auditdistd

secure and reliable distribution of audit trail files

Paweł Jakub Dawidek
<pjd@FreeBSD.org>

audit

logs security-relevant events

does not protect

alternatives?

ktrace

dtrace

accounting

syslog

audit

detailed

event: execve(2)
time: 2012.05.01 12:37:43 862ms
path: /usr/sbin/pwd_mkdb
args: -p -d /etc -u pjd /etc/pw.7E8H1a
executable mode: 0555
executable uid: root
executable gid: wheel
fsid, nodeid, device
subject:
audit-uid: pjd
uid: root
gid: staff
ruid: pjd
rgid: staff
return: success

low overhead

reliability

predicatble loss

configurable

trustworthy(?)

audit

- security-relevant events
- detailed information
- low overhead
- reliability
- predictable loss
- configurable
- trustworthy(?)

ktrace, dtrace, accounting, syslog

- security-relevant events
- detailed information
- low overhead
- reliability
- predictable loss
- configurable
- trustworthy(?)

usefullness

postmortem analysis

intrusion detection via auditpipe

configuration

/etc/security/

audit record format

header	*<token>*	*...*	*<token>*	subject	return	trailer

audit

- security-relevant events
- detailed information
- low overhead
- reliability
- predictable loss
- configurable
- trustworth(?)

trustworthy (?)

hack in

rm -f /var/audit/*

cat betterlog > /var/audit/current

enter auditdistd

FreeBSD Foundation

sends audit trail files

to another machine

how hard can it be?

secure

reliable

low latency

the curse

sender

receiver

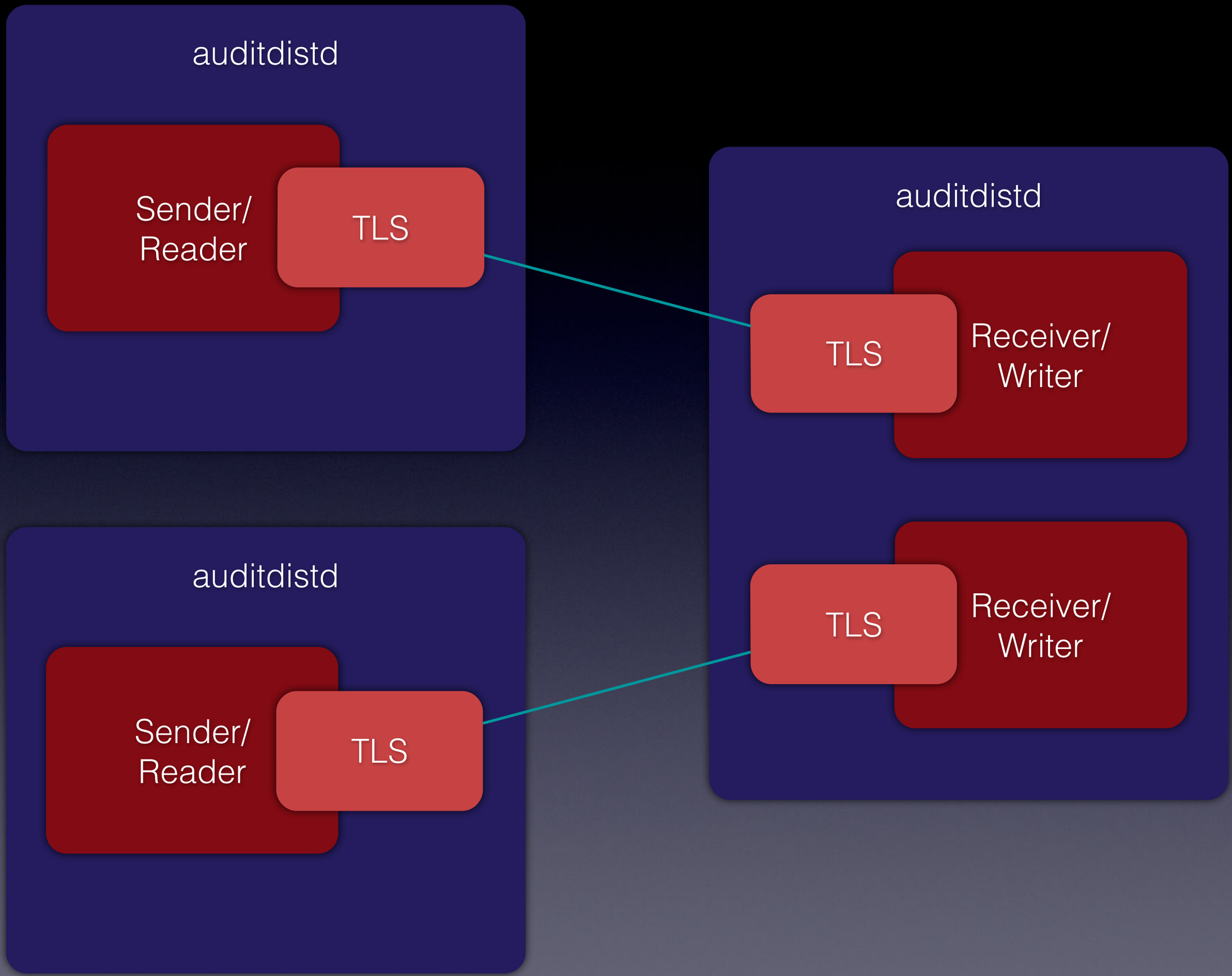
auditd: create /var/audit/<date>.not_terminated

auditd: link /var/audit/<date>.not_terminated /var/audit/dist/<date>.not_terminated

auditd: rename /var/audit/<date>.not_terminated /var/audit/<date>.<date>

auditd: rename /var/audit/dist/<date>.not_terminated /var/audit/dist/<date>.<date>

auditdistd: unlink /var/audit/dist/<date>.<date>

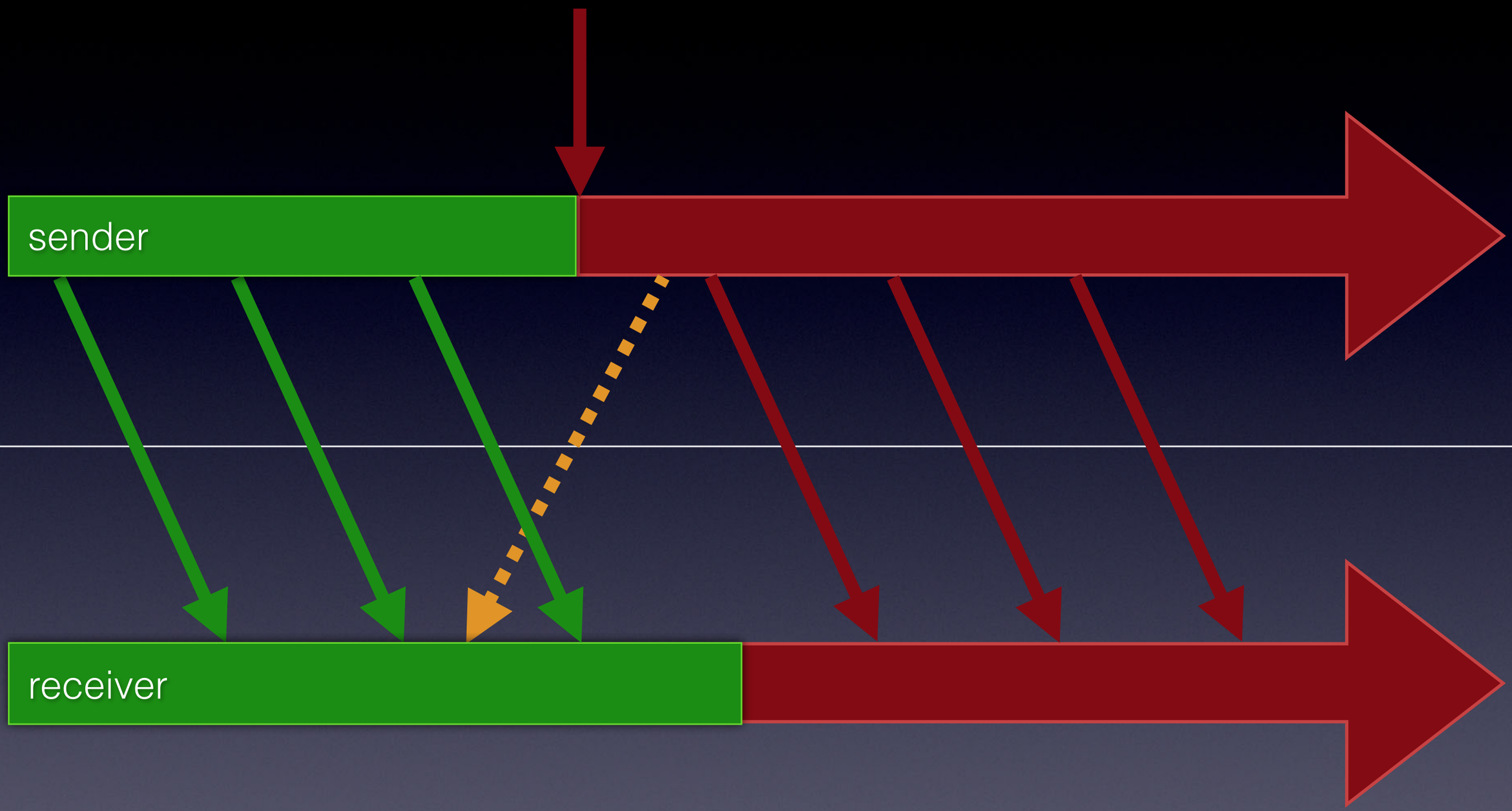

auditdistd
Sender/
Reader
TLS
auditdistd
TLS
Receiver/
Writer
auditdistd
Sender/
Reader
TLS
auditdistd
TLS
Receiver/
Writer

jail (chroot)

setgroups+setgid+setuid

capsicum

assertions


sender
receiver

```
sender {
   host "receiver" {
      remote "tls://10.0.0.1"
      fingerprint "SHA256=8F:0A:FC:8A:3D:09:80:AF:D9:AA:38:CC:..."
      password "YjwbK69H5cEBlhcT+eJpJgJTFn5B2SrG"
   }
}
```

```
receiver {
   host "foo" {
      remote "tls://10.0.0.2"
      password "YjwbK69H5cEBlhcT+eJpJgJTFn5B2SrG"
   }
   host "bar" {
      remote "tls://10.0.0.3"
      password "CG1qbqocOmAFOeWSWidMlvtLa5TWu6li"
   }
}
```