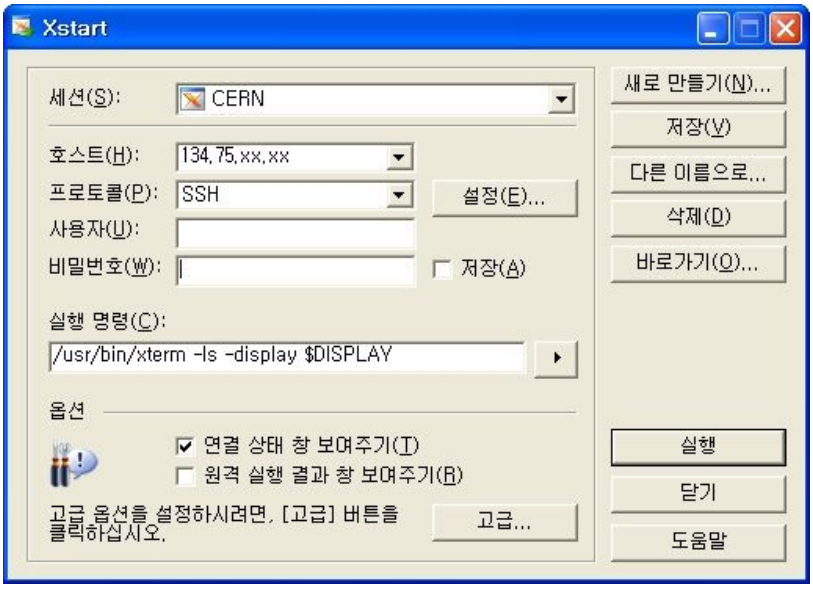
a. cygwin

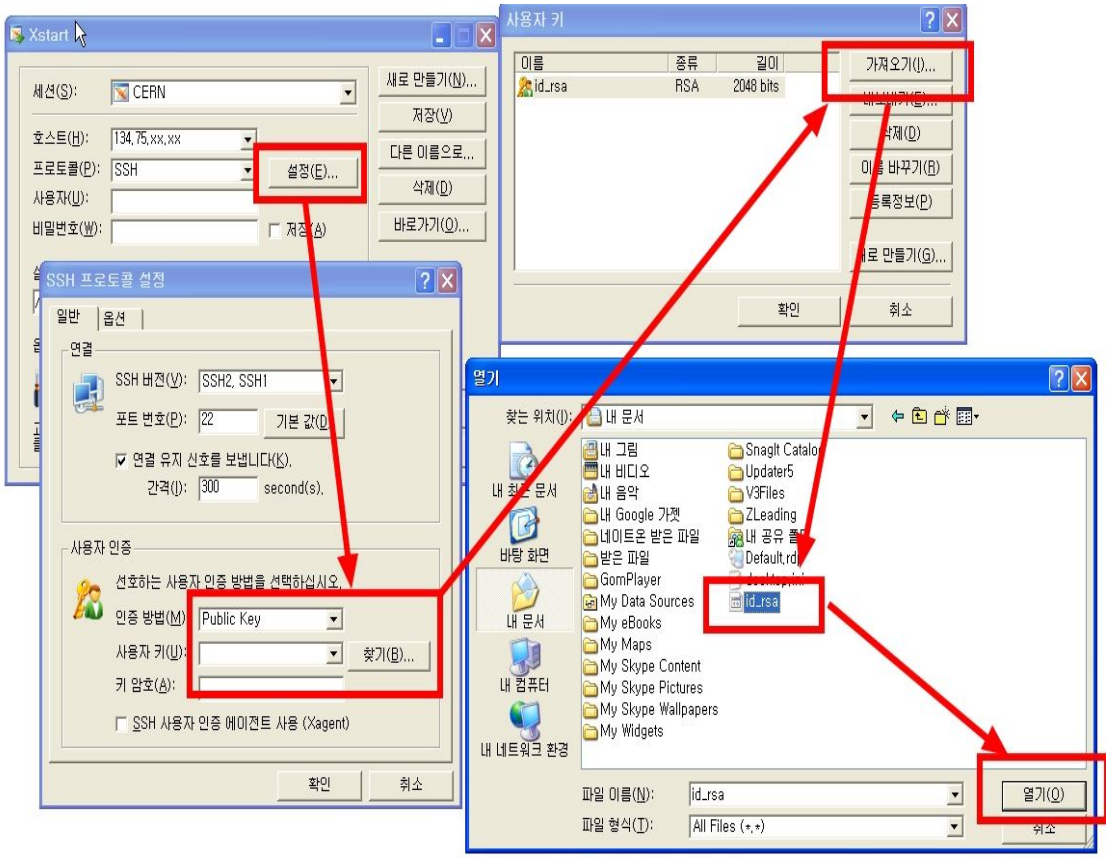
cygwin 터미널을 실행시킨 후에 linux 시스템의 경우와 동일한 방법으로 로그인하면 된다.



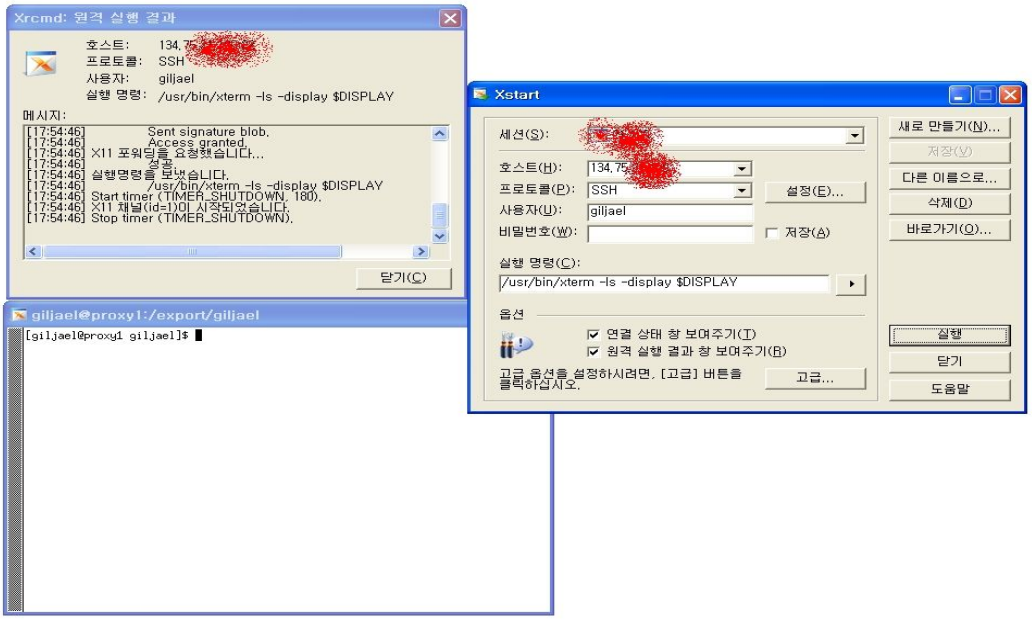
b. Xmanager

사용자의 시스템에 Xmanager 프로그램이 설치되어 있다고 가정한다. 먼저 Xstart를 실행한다. 접속하고자 하는 호스트명 등 관련 정보를 입력한 후에 설정버튼을 누른다.





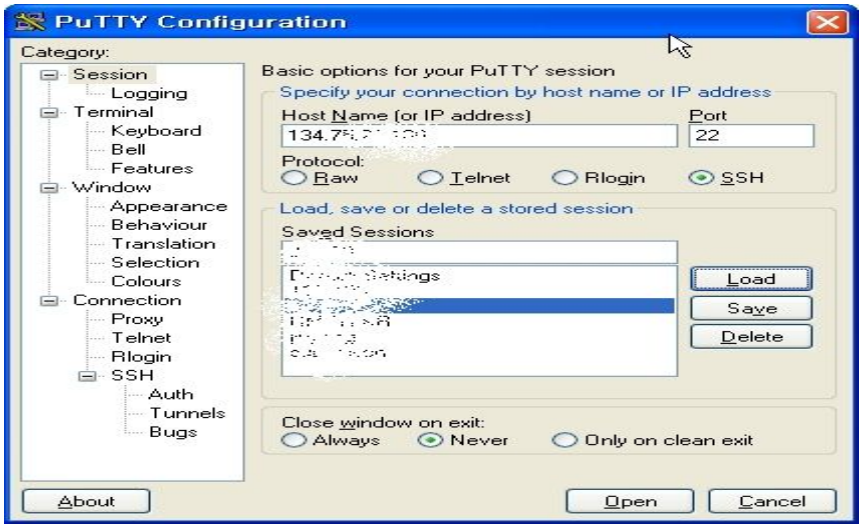
SSH 프로토콜 설정 창->사용자 인증 부분을 Public Key로 설정한 후에 "찾기"버튼을 눌러서 사용자 키->가져오기를 실행하여 이미 생성된 개인키를 선택하여 등록한다. Xstart의 시작 창에서 실행을 눌러서 해당 서버에 접속하면 된다. 아래 그림은 Xstart를 통한 실제 접속화면이다.

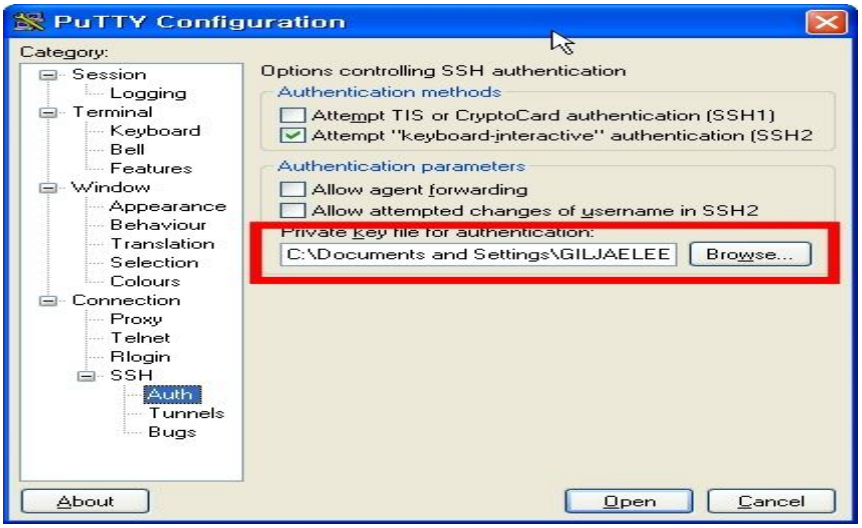


c. putty

puttygen.exe를 이용해서 생성한 공개키가 등록된 서버에 접속하기 위해서는 비밀키를 putty.exe에 첨부해야 한다. putty.exe를 실행하여 해당 설정을 해야 한다.

먼저, Host name과 Protocol을 설정한다. 비밀키를 이용하기 위해서 Category->Connection->SSH->Auth에서 puttygen을 이용해서 생성하여 저장해 놓은 비밀키의 위치를 지정해 준다. 그리고 다시 Category->Session으로 돌아와서 해당 설정을 Save key를 이용해서 저장한다. 모든 설정이 마무리 되었으므로 이제 해당 서버에 접속하면 된다. 아래의 그림은 134.75.xx.xx 시스템에 접속하는 과정을 보여준다.




PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Proxy
Telnet
Rlogin
SSH
Auth
Tunnels
Bugs
Options controlling SSH authentication
Authentication methods
Attempt TIS or CryptoCard authentication (SSH1)
Attempt "keyboard-interactive" authentication (SSH2
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH2
Private key file for authentication:
C:\Documents and Settings\GILJAELEE
Browse...
About
Open
Cancel


giljael@proxy1:~
login as:
Authenticating with public key "giljael@gmail.com"
Last login: Wed Dec 12 18:08:50 2007 from 150.183.
[giljael@proxy1 ~]$

참조

[1] http://sial.org/howto/openssh/publickey-auth/#s2.3
[2] https://www.racf.bnl.gov/docs/authentication/ssh/sshkeygenwin
[3] http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
[4] http://publib.boulder.ibm.com/infocenter/tsmscv13/index.jsp?topic=/com.ibm.mconsole.doc/fqg0_t_generating_an_ssh_key.html
[5] http://unixwiz.net/techtips/putty-openssh.html
[6] http://www.netsarang.co.kr/products/xsh_tutorial2.html#p1