joe ist ein simpler Texteditor.
pine und **mutt** sind Mail-Programme.
tin ist ein Newsreader unter Unix.

SSH-Tunnel aufbauen

Ein SSH-Tunnel wird dazu verwendet, eine bestimmte Verbindung vom eigenen Rechner, bzw. Netzwerk, zu einem Zielrechner oder Zielnetzwerk zu verschlüsseln.

In Putty unter Windows, geht man wie folgt vor: Man geht entweder vor dem Verbindungsaufbau oder nachdem die Verbindung schon steht, in die Einstellungen (dann, oben links klicken --> „Change Settings“). Hier zu „Connection“ --> „SSH“ --> „Tunnels“. Als „Sorce port:“ gibt man einen Port an, der am lokalen Rechner noch nicht belegt ist. Am besten einen Port größer als 1024.
Bei „Destination:“ gibt man den Zielrechner und den Port der Applikation an. Dies geschieht in folgender Form:<AdresseZielrechner>:<PortDerAnwendung>
Mit einem Klick auf „Add“ fügt man diesen Tunnel der Verbindung hinzu. Nach dem Bestätigen, startet man die lokale Anwendung.

Unter Linux und Mac OS X wird ein Tunnel direkt bei Verbindungsauf- bau, beim SSH-Befehl angegeben:
SSH -L <PortAmRechner><AdresseZielrechner>
<Port der Anwendung> <Account>@<SSH-Host>

In der Anwendung gibt man dann als Zieladresse Folgendes an:
localhost: < Port am eigenen Rechner>
Die Anwendung wird daraufhin durch SSH getunnelt.

Zusammenfassung

Hier noch einmal die wichtigsten Einstellungen:
Download von Putty:
http://www.chiark.greenend.org.uk/~sgtatham/putty/
Download von WinSCP: http://www.winscp.net
Verbindungsdaten:
Host: linux.student.kit.edu: 22
Username: uxxxx **(KIT-Benutzerkonto)**
Passwort: Login-Passwort (wie in den Pools)

Fingerprints:
DSA:
1024 2a:a0:e8:00:23:29:e2:50:91:cb:f4:db:e7:78:e3:14
ECDSA:
256 5c:96:76:06:c7:6f:b7:f9:bd:43:1b:6c:be:5c:fc:bd
RSA1:
2048 43:df:04:c3:17:2d:58:01:64:b0:d9:4a:b4:69:63:05
RSA:
2048 32:08:8a:b3:0a:32:8d:79:c8:00:b5:aa:a9:42:de:22

Kontakt

Karlsruher Institut für Technologie (KIT)
Steinbuch Centre for Computing

MicroBIT - Campus Süd
Zirkel 2
76131 Karlsruhe

Telefon: 0721 608-42997
E-Mail: microbit@scc.kit.edu

www.scc.kit.edu/microbit

Herausgeber

Karlsruher Institut für Technologie (KIT)
Steinbuch Centre for Computing
Zirkel 2 | 76131 Karlsruhe

Stand September 2014

www.kit.edu

Karlsruher Institut für Technologie

SSH

Per Shell auf den Linux-Maschinen des SCC arbeiten

ssh

Steinbuch Centre for Computing

KIT – Universität des Landes Baden-Württemberg und
nationales Forschungszentrum in der Helmholtz-Gemeinschaft

www.kit.edu

SSH – Was ist das?

Secure Shell oder SSH ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man sich über eine verschlüsselte Netzwerkverbindung auf einem entfernten Computer (bspw. die Linux-Maschinen im SCC) einloggen und dort Programme ausführen kann.

Hinweis: Im Flyer ist oft vom KIT-Benutzerkonto die Rede. Damit ist das Benutzerkonto uxxxx (für Studierende) oder ab1234 (für Mitarbeiter) gemeint.

Windows 7/8

Unter Windows gibt es mehrere Programme, die man verwenden kann, wir empfehlen Folgende:

Putty Client:
Putty ist ein kostenloses und frei verfügbares Programm. Es ermöglicht Befehle auf einem entfernten Rechner auszuführen. Download von Putty:
http://www.chiark.greenend.org.uk/~sgtatham/putty/

WinSCP:
WinSCP ist ein ebenfalls kostenloses und frei verfügbares Programm. Es ermöglicht den Datenaustausch mit einem entfernten Rechner durch eine dem Windows Explorer bzw. Norton Commander nachempfundene Oberfläche.
Download von WinSCP: http://www.winscp.net/

Bei beiden Programmen müssen nach der Installation und dem Start des Programms noch die Verbindungsdaten eingegeben werden. Siehe dazu den Abschnitt „Verbindungsdaten“.

Mac OS X

Mac OS X unterstützt von Haus aus das SSH-Protokoll. Dazu das „Terminal“ öffnen und bei „Ablage“ --> „Mit Server verbinden...“ klicken. Hier „Sichere Shell (SSH)“ auswählen. Dann bei „Benutzer“ das KIT-Benutzerkonto (siehe Hinweis oben) eingeben und „SSH (automatisch)“ auswählen. Das Feld darunter bleibt zunächst frei. Mit einem Klick auf das Plussymbol, rechts am Fenster, erscheint ein neues Eingabefeld. Hier den
Host eingeben. (siehe Abschnitt „Verbindungsdaten“) Nun auf „OK“ klicken, jetzt muss im zuvor leer gelassen Feld „ssh <Verbindungsdaten>“ stehen.

Linux

Unter Linux kann man sich direkt im Terminal mit dem Befehl: *ssh <**KIT-Benutzerkonto**>@<Server>*
und den Verbindungsdaten anmelden.

Verbindungsdaten

Die folgenden Verbindungsdaten müssen immer an der entsprechenden Stelle angegeben werden.

Host:	linux.student.kit.edu
Port:	22
Username:	uxxxx (KIT-Benutzerkonto)
Passwort:	Login-Passwort

(wie bei der Anmeldung in den Poolräumen)

Verbindungsaufbau

Wenn man sich das erste Mal mit SSH an die Uni verbindet, wird man gefragt, ob man einen Host-Key annehmen will. Dabei wird ein „Fingerprint“ angezeigt, der dem oben angegebenen entsprechen sollte. Nur dann kann man sicher sein, dass man sich tatsächlich mit einer *Linux-Maschine* des SCC verbindet.
Hinter dieser *Linux-Maschine* verbirgt sich *linux.student.kit.edu*

Details zu den Windows Programmen

Hier eine Anleitung, wie man sich mittels Putty und WinSCP an das Steinbuch Centre for Computing verbindet.

Putty Client für Windows:
Nachdem Putty gestartet wurde, die Verbindungsdaten eingeben und auf „Open“ klicken. Es wird nun nach Username und Passwort gefragt. In der nun erscheinenden Shell (Eingabeaufforderung) können Befehle eingeben werden. Dazu mehr im Abschnitt „Wichtige SSH Befehle“. Achtung: Im Gegensatz zu Windows verrät Putty einem neugierigen Schultergucker auch nicht durch Sternchen wie viele Zeichen das Passwort hat.

WinSCP Client für Windows:
Wenn WinSCP gestartet wurde, auf „New“ klicken. Es erscheint ein Bildschirm, in dem die Verbindungsdaten eingegeben werden können. Als Protokoll „SCP“ wählen und auf „Speichern“ klicken. Nach
erfolgreichem Speichern kann man sich zukünftig nach Auswahl des eben erstellten Profils mit einem Klick auf „Laden“ am SCC anmelden. Man sieht nun die Ordnerstruktur des eigenen „Home-Verzeichnisses“. Es entspricht dem „Eigene Dateien“ Verzeichnis, wenn man sich in einem Poolraum am SCC einloggt.

Wichtig! Putty kann nur Dateien auf dem Home-Verzeichnis oder einem Unterverzeichnis davon ansprechen. Soll also eine Datei auf dem eigenen Computer verwendet werden (bspw. um sie auszudrucken), muss sie vorher z.B. per WinSCP in das „Home-Verzeichnis“ geladen werden.

Wichtige SSH-Befehle

- *ls* listet den Inhalt des aktuellen Verzeichnisses.
- Die Option *–a* listet den Inhalt des aktuellen Verzeichnisses mit den versteckten Dateien.
- *cd <Verzeichnis>* wechselt in das angegebene Verzeichnis. Ohne weitere Angabe eines Verzeichnisses wechselt man ins Homeverzeichnis zurück. Mit der Angabe „*/*“ wechselt man ins Wurzel-Verzeichnis.
- *rm <Option> <Datei oder Verzeichnis>* löscht Dateien oder Verzeichnisse. Die Option *-f* erzwingt das Löschen ohne nachzufragen. Die Option *-r* löscht Verzeichnisse rekursiv (also auch Unterordner).
- *pm <Datei>* druckt die angegebene Datei aus, nachdem der gewünschte Drucker aus dem Menü gewählt wurde. Anstatt <Datei> können auch Wildcards verwendet werden. Bspw. * für alle Dateien im Verzeichnis.
- *pdftops <Input.pdf> <Output.ps>* wandelt die angegebene PDF-Datei in eine PostScript-Datei um.
- *pstops <Input.ps> <Output.ps>* wandelt eine PostScript-Datei in ein von den SCC-Druckern lesbares PostScript-Format um.
- *psselect –p<Seite>-<Seite> <Input> <Output>* Nur bestimmte Seiten in die Ausgabedatei schreiben.
- *psnup -<Option> -<Seiten> <Input> <Output>* Um eine bestimmte Anzahl von Seiten auf einer Seite zusammenzufassen. Wichtig sind hier die Optionen **-l**, für die korrekte Ausgabe von Querformat-Dateien und *-d*, wenn man Linien zwischen den einzelnen Seiten haben will.
- *psresize* Um beliebig zu skalieren. Beispiel:
  psresize –pA4 – pA3 <Input.pdf> <Output.ps>
  Wandelt das Dokument von A4 nach A3 um (wählbare Formate sind A3, A4, A5, B5, letter, legal und 10x14).
- *bvprint* zeigt das noch verfügbare Papierkontingent an.
- *bvpasswd* ändert das Passwort.
- *newpublichtml* erstellt eine Homepage des Benutzers im Verzeichnis ~/.public _ html/ (Näheres im Flyer 06 „Homepage“).
- *chmod <Wert>* ändert die Rechte von Dateien und Verzeichnissen. Genaueres mit man chmod.
- *less <Datei>* zeigt den Inhalt einer Datei an.