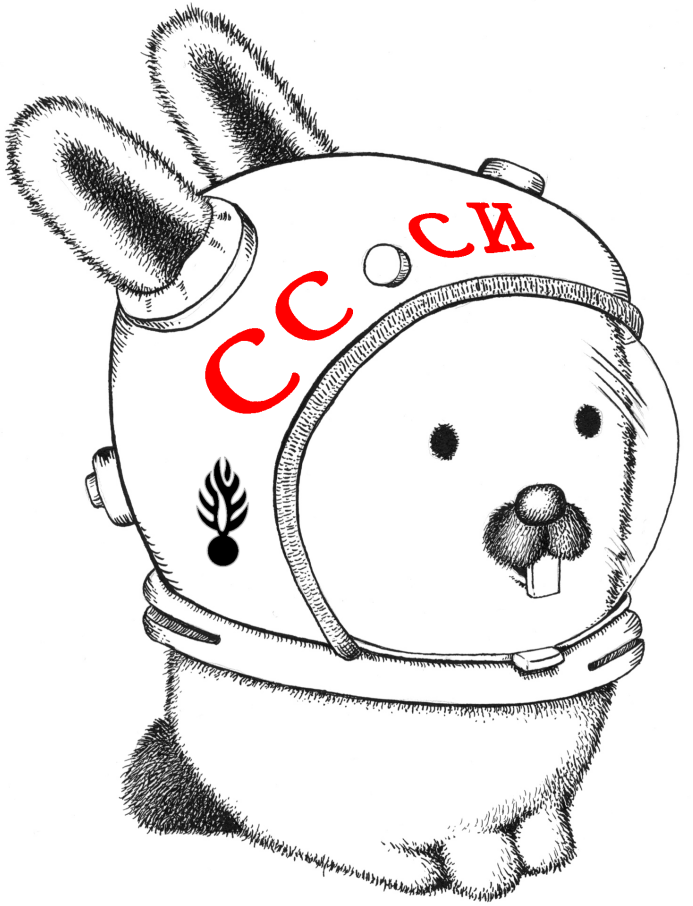
Dr Glendarme, etc.

2023-04-21 9^{th} IWP9

Edouard Klein

Porting Plan 9's security model to Linux



Thanks

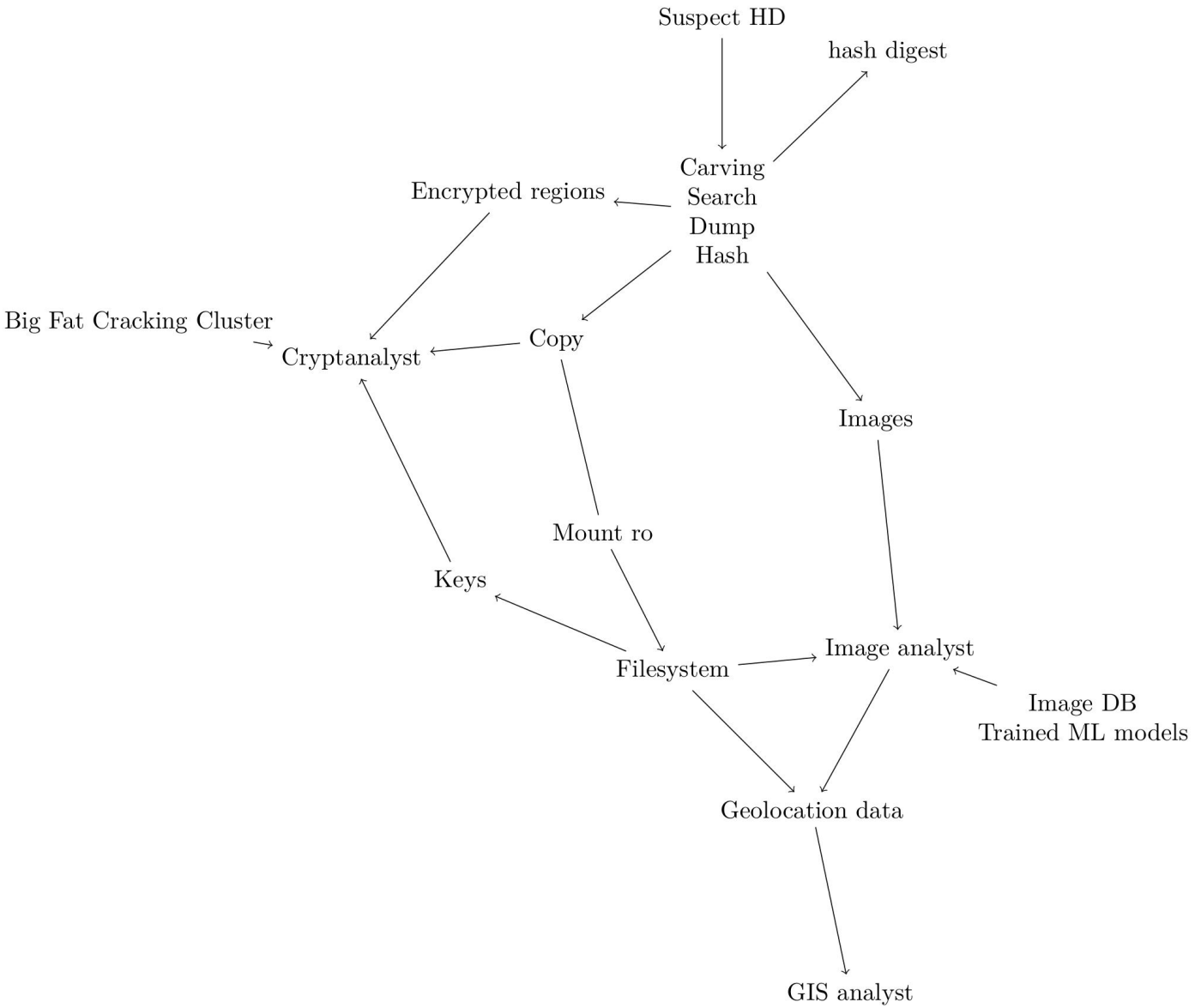
Context

French National Computer Crime Unit, 2019

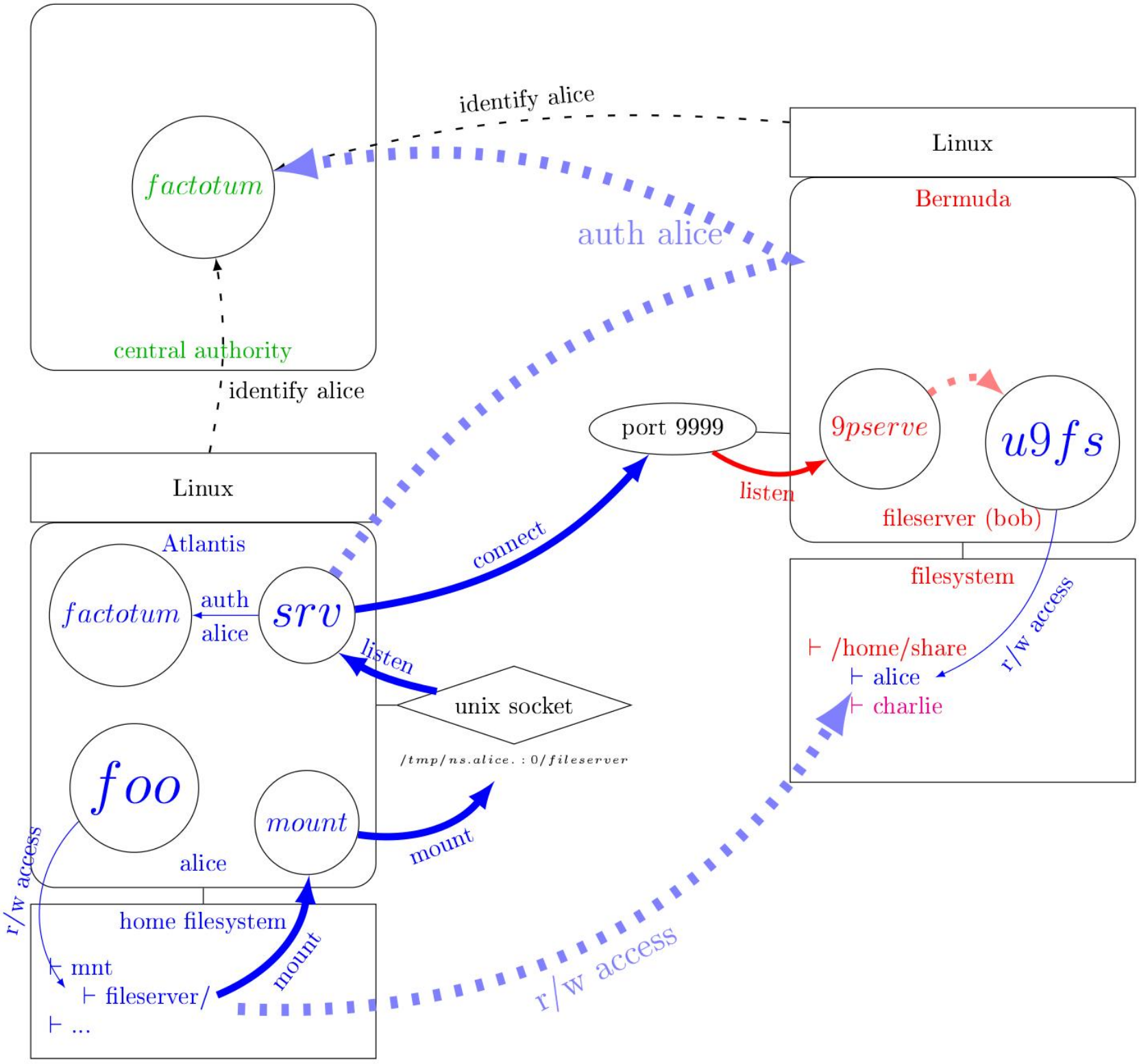
C3N

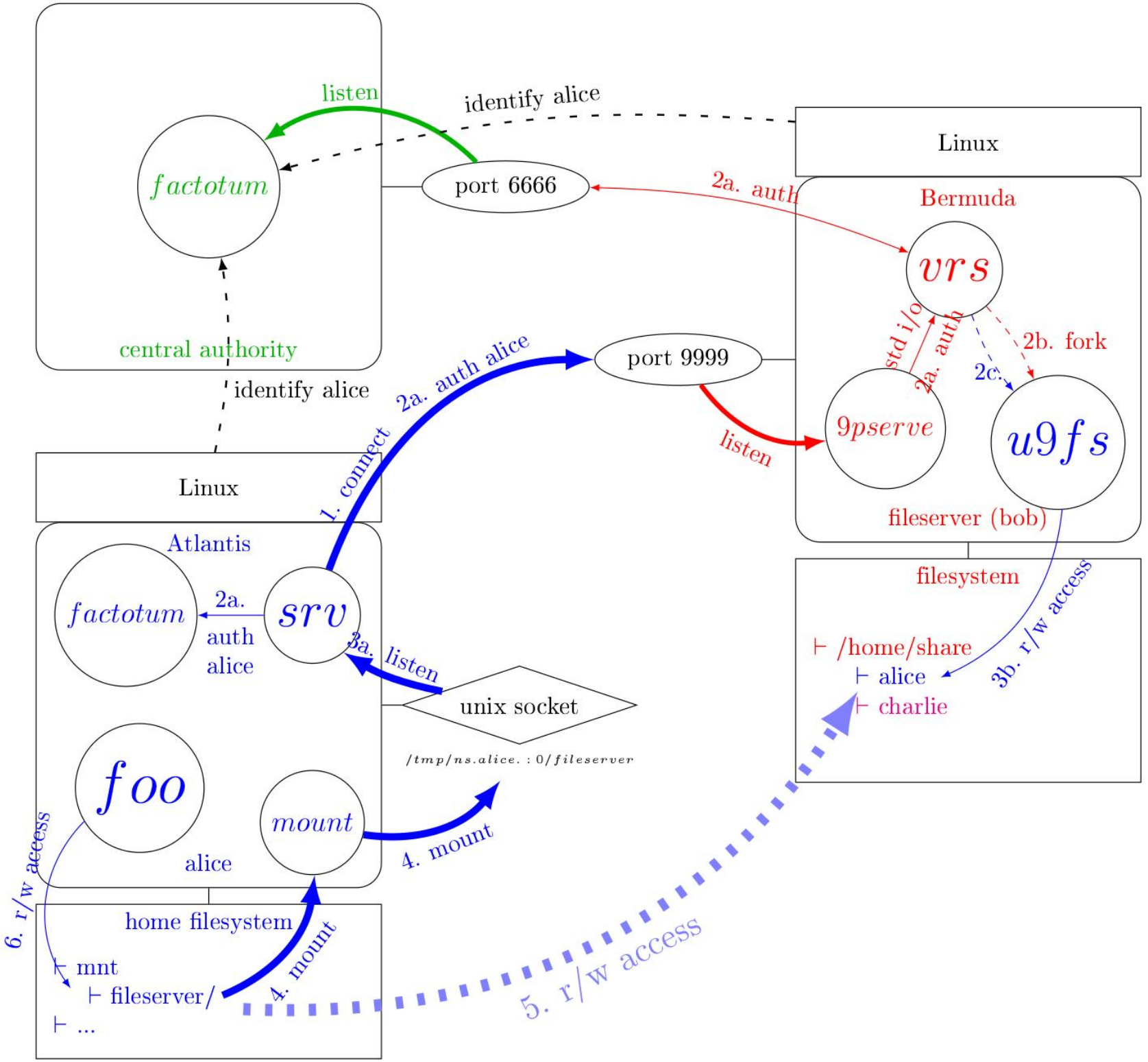
ССCИ

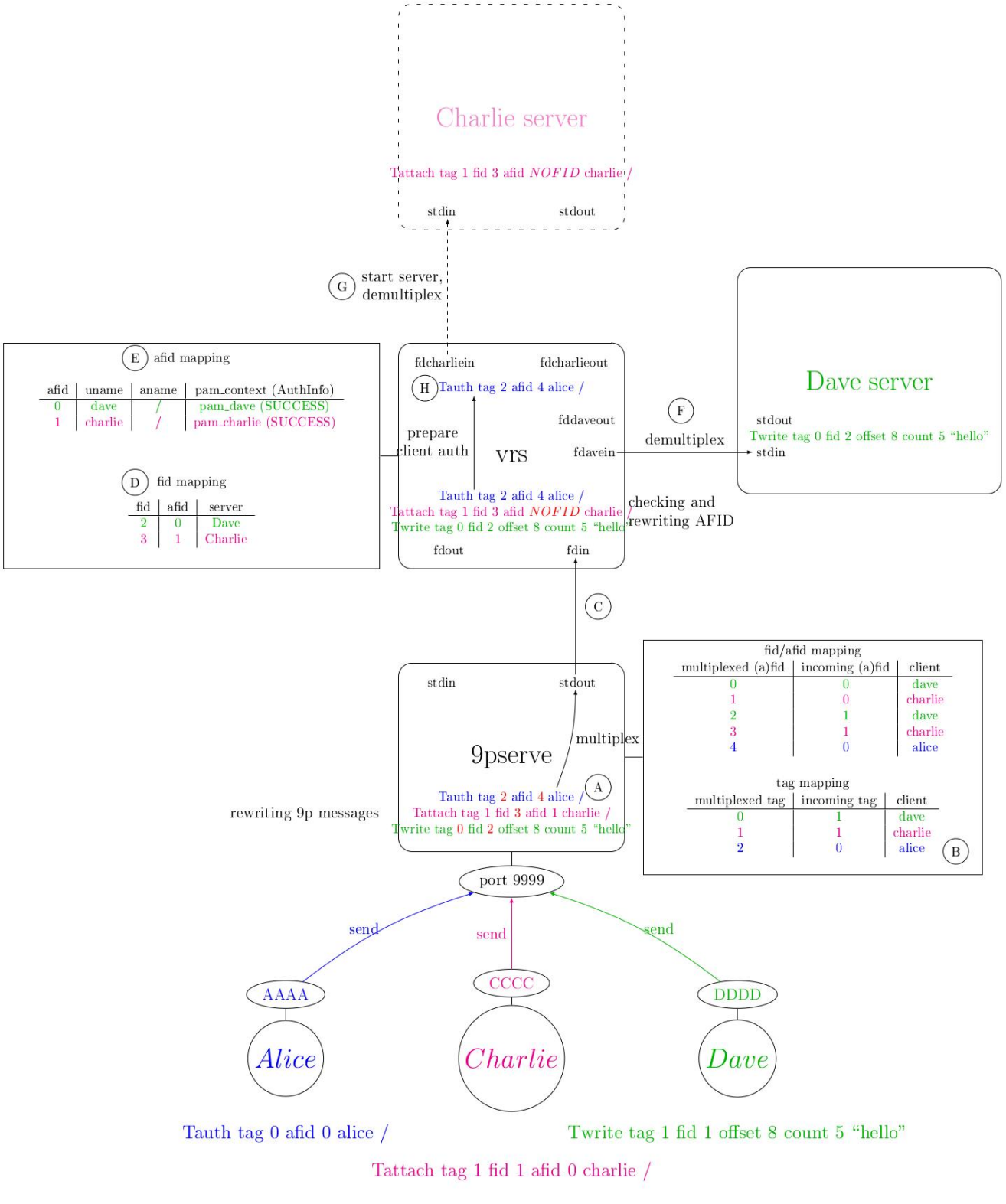
Example workload

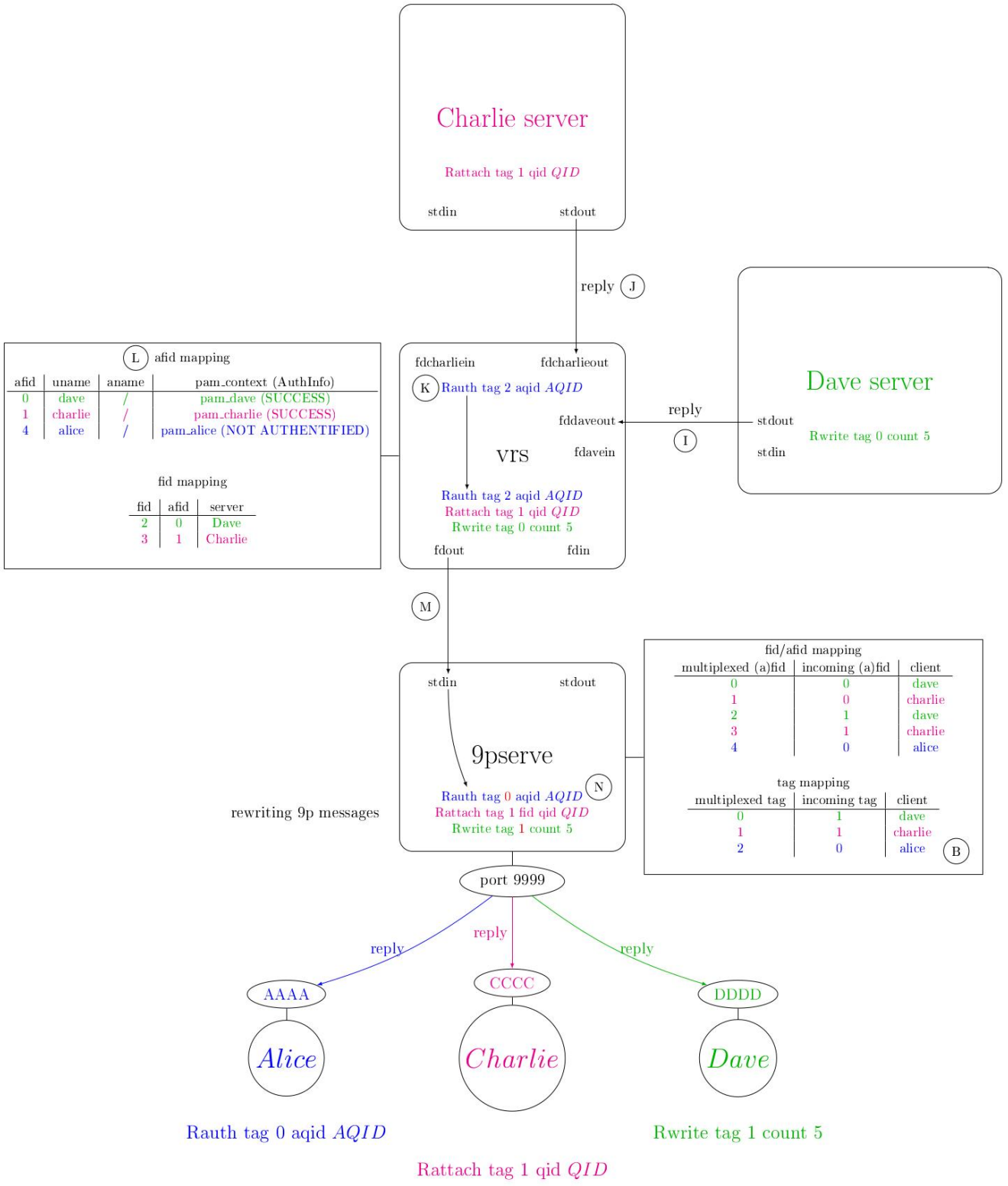


PAYLOAD


factotum
central authority
identify alice
identify alice
Linux
Bermuda
auth alice
port 9999
9pserve
u9fs
listen
fileserver (bob)
Linux
Atlantis
factotum
auth
alice
srv
connect
listen
unix socket
/tmp/ns.alice.:0/fileserver
filesystem
⊢ /home/share
⊢ alice
⊢ charlie
r/w access
foo
alice
mount
mount
r/w access
home filesystem
⊢ mnt
⊢ fileserver/
⊢ ...
mount
r/w access


listen
identify alice
factotum
port 6666
Linux
2a. auth
Bermuda
vrs
std i/o
2a. auth
2b. fork
2c.
central authority
identify alice
port 9999
2a. auth alice
1. connect
listen
9pserve
u9fs
Linux
fileserver (bob)
Atlantis
filesystem
factotum
2a.
auth
alice
srv
3a. listen
3b. r/w access
/home/share
alice
charlie
unix socket
/tmp/ns.alice.:0/fileserver
foo
mount
4. mount
alice
6. r/w aceess
home filesystem
mnt
fileserver/
...
4. mount
5. r/w access


Charlie server
Tattach tag 1 fid 3 afid NOFID charlie /
stdin
stdout
G start server, demultiplex
E afid mapping
afid | uname | aname | pam_context (AuthInfo)
0 | dave | / | pam_dave (SUCCESS)
1 | charlie | / | pam_charlie (SUCCESS)
D fid mapping
fid | afid | server
2 | 0 | Dave
3 | 1 | Charlie
fdcharliein
fdcharlieout
H Tauth tag 2 afid 4 alice /
prepare client auth
vrs
fddaveout
fdavein
Tauth tag 2 afid 4 alice /
Tattach tag 1 fid 3 afid NOFID charlie /
Twrite tag 0 fid 2 offset 8 count 5 "hello"
fdout
fdin
F demultiplex
checking and rewriting AFID
Dave server
stdout
Twrite tag 0 fid 2 offset 8 count 5 "hello"
stdin
C
fid/afid mapping
multiplexed (a)fid | incoming (a)fid | client
0 | 0 | dave
1 | 0 | charlie
2 | 1 | dave
3 | 1 | charlie
4 | 0 | alice
tag mapping
multiplexed tag | incoming tag | client
0 | 1 | dave
1 | 1 | charlie
2 | 0 | alice
B
stdin
stdout
multiplex
9pserve
A
Tauth tag 2 afid 4 alice /
Tattach tag 1 fid 3 afid 1 charlie /
Twrite tag 0 fid 2 offset 8 count 5 "hello"
rewriting 9p messages
port 9999
send
send
send
AAAA
CCCC
DDDD
Alice
Charlie
Dave
Tauth tag 0 afid 0 alice /
Twrite tag 1 fid 1 offset 8 count 5 "hello"
Tattach tag 1 fid 1 afid 0 charlie /


Charlie server
Rattach tag 1 qid QID
stdin
stdout
reply J
Dave server
Rwrite tag 0 count 5
stdout
stdin
reply
I
L afid mapping
afid | uname | aname | pam_context (AuthInfo)
0 | dave | / | pam_dave (SUCCESS)
1 | charlie | / | pam_charlie (SUCCESS)
4 | alice | / | pam_alice (NOT AUTHENTIFIED)
fid mapping
fid | afid | server
2 | 0 | Dave
3 | 1 | Charlie
fdcharliein
fdcharlieout
K Rauth tag 2 aqid AQID
fddaveout
fdavein
VFS
Rauth tag 2 aqid AQID
Rattach tag 1 qid QID
Rwrite tag 0 count 5
fdout
fdin
M
stdin
stdout
9pserve
N
Rauth tag 0 aqid AQID
Rattach tag 1 fid qid QID
Rwrite tag 1 count 5
rewriting 9p messages
fid/afid mapping
multiplexed (a)fid | incoming (a)fid | client
0 | 0 | dave
1 | 0 | charlie
2 | 1 | dave
3 | 1 | charlie
4 | 0 | alice
tag mapping
multiplexed tag | incoming tag | client
0 | 1 | dave
1 | 1 | charlie
2 | 0 | alice
B
port 9999
reply
reply
reply
AAAA
CCCC
DDDD
Alice
Charlie
Dave
Rauth tag 0 aqid AQID
Rwrite tag 1 count 5
Rattach tag 1 qid QID

Transport security

(a)fid == capability

$\Rightarrow$ stunnel

USAGE

Moving parts

vrs

PAM

Factotum

NSS

Usage

Last seen working...

`gitlab.com/edouardklein/vrs`

...on a stable debian circa 2020

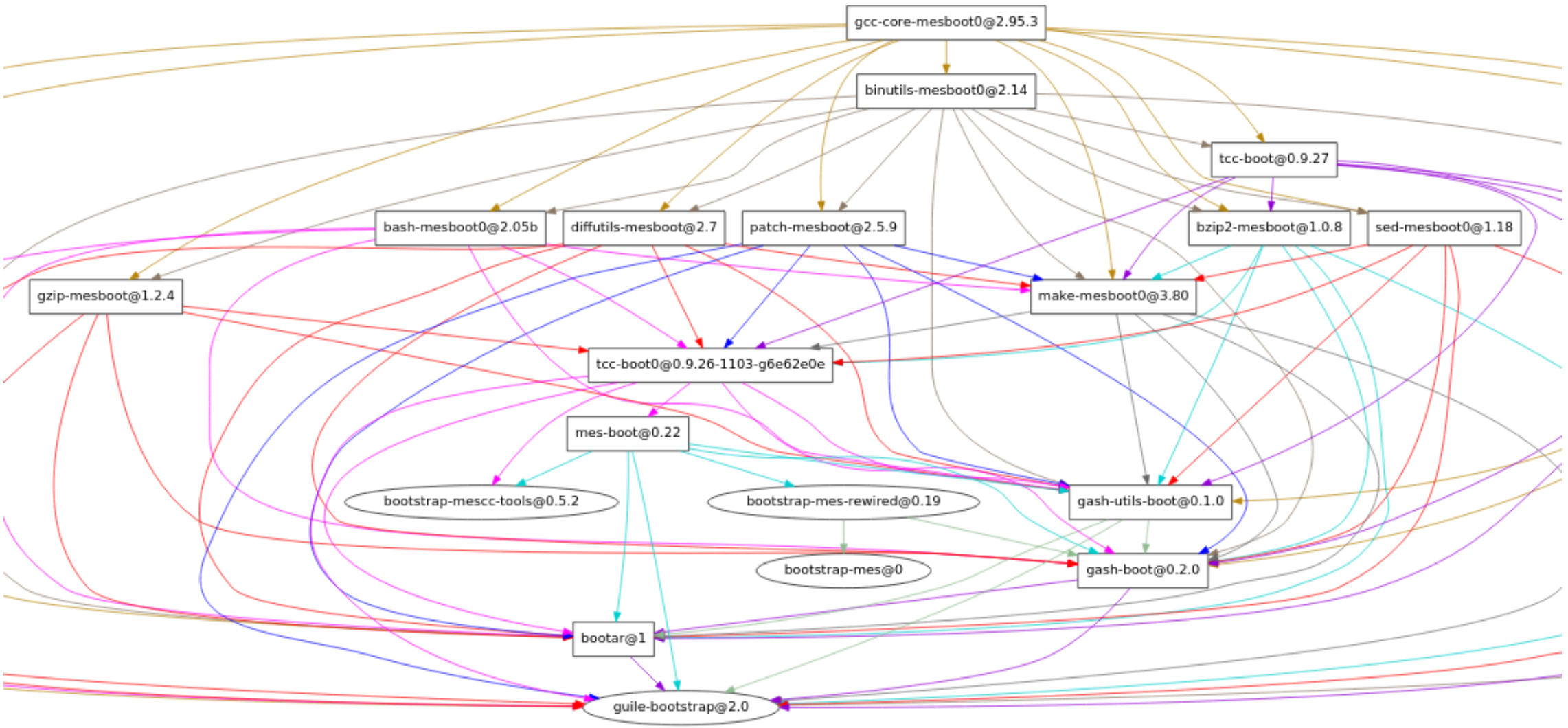
Current efforts

A tale of two communities

Guix

```
EMACS(1)

NAME
     emacs - editor macros

SYNOPSIS
     emacs [ options ]

DESCRIPTION
     This page intentionally left blank.

SOURCE
     MIT

SEE ALSO
     sam(1), vi(1)

BUGS
     Yes.
```

Remember Trusting Trust ?



This is good for software quality

xz needs gcc needs sed needs xz

(GNU) coreutils from 2011 to 2020

(GNU) sed from 1.18 (1993) to 4.8 (2020)

Their aim: reproducible science
(Also, I switched jobs in 2020)

Why am I telling you this?

(Also, we got better hardware)

C3N aim: reproducible forensics

Join us

ssh <you>@the-dam.org

https://goforintegrity.org

Charity