# Traveling in time

# from past to future

# Time travel

- Ideally, a  Frankenstein-like experiment.
- Reconstruct sequences of past events.
- Correlate information from different sources.
- Time machine - a look into the future.

# who - active user snapshot

- Username.
- Terminal (or window).
- Start of session.
- Origin if remote (often truncated, easily masked).

```
% who
wietse     console      Jul 25 15:05    (:0)
wietse     pts/1        Jul 28 19:59    (beukel.porcupine.org)
wietse     pts/5        Jul 25 15:06
```

- Files: /etc/utmp, /var/run/utmp, /var/adm/utmp(x).
  Easy to forge, easy to unremove.

# last - past login activity

- Username.
- Terminal (or window).
- Session start/end/duration.
- Origin if remote (often truncated).
- Logout times scatter, making output hard to interpret.

```
% last
dbtpto    tty03    SVRC05           Thu Feb 21 12:48 - 12:52  (00:03)
tgtawb    tty02    SVRC05           Thu Feb 21 12:44   still logged in
rcsamw    :0                        Thu Feb 21 12:29 - 13:13  (00:44)
```

- Files: /var/adm/wtmp, /var/log/wtmp, /var/adm/wtmpx. Easy to forge, easy to unremove.

# lastlog - time of last login

- One entry per user, indexed by numerical userid.
- Terminal port.
- Time of login.
- Origin if remote (often truncated).

```
Last login: Wed Jul 28 19:59:56 1999 from beukel.porcupine
```

- Files: /var/adm/lastlog, /var/log/lastlog.
  Easy to forge, hard to unremove.

# Login/time correlations

- What users had access to the system around 13:15?

```
wmorrg    tty06    SVRC05             Wed Feb 20 12:58 - 13:24  (00:25)
rcbajvl   tty05    SVRC05             Wed Feb 20 12:30 - 13:34  (01:04)
bdbert    tty03    SVRC05             Wed Feb 20 12:26 - 13:27  (01:01)
rcstack   tty02    SVRC05             Wed Feb 20 12:19 - 13:44  (01:24)
rcmart    ttyp1    rwc.urc.tue.nl     Wed Feb 20 11:49 - 16:15  (04:25)
```

- What is the usage pattern of a specific account?

```
wsbsym@wsinfo01    ttyp8    rw8.urc.tue.nl    Mon Jun 15 15:33 - down   (00:27)
wsbsym@wsinpa01    ttyp2    wsinfo01          Mon Jun 15 14:14 - 14:24  (00:10)
wsbsym@wsinfo01    ttyp8    wsinfo01          Mon Jun 15 14:11 - 14:11  (00:00)
wsbsym@wsinfo01    ttyp2    rw8.urc.tue.nl    Mon Jun 15 13:58 - 14:24  (00:26)
```

# ps - process status snapshot

- Username.
- Terminal (or window).
- Start time.
- Memory and CPU usage.
- Command line (easily forged).
- Process status (running, sleeping, suspended, dead).
- Other utilities of interest: top, lsof (both freeware).
- Files: /vmunix, /dev/kmem, /proc

# lastcomm - past process activity

- Command (easy to forge).
- Status: abnormal exit, privilege change.
- Username.
- Terminal (or window).
- CPU usage.
- Start time + elapsed time (elapsed not shown).

```
w              wsingus  ttyp9      0.61 secs Mon Mar 11 13:46
ps             wsingus  ttyp9      0.33 secs Mon Mar 11 13:46
rn             wsingus  ttyp9      1.91 secs Mon Mar 11 13:44
w              wsingus  ttyp9      0.61 secs Mon Mar 11 13:44
rm             wsingus  ttyp9      0.06 secs Mon Mar 11 13:44
```

- File: /var/adm/pacct, /var/account/acct, /var/log/pacct.
- Easy to forge records.

# Process/time correlations

- All commands executed by a specific user.
- All commands within a specific login session.
- Successive instances of a (resident) process.
- (Sequences of) specific commands by any user.
- All processes running during some time window.
- Resident process started long after boot time.

# tcp wrapper - network connections

- Date and time.
- Target host.
- Network process name and ID.
- Client host (optional: client user).
- Relies on connection information supplied by client.

```
May 20 01:04:42 tuegate: 14498 systatd: connect from litp.ibp.fr
May 20 01:10:19 tuegate: 14536 systatd: connect from monk.rutgers.edu
May 20 01:23:49 tuegate: 15040 systatd: connect from monk.rutgers.edu

May 20 12:37:55 tuegate: 26546 systatd: connect from litp.ibp.fr
May 20 13:02:45 tuegate: 27048 systatd: connect from litp.ibp.fr
May 20 14:04:51 tuegate: 27668 systatd: connect from litp.ibp.fr
May 20 14:08:53 tuewsd in.fingerd[7075]: connect from litp.ibp.fr

.
```

# tcp wrapper/time correlations

- All connections from a specific site.
- All connections for specific services, for example finger and systat.
- Sequences of specific connections from any site, for example, finger followed by login attempt.
- All  connections made in a specific time window.

# File m/a/c times

- Significant amount of information: with 10^5 files on a typical single-user UNIX box, 10 MBytes of data.
- If available, as easy to read as footsteps in fresh snow. Example: compiling a "hello world" program.

```
Jul 30 99 18:45:45    3743 .a. -rw-r--r-- root     wheel    /etc/make.conf
                      4347 .a. -r--r--r-- bin      bin      /usr/include/machine/ansi.h
                      3911 .a. -r--r--r-- bin      bin      /usr/include/machine/endian.h
                      2697 .a. -r--r--r-- bin      bin      /usr/include/machine/types.h
                     13063 .a. -r--r--r-- bin      bin      /usr/include/stdio.h
                      5704 .a. -r--r--r-- bin      bin      /usr/include/sys/cdefs.h
                      5903 .a. -r--r--r-- bin      bin      /usr/include/sys/types.h
                       512 .a. drwxr-xr-x bin      bin      /usr/share/mk
                      3528 .a. -r--r--r-- bin      bin      /usr/share/mk/bsd.own.mk
                      3945 .a. -r--r--r-- bin      bin      /usr/share/mk/sys.mk
Jul 30 99 18:45:46    1949 .a. -r--r--r-- bin      bin      /usr/lib/crt0.o
                     22544 .a. -r--r--r-- bin      bin      /usr/lib/libgcc.a
```

m = content modified          a = read/execute access          c = status change (permission, owner, reference count, etc.)

# Time machine

- Correlating by time-aligning data from different sources.
- It slices and dices time into frames.
- Unification of data gathering tools.
- And you thought that SATAN+Netscape was a pig...
- Guaranteed to be Year 2000 compliant.