Introduction to Linux System Logging (with rsyslogd)

Andre M. Maier
Elektronikschule Tettnang

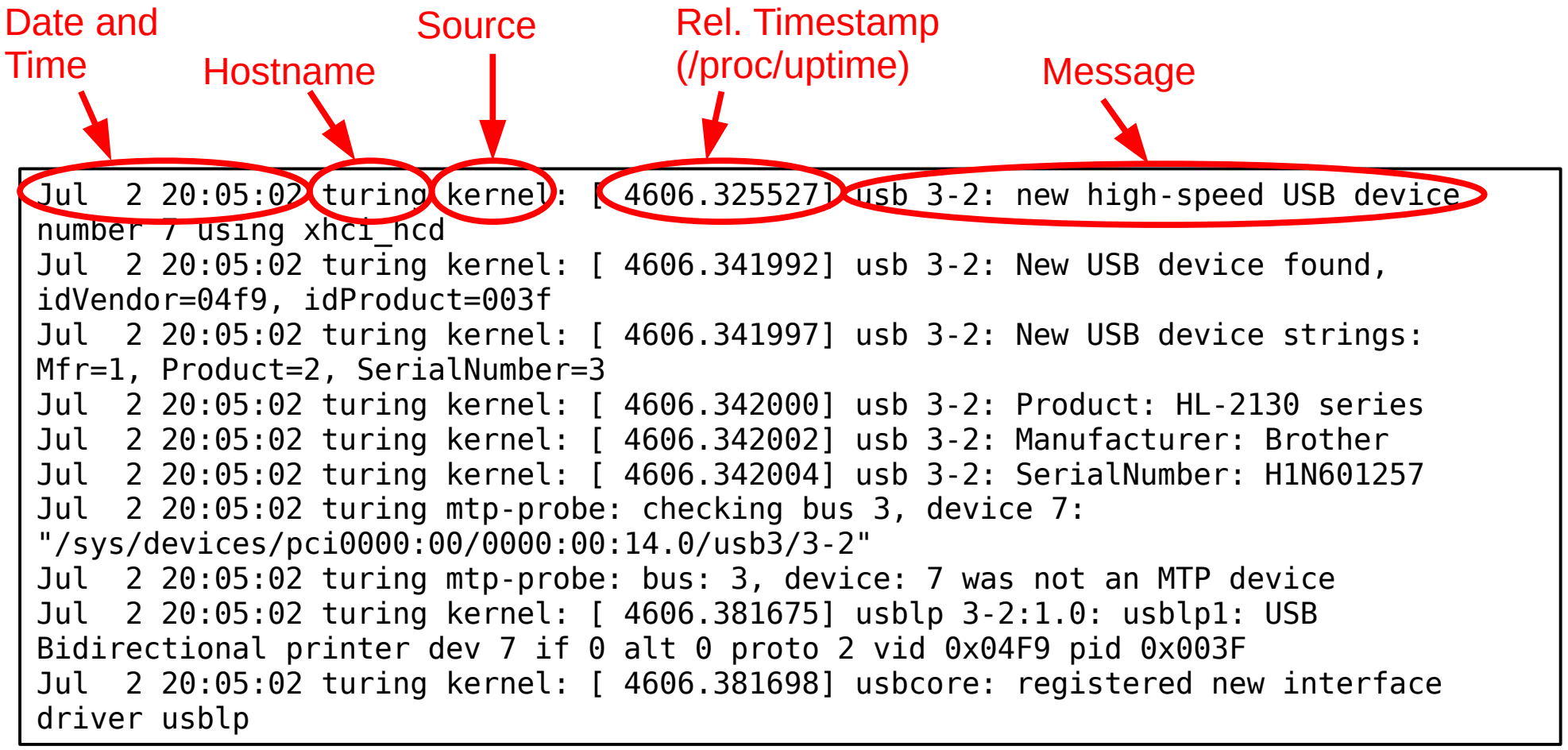
andre.maier@elektronikschule.de

Why is logging important?

- Debugging
- System Security
- Quality Management

Warning!
Experienced hackers are interested in gaining access to system logs, so all logfiles are subject to protection!

What information does a logfile contain?



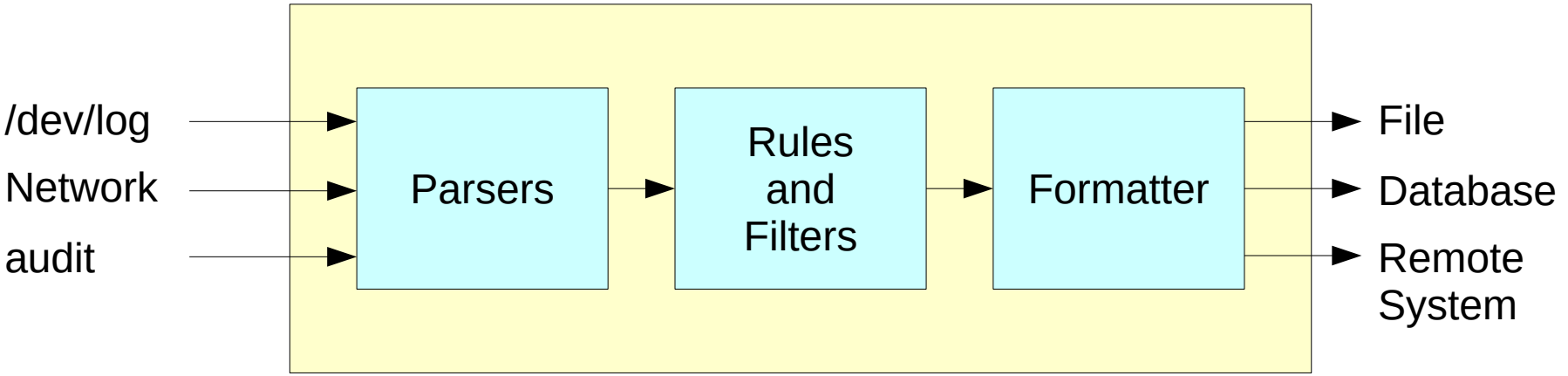
Logfiles

- /var/log
  - contains all kinds of logfiles
  - should be located on a separate partition
- Logfile names may vary between distributions.
- Example (Ubuntu):

auth.log	System authentication (e.g. sudo, login, ...)
boot.log	Booting process
dmesg	Kernel ringbuffer
dpkg.log	Package management
kern.log	Kernel messages
syslog	Global system messages (including information from other logfiles)

(r)syslogd

- is the demon responsible for logging
- offers a large number of features



Configuring (r)syslogd

- Configuration files
  - /etc/rsyslog.conf
  - files in /etc/rsyslog.d
- Example (excerpt):

```
kern.*                  /var/log/kern.log
kern.crit               @192.168.178.24
kern.crit               /dev/console
kern.info               /var/log/kernelinfo.log
```

Facilities, Priorities, and Actions

- Facilities
  - auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, security, syslog, user, uucp, local0 ... local7
  - Asterisk (*) refers to all facilities
- Priorities
  - debug, info, notice, warning, err, crit, alert, emerg
  - error, warn, and panic are deprecated
  - Asterisk (*) refers to all priorities
- Actions
  - Most commonly, the action is a filename in /var/log
  - Asterisk (*) means all logged-in users

Generating Logs from bash

- logger command

  Example: `logger "Hi there!"`

```
NAME
     logger – a shell command interface to the syslog(3) system log
              module

SYNOPSIS
     logger [-dhisV] [-f file] [-n server] [-P port] [-p pri]
            [-t tag] [-u socket] [message]

DESCRIPTION
     logger makes entries in the system log.  It provides a shell
     command interface to the syslog(3) system log module.
```

Generating Logs in C

- Example:

```
#include <syslog.h>

int main( int argc, char** argv )
{
   setlogmask( LOG_UPTO( LOG_NOTICE ));
   openlog( "demoprog", LOG_CONS | LOG_PID |
                        LOG_NDELAY, LOG_LOCAL1 );
   syslog( LOG_NOTICE, "Program started by user %d",
           getuid() );
   syslog( LOG_INFO, "Hi there!" );
   closelog();
   return 0;
}
```

logrotate

- is a tool designed to simplify the administration of log files
- allows to rotate, compress, mail, ... logfiles
- is usually run automatically (cronjob) on a daily basis
- Configuration files
  - /etc/logrotate.conf
  - files in /etc/logrotate.d