delight, ssh, sshkey, key, keychain, ed25519, rsa

Stronger SSH Key and keychain

Sources

- https://security.stackexchange.com/questions/5096/rsa-vs-dsa-for-ssh-authentication-keys
- https://medium.com/risan/upgrade-your-ssh-key-to-ed25519-c6e8d60d3c54
- https://rubysash.com/operating-system/linux/enable-ed25519-ssh-keys-auth-on-ubuntu-18-04/
- https://linuxize.com/post/using-the-ssh-config-file/
- https://stefanbauer.me/articles/update-your-ssh-keys-to-ed25519

Implementation

```
ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/id_ed25519 -C "def@delight.wiretrip.inside"
touch ~/.bash_profile
chmod 600 ~/.bash_profile
vim ~/.bash_profile
```

```
/usr/bin/keychain --clear
```

```
touch ~/.ssh/config
chmod 600 ~/.ssh/config
vim ~/.ssh/config
```

```
Host *
  AddKeysToAgent        yes
  IdentityFile          ~/.ssh/id_ed25519
  IdentityFile          ~/.ssh/id_rsa
  ControlMaster         auto
  ControlPath           ~/.ssh/master-%r@%h:%p.socket
  ControlPersist        yes
  ServerAliveInterval   5
  ServerAliveCountMax   10

Host ONE
  HostName              one.domain.tld
Host TWO
  HostName              two.domain.tld

Host THREE
  HostName              three.domain.tld
```

```
vim ~/.bashrc
```

```
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
```

```
    *i*) ;;
      *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# If set, the pattern "**" used in a pathname expansion context will
# match all files and zero or more directories and subdirectories.
#shopt -s globstar

# make less more friendly for non-text input files, see lesspipe(1)
[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, unless we know we "want" color)
case "$TERM" in
    xterm-color|*-256color) color_prompt=yes;;
esac

# uncomment for a colored prompt, if the terminal has the capability; turned
# off by default to not distract the user: the focus in a terminal window
# should be on the output of commands, not on the prompt
#force_color_prompt=yes

if [ -n "$force_color_prompt" ]; then
    if [ -x /usr/bin/tput ] && tput setaf 1 >&/dev/null; then
        # We have color support; assume it's compliant with Ecma-48
        # (ISO/IEC-6429). (Lack of such support is extremely rare, and such
        # a case would tend to support setf rather than setaf.)
        color_prompt=yes
    else
        color_prompt=
    fi
fi

if [ "$color_prompt" = yes ]; then
PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]\$
'
else
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi
unset color_prompt force_color_prompt

# If this is an xterm set the title to user@host:dir
case "$TERM" in
xterm*|rxvt*)
    PS1="\[\e]0;${debian_chroot:+($debian_chroot)}\u@\h: \w\a\]$PS1"
    ;;
*)
    ;;
esac
```

```
# enable color support of ls and also add handy aliases
if [ -x /usr/bin/dircolors ]; then
    test -r ~/.dircolors && eval "$(dircolors -b ~/.dircolors)" || eval "$(dircolors -b)"
    alias ls='ls --color=auto'
    #alias dir='dir --color=auto'
    #alias vdir='vdir --color=auto'

    alias grep='grep --color=auto'
    alias fgrep='fgrep --color=auto'
    alias egrep='egrep --color=auto'
fi

# colored GCC warnings and errors
#export GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'

# some more ls aliases
alias ll='ls -alF'
alias la='ls -A'
alias l='ls -CF'

# Add an "alert" alias for long running commands.  Use like so:
#   sleep 10; alert
alias alert='notify-send --urgency=low -i "$([ $? = 0 ] && echo terminal || echo error)" "$(history|tail
-n1|sed -e '\''s/^\s*[0-9]\+\s*//;s/[;&|]\s*alert$//'\'')"'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi
[ -r /home/<USER>/.byobu/prompt ] && . /home/<USER>/.byobu/prompt   #byobu-prompt#

PATH="${PATH}:~/bin"

# SSH AGENT KEYCHAIN
eval $(keychain --eval id_rsa id_ed25519)

# gitprompt
. ~/repos/bash-git-prompt/gitprompt.sh

# alias for Python 3
alias "python"="python3"
```

From:
https://wiki.nanoscopic.de/ - **nanoscopic wiki**

Permanent link:
https://wiki.nanoscopic.de/doku.php/pages/howtos/ssh/stronger-ssh-key-and-keychain?rev=1612959784

Last update: **2021/02/10 12:23**