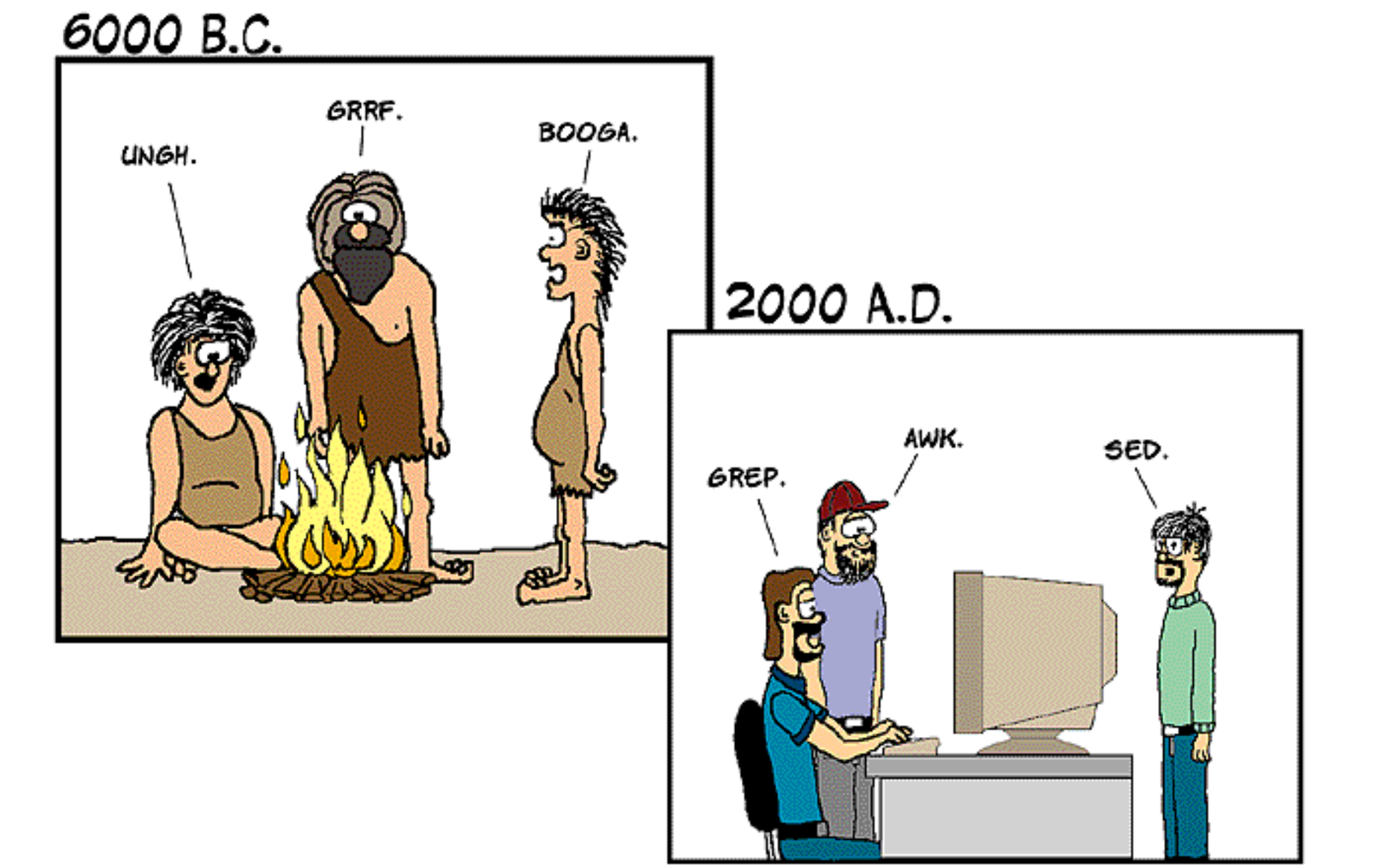
Tricks of the Trade

Hands-On UNIX System Administration DeCal

Week 7 — 7 March 2011

Last time



source: http://ars.userfriendly.org/cartoons/?id=19990815

Today

- Tips and tricks that'll make your life easier, whether you're a sysadmin or normal user. We won't go into detail about all of these, so you should experiment on your own.
- Final project ideas! We're halfway through the semester, so start brainstorming.

SSH key authentication

- A secure alternative to password-based authentication: uses **public/private key cryptography** to guarantee that you are who you say you are.
- Use an **SSH agent**, like Pageant (Windows) or ssh-agent (UNIX), to cache your SSH key and allow for passwordless logins.

SSH key authentication

- Use **ssh-keygen** to generate a keypair:
  `ssh-keygen -t rsa -b 4096`
- This will generate…
  - a private key, `~/.ssh/id_rsa`
  - a public key, `~/.ssh/id_rsa.pub`
- Public keys you want to accept are stored in `~/.ssh/authorized_keys`.

GNU screen

- First, a word about **TERM types**. They're set by your terminal emulator to indicate supported functionality, like colors.
- It's a shell variable — try `echo $TERM`. If you're on a system that doesn't recognize your TERM type, things will misbehave. Quick fix: `TERM=xterm; export TERM`.

GNU screen

- GNU screen is a **terminal multiplexor** (think "tabbed browsing") that can be **detached from** and **reattached to**.
- Suppose you're running a long backup job. You don't need to keep a terminal open for days — just run it in screen and detach/reattach at your convenience. (This also comes in handy on flaky wifi!)

GNU screen

- Start a new screen: `% screen`
- Create a new window: `^A ^C`, `^A c`
  switch between them: `^A ^A`, `^A a`
  view all open windows: `^A "`
- Detach from screen: `^A d`
- Reattach to screen: `% screen -r`

RCS

- Heard of Subversion, Git, Mercurial? These are **version control** tools — they keep track of, and can revert, changes to files.
- RCS is the original **Revision Control System**. It manages individual files (CVS was developed as a shell-script frontend to RCS) and is still used today to manage server configuration files.

RCS

- RCS doesn't require repositories, like Subversion. Instead, checking in `foobar` will create an **RCS file**, `foobar,v`, in the same directory (or, if it exists, in `RCS/`).
- Surprising behavior: `ci foobar` will check in `foobar`, and then delete it!

PGP/GnuPG

- **PGP** (Pretty Good Privacy) and **GnuPG** (GNU Privacy Guard, GPG) are two tools that use private/public key cryptography to digitally sign and encrypt data.
- After verifying someone's PGP fingerprint and adding it to your trusted keyring, you can verify signed messages from them and encrypt messages that only they can read.

Mutt

"All mail clients suck. This one just sucks less."

- Mutt is an email swiss-army knife — it can access and manipulate any mailstore you can think of (Maildir, mbox, IMAP, POP…).
- Uses `vi` keybindings, is lightning-fast, has awesome threading … it's the perfect mail client for power users and sysadmins.

netcat

- Netcat (nc) is a TCP/IP swiss-army knife.
- At its most basic, it can be used to connect to servers on arbitrary ports à la telnet, but it's fully automatable — one project group built a web server with bash and netcat.
- Everything you can do with stdin/stdout and pipes, netcat can do with networking.

openssl s_client

- Netcat doesn't have SSL support. Need to debug something? Use OpenSSL.
- Connect to a secured web server (HTTPS):

```
openssl s_client -connect \
secure.OCF.Berkeley.EDU:443
```

- And a STARTTLS-secured mail server:

```
openssl s_client -starttls smtp \
-connect mail.OCF.Berkeley.EDU:25
```

Makefiles

- A lazy sysadmin is a good sysadmin.
- Makefiles are a useful automation tool: they have a dependency system, and will report failure if any subcomponent fails.
- CSUA: a Makefile is used to automatically update configuration files, including a file containing SSH public keys for root staff.