Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Even more Isabelle and Firewalls

NetSec

Cornelius Diekmann

8th September 2016

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit        ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip      ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit        ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip      ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit        ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip      ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit        ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip      ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

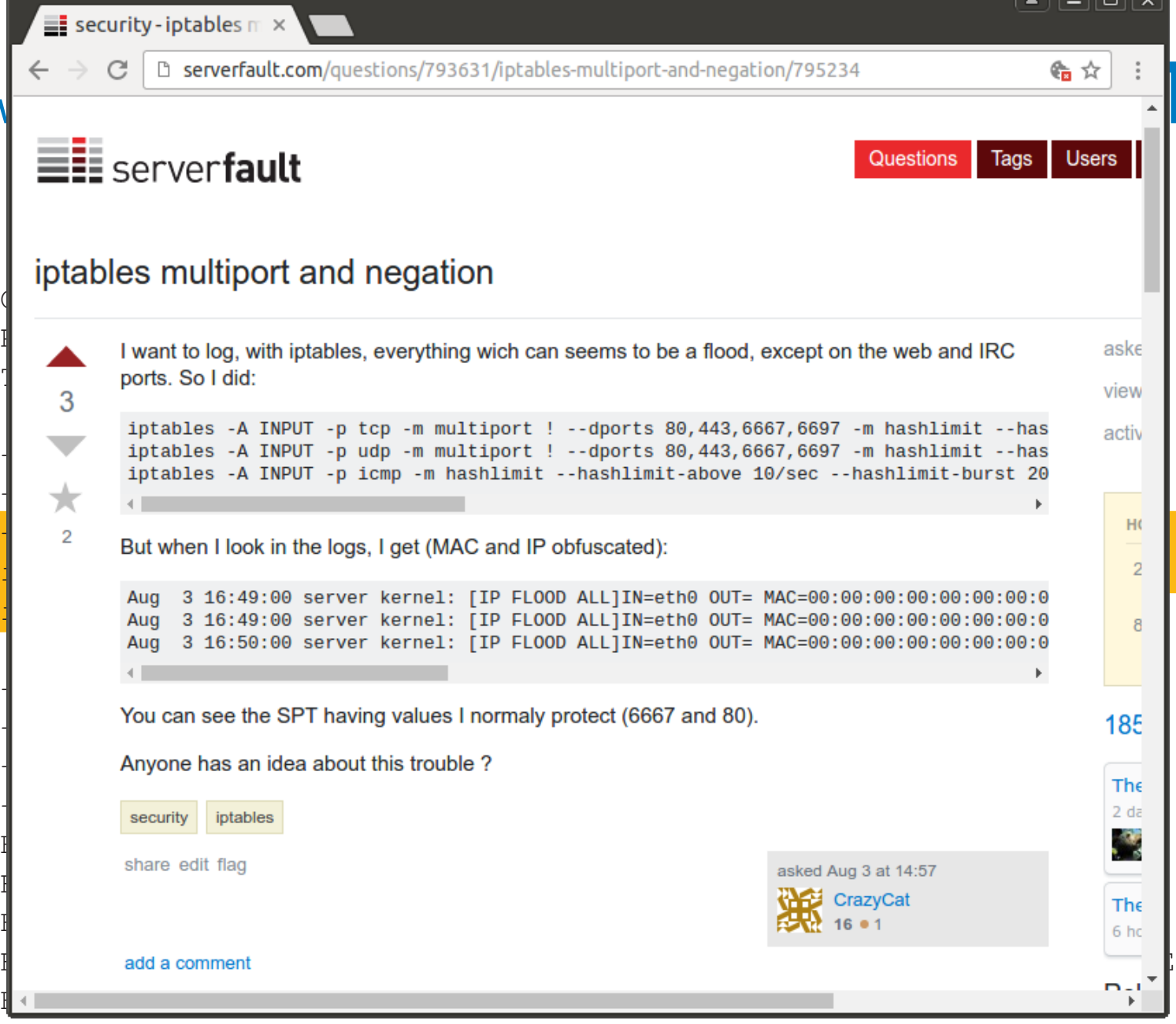
```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall


```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multipo  dpor  ,6697 -m hashlimit       ↩
    --hashlimit-above 10/sec  limi  hashlimit-mode srcip     ↩
    --hashlimit-name aflood  imit-  j LOG
-A FORWARD ! -i lo -s 127.0  -j DR
-A FORWARD -i internal -s 13  21.0
-A FORWARD -s 131.159.15.240  -d 131  21  j DROP
-A FORWARD -p tcp -d 131.159.15.240/2  C
-A FORWARD -i  -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firev

```
*filter
:INPUT DROP
:FORWARD DRO
:OUTPUT DROP
:DOS_PROTECT
:GOOD~STUFF
-A FORWARD -
-A FORWARD -
-A FORWARD -
    --hashli
    --hashli
-A FORWARD
-A FORWARD -
-A FORWARD -
-A FORWARD -
-A FORWARD -
-A GOOD~STUF
-A GOOD~STUF
-A GOOD~STUF
-A DOS_PROTE                                    TURN
-A DOS_PROTE
COMMIT
```



Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit        ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip      ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit        ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip      ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

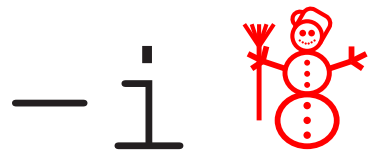
```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit        ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip      ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i  -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i  -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

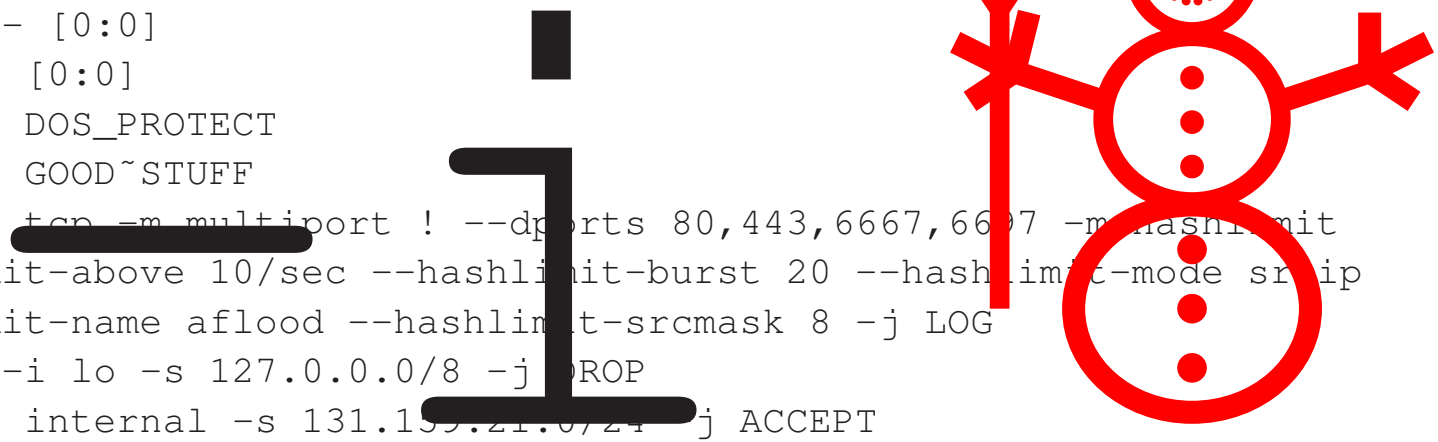


Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit       ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip     ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i ☃ -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

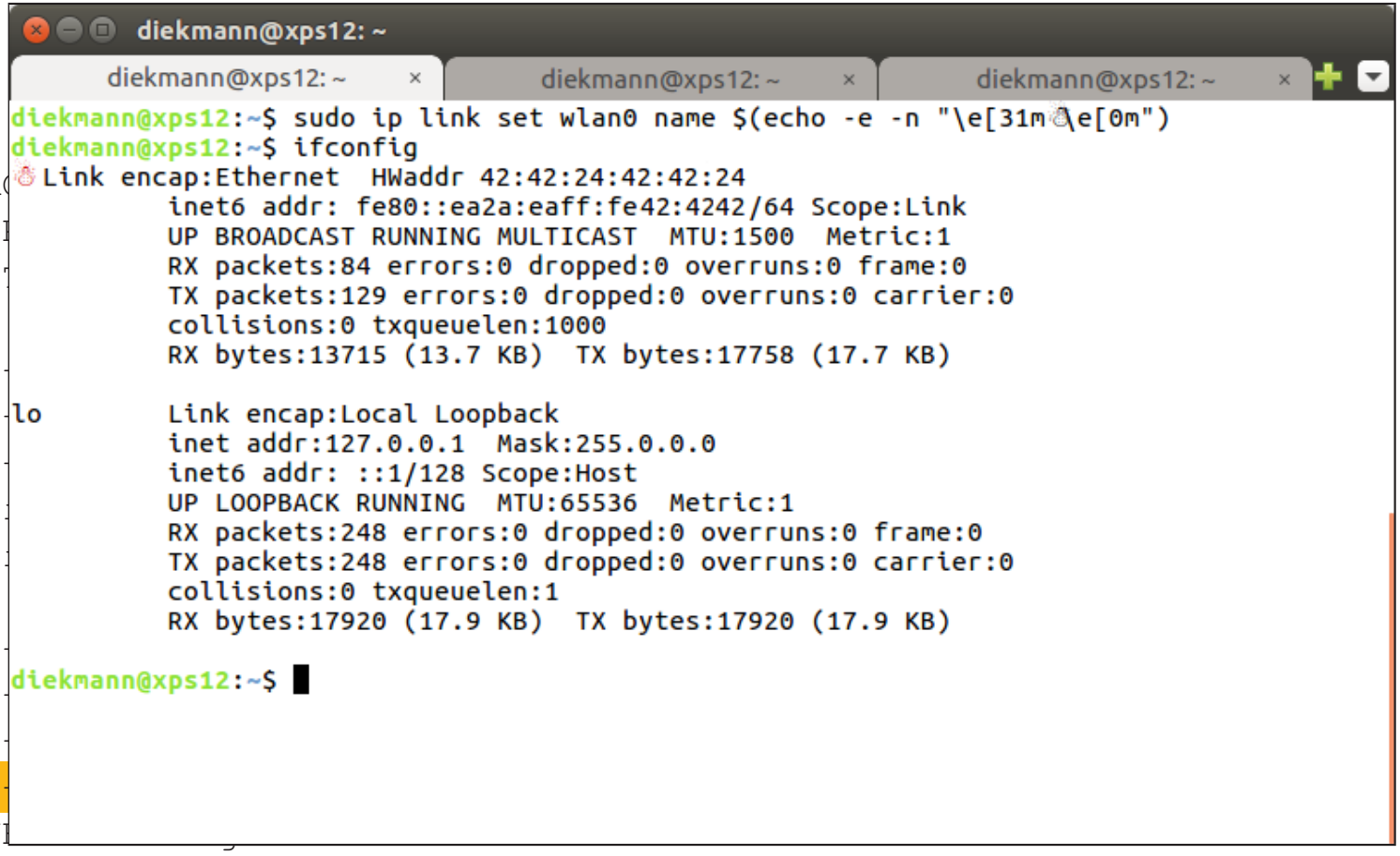
Linux Firewall

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit ↩
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip ↩
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [redacted] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

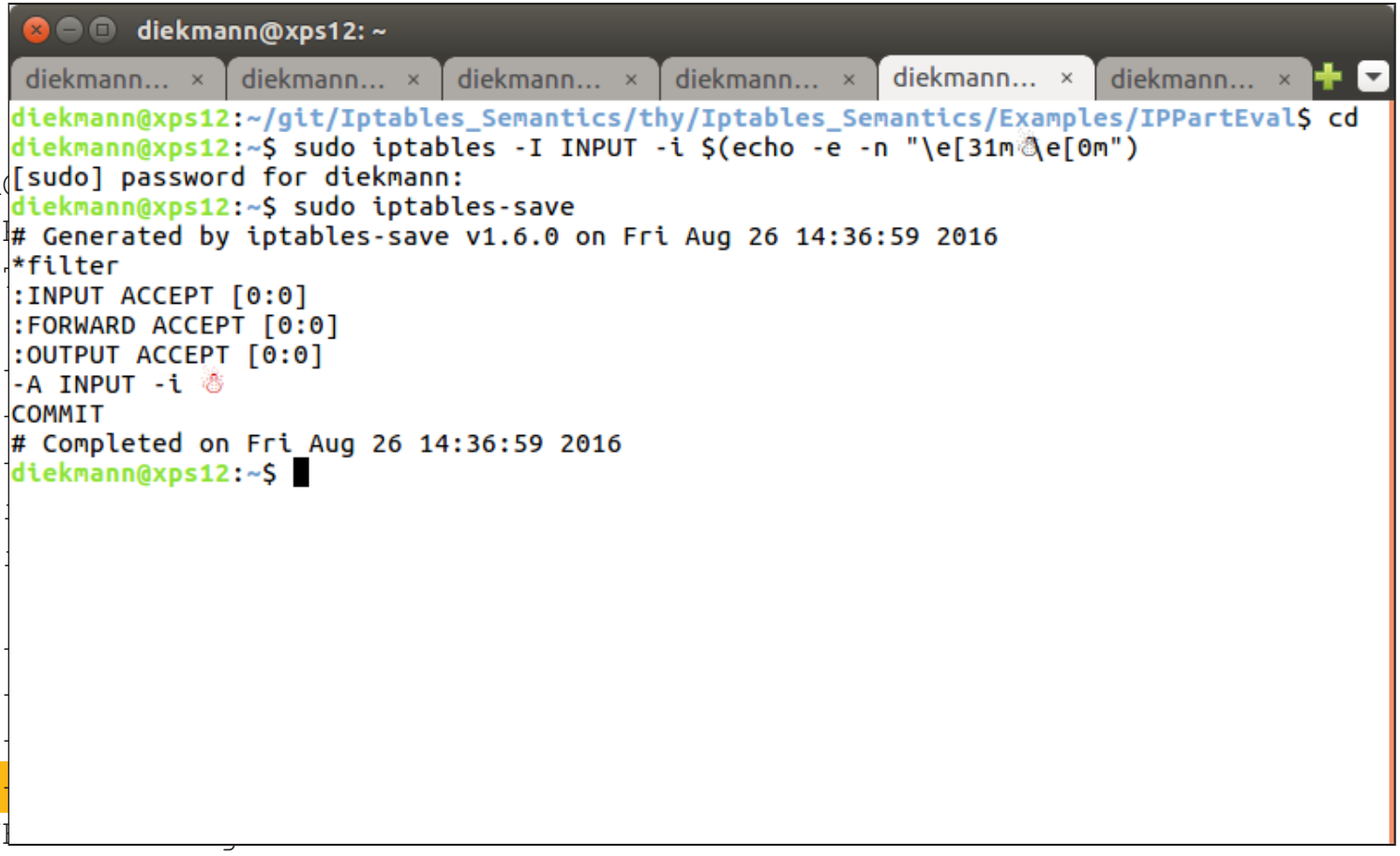


Linux Firewall

```
*filter
:INPUT DROP
:FORWARD DRO
:OUTPUT DROP
:DOS_PROTECT
:GOOD~STUFF
-A FORWARD -
-A FORWARD -
-A FORWARD -
    --hashl
    --hashl
-A FORWARD
-A FORWARD -
-A FORWARD -
-A FORWARD -
-A FORWARD -
-A GOOD~STU
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```



Linux Firewall




```
*filter
:INPUT DROP
:FORWARD DR
:OUTPUT DRO
:DOS_PROTEC
:GOOD~STUFF
-A FORWARD
-A FORWARD
-A FORWARD
    --hashl
    --hashl
-A FORWARD
-A FORWARD
-A FORWARD
-A FORWARD
-A FORWARD
-A GOOD~STU
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

```
*filter
:INPUT DROP
:FORWARD DRO
:OUTPUT DROP
:DOS_PROTECT
:GOOD~STUFF
-A FORWARD -
-A FORWARD -
-A FORWARD -
    --hashli
    --hashli
-A FORWARD
-A FORWARD -
-A FORWARD -
-A FORWARD -
-A FORWARD -
-A GOOD~STUF
-A GOOD~STUF
-A GOOD~STUF
-A DOS_PROTI
-A DOS_PROTI
COMMIT
```

serverfault

Questions Tags Use

Match an interface named “+” in iptables

0

1

Just for fun, I renamed my primary network interface of my laptop from `wlan0` to `+`:

```
ip link set wlan0 name +
```

The tools `ifconfig` and `ip` confirm that this works.

Question: How can I match incoming traffic from and only from my interface `+` with `iptables`?

Now the fun part: iptables treats `+` at the end of an interface match expression as wildcard. Consequently, `iptables -I INPUT -i +` matches every packet.

A glimpse at the kernel and iptables userland source code hints that interface matching is done with a bitmask, set up by the userland tool `iptables`. The kernel should be able to do a normal string equality check on any interface name, given the bitmask is set up accordingly. But I don't see a possibility to tell the `iptables` userland command that I don't want to consider `+` as a wildcard for one rule.

I'm running kernel 4.4.0, ubuntu, iptables 1.6.0. The `+` character in an iptables `-i` match expression is only interpreted as a wildcard character if it appears at the end of an interface match expression. Consequently, no *funny* behavior occurs if I rename my interface to `+foo` (e.g. `ip link set + name +foo`). Matching on the interface name then becomes a normal string equality test, i.e. `-I INPUT -i +foo` matches while `-I INPUT -i +foobar` does not match.

Disclaimer: This question is primarily asked for fun and meant to be a brain teaser. I'm not sure if an easy solution exists. Seriously, I'm aware that it is a bad idea to name my interface `+` ;-)

iptables firewall linux-networking

share edit delete flag

edited yesterday

asked Aug 18 at 10:55

corny

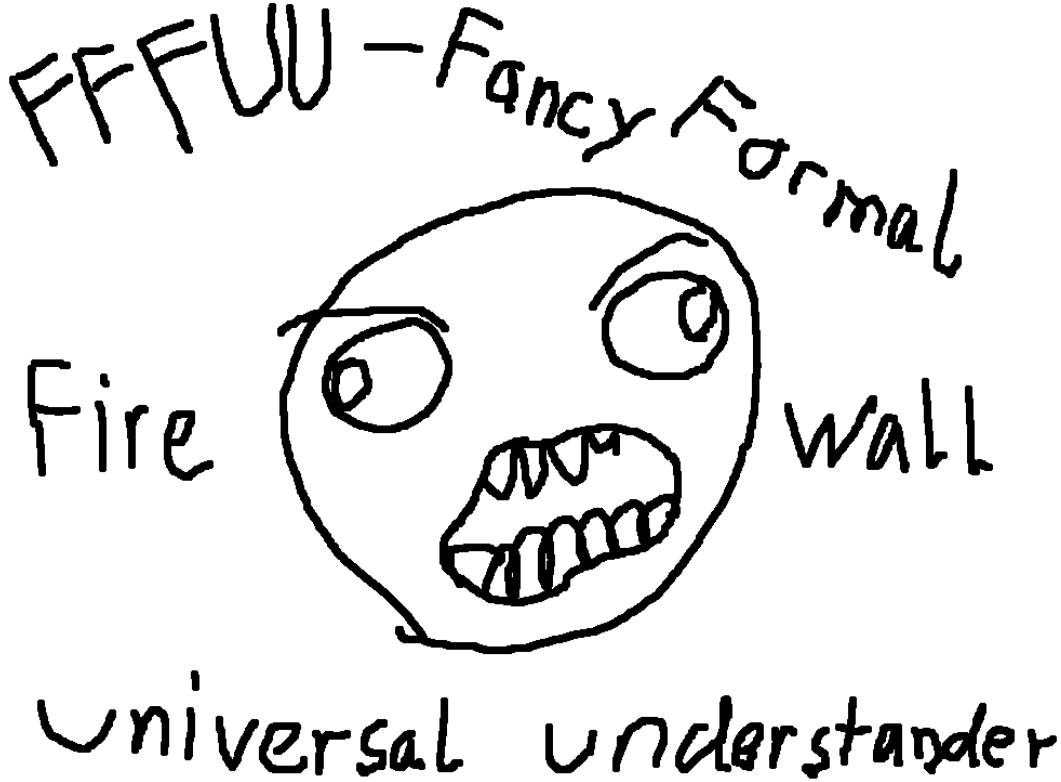
199 ● 6

TURN

Linux Firewall

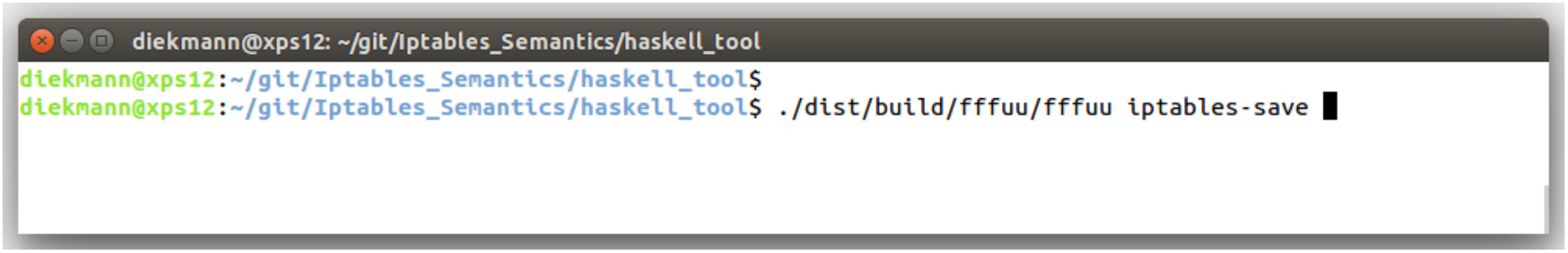
```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:DOS_PROTECT - [0:0]
:GOOD~STUFF - [0:0]
-A FORWARD -j DOS_PROTECT
-A FORWARD -j GOOD~STUFF
-A FORWARD -p tcp -m multiport ! --dports 80,443,6667,6697 -m hashlimit
    --hashlimit-above 10/sec --hashlimit-burst 20 --hashlimit-mode srcip
    --hashlimit-name aflood --hashlimit-srcmask 8 -j LOG
-A FORWARD ! -i lo -s 127.0.0.0/8 -j DROP
-A FORWARD -i internal -s 131.159.21.0/24 -j ACCEPT
-A FORWARD -s 131.159.15.240/28 -d 131.159.21.0/24 -j DROP
-A FORWARD -p tcp -d 131.159.15.240/28 -j ACCEPT
-A FORWARD -i [illegible] -p tcp -s 131.159.15.240/28 -j ACCEPT
-A GOOD~STUFF -i lo -j ACCEPT
-A GOOD~STUFF -m state --state ESTABLISHED -j ACCEPT
-A GOOD~STUFF -p icmp -m state --state RELATED -j ACCEPT
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 ... --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
COMMIT
```

FFFUU



http://iptables.isabelle.systems/

FFFUU: Usage

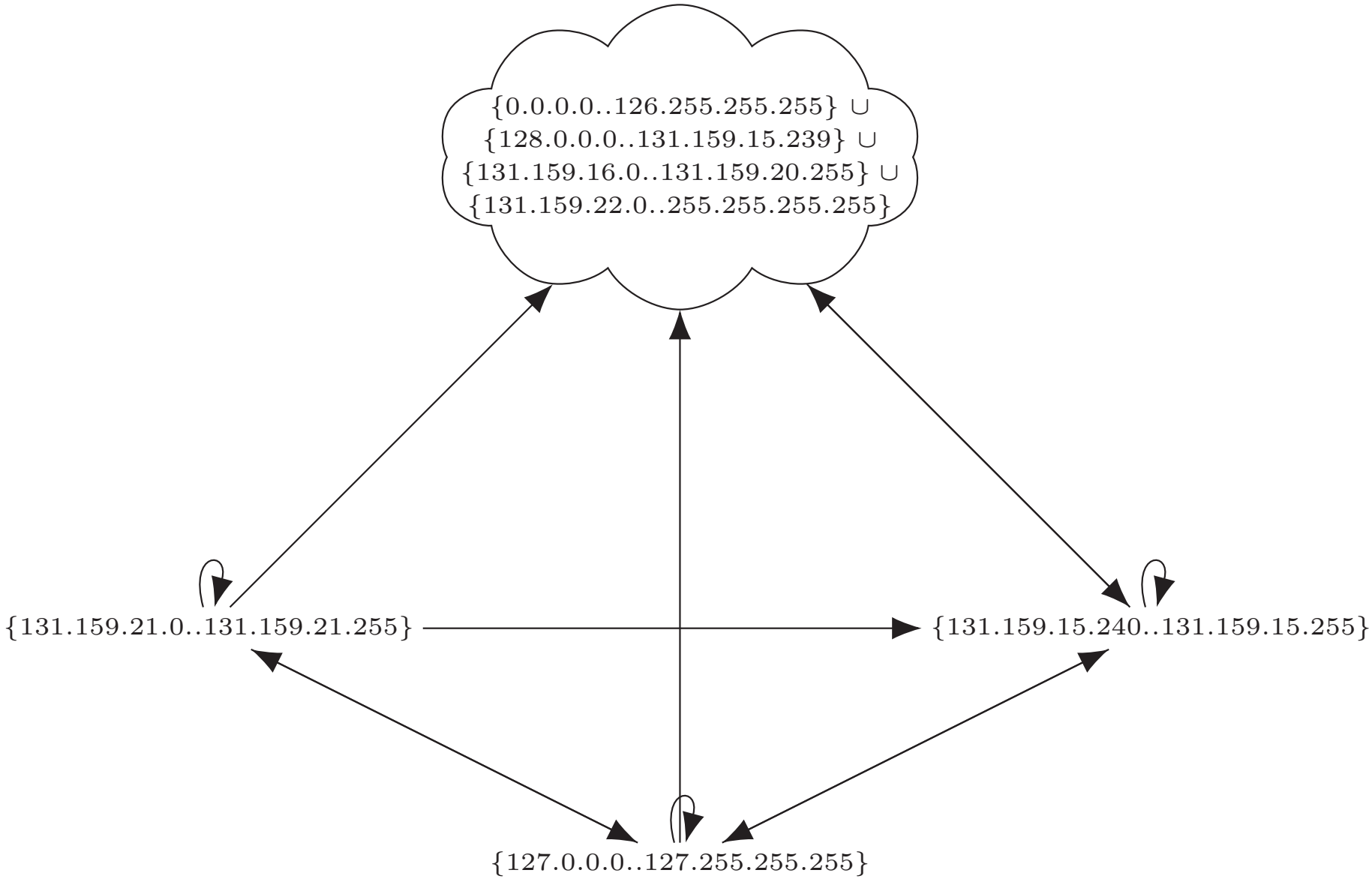


http://iptables.isabelle.systems/

diekmann@xps12: ~/git/Iptables_Semantics/haskell_tool

```
== to even-simpler firewall ==
ACCEPT     all  --  127.0.0.0/8            0.0.0.0/0
ACCEPT     all  --  131.159.21.0/24            0.0.0.0/0
DROP     all  --  131.159.15.240/28            131.159.21.0/24
ACCEPT     tcp  --  0.0.0.0/0            131.159.15.240/28
ACCEPT     tcp  --  131.159.15.240/28            0.0.0.0/0
DROP     all  --  0.0.0.0/0            0.0.0.0/0
== checking spoofing protection ==
WARNING There are some interfaces in your firewall ruleset which are not defined in your ipassmt.
distinct: passed
ipassmt_sanity_nowildcards: passed
ipassmt_sanity_defined (interfaces defined in the ruleset are also in ipassmt): fail: [dmz, inteneral]
ipassmt_sanity_disjoint (no zone-spanning interfaces): passed
ipassmt_sanity_disjoint excluding UNIV interfaces: passed
ipassmt_sanity_complete: the following is not covered: {0.0.0.0 .. 126.255.255.255} u {128.0.0.0 .. 255.255.255.255}
ipassmt_sanity_complete excluding UNIV interfaces: the following is not covered: {0.0.0.0 .. 126.255.255.255} u {128.0.0.0
.. 255.255.255.255}
Spoofing certification results:
("lo","Probably not (False)")
== calculating service matrices ==
========== TCP port 10000->22 =========
a |-> {131.159.21.0 .. 131.159.21.255}
b |-> {131.159.15.240 .. 131.159.15.255}
c |-> {127.0.0.0 .. 127.255.255.255}
d |-> {0.0.0.0 .. 126.255.255.255} u {128.0.0.0 .. 131.159.15.239} u {131.159.16.0 .. 131.159.20.255} u {131.159.22.0 .. 25
5.255.255.255}

(a,a)
(a,b)
(a,c)
(a,d)
(b,b)
(b,c)
(b,d)
(c,a)
(c,b)
(c,c)
(c,d)
(d,b)
```


{0.0.0.0..126.255.255.255} ∪
{128.0.0.0..131.159.15.239} ∪
{131.159.16.0..131.159.20.255} ∪
{131.159.22.0..255.255.255.255}
{131.159.21.0..131.159.21.255}
{131.159.15.240..131.159.15.255}
{127.0.0.0..127.255.255.255}

Properties

Soundness

- You can lookup any pair of IPv4 addresses in the picture
- If there is an arrow between the IPs, then the firewall may allow the communication
- If there is no arrow, then the firewall definitely blocks the communication

Properties

Soundness

- You can lookup any pair of IPv4 addresses in the picture
- If there is an arrow between the IPs, then the firewall may allow the communication
- If there is no arrow, then the firewall definitely blocks the communication

Properties

Soundness

- You can lookup any pair of IPv4 addresses in the picture
- If there is an arrow between the IPs, then the firewall may allow the communication
- If there is no arrow, then the firewall definitely blocks the communication

¬ Completeness

- We translate to a simplified firewall model which is less expressive

Properties

Soundness

- You can lookup any pair of IPv4 addresses in the picture
- If there is an arrow between the IPs, then the firewall may allow the communication
- If there is no arrow, then the firewall definitely blocks the communication

¬ Completeness

- We translate to a simplified firewall model which is less expressive
- Overapproximation: our simplified firewall accepts at least all the packets which the original firewall accepts

Properties

Soundness

- You can lookup any pair of IPv4 addresses in the picture
- If there is an arrow between the IPs, then the firewall may allow the communication
- If there is no arrow, then the firewall definitely blocks the communication

¬ Completeness

- We translate to a simplified firewall model which is less expressive
- Overapproximation: our simplified firewall accepts at least all the packets which the original firewall accepts
- Approximation: it may accept more

Properties

Soundness

- You can lookup any pair of IPv4 addresses in the picture
- If there is an arrow between the IPs, then the firewall may allow the communication
- If there is no arrow, then the firewall definitely blocks the communication

¬ Completeness

- We translate to a simplified firewall model which is less expressive
- Overapproximation: our simplified firewall accepts at least all the packets which the original firewall accepts
- Approximation: it may accept more

Example

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j ACCEPT
COMMIT
```

Example

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j ACCEPT
COMMIT
```

Example

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j ACCEPT
COMMIT
```

Example

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j ACCEPT
COMMIT
```

- Overapproximation: Firewall accepts everything

```
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

Example

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j ACCEPT
COMMIT
```

- Overapproximation: Firewall accepts everything

```
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Sound ☺

Example

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j ACCEPT
COMMIT
```

- Overapproximation: Firewall accepts everything

```
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Sound ☺
- But useless ☹

Example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j DROP
COMMIT
```

Example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon
    -m comment --comment Sprechzeiten -j DROP
COMMIT
```

Example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j DROP
COMMIT
```

- Overapproximation: Firewall accepts everything

```
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

Example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon
    -m comment --comment Sprechzeiten -j DROP
COMMIT
```

- Overapproximation: Firewall accepts everything

```
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Sound ☺

Example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -m time --timestart 07:45 --timestop 08:00 --weekdays Mon ↩
    -m comment --comment Sprechzeiten -j DROP
COMMIT
```

- Overapproximation: Firewall accepts everything

```
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Sound ☺
- Exactly what we want ☺

Another Example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:CHAIN - [0:0]
-A FORWARD -j CHAIN
-A CHAIN -p tcp -m tcp --sport 22 -j RETURN
-A CHAIN -p udp -m udp --dport 80 -j RETURN
-A CHAIN -j DROP
COMMIT
```

- What does it do?

Another Example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:CHAIN - [0:0]
-A FORWARD -j CHAIN
-A CHAIN -p tcp -m tcp --sport 22 -j RETURN
-A CHAIN -p udp -m udp --dport 80 -j RETURN
-A CHAIN -j DROP
COMMIT
```

- What does it do?
- Accepts everything from TCP srcport 22 and UDP dstport 80.

Another Example: Running fffuu

- Accept everything from TCP srcport 22 and UDP dstport 80.
- drop the rest

```
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 0:21 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 0:21 dports: 81:65535
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 23:65535 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 23:65535 dports: 81:65535
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

Another Example: Running fffuu

- Accept everything from TCP srcport 22 and UDP dstport 80.
- drop the rest

```
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 0:21 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 0:21 dports: 81:65535
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 23:65535 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 23:65535 dports: 81:65535
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Wait, . . .

Another Example: Running fffuu

- Accept everything from TCP srcport 22 and UDP dstport 80.
- drop the rest

```
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 0:21 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 0:21 dports: 81:65535
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 23:65535 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 23:65535 dports: 81:65535
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Wait, . . .

Another Example: Running fffuu

- Accept everything from TCP srcport 22 and UDP dstport 80.
- drop the rest

```
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 0:21 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 0:21 dports: 81:65535
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 23:65535 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0    sports: 23:65535 dports: 81:65535
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Wait, . . .
- Does this even make sense?

Another Example: Running fffuu

- Accept everything from TCP srcport 22 and UDP dstport 80.
- drop the rest

```
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 0:21 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 0:21 dports: 81:65535
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 23:65535 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 23:65535 dports: 81:65535
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Wait, . . .
- Does this even make sense?
- Not the policy we wanted: Accepts anything with srcport 22 or dstport 80. TCP, UDP, SCTP,

Another Example: Running fffuu

- Accept everything from TCP srcport 22 and UDP dstport 80.
- drop the rest

```
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 0:21 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 0:21 dports: 81:65535
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 23:65535 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0           sports: 23:65535 dports: 81:65535
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Wait, . . .
- Does this even make sense?
- Not the policy we wanted: Accepts anything with srcport 22 or dstport 80. TCP, UDP, SCTP, ICMP, . . .

Another Example

- Accept everythi
- drop the rest

```
target     prot opt so
DROP       all  --  0
DROP       all  --  0
DROP       all  --  0
DROP       all  --  0
ACCEPT     all  --  0
```

```
9
65535
0:79
81:65535
```

- Wait, . . .
- Does this even
- Not the policy w
  UDP, SCTP, ICM
- Very broken!

t 80. TCP,

Another Example: Running fffuu

- Accept everything from TCP srcport 22 and UDP dstport 80.
- drop the rest

```
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 0:21 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 0:21 dports: 81:65535
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 23:65535 dports: 0:79
DROP       all  --  0.0.0.0/0            0.0.0.0/0     sports: 23:65535 dports: 81:65535
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

- Wait, . . .
- Does this even make sense?
- Not the policy we wanted: Accepts anything with srcport 22 or dstport 80. TCP, UDP, SCTP, ICMP, . . .
- Very broken!
- Challenge: Construct unsoundness.

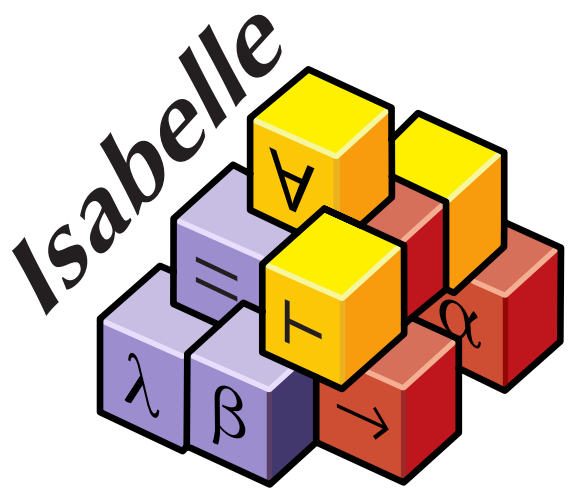
It is ‘formally verified’, how can it be unsound?

It is ‘formally verified’, how can it be unsound?

- Proof?

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)



It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means?

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?
- Rowhammer!

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?
- Rowhammer! Hardware Rootkit!

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?
- Rowhammer! Hardware Rootkit! Put on your tinfoil hats!

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?
- Rowhammer! Hardware Rootkit! Put on your tinfoil hats! ✗
  (could be, but there is a simpler explanation)

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?
- Rowhammer! Hardware Rootkit! Put on your tinfoil hats! ✗
  (could be, but there is a simpler explanation)
- Okay, it’s the assumptions:

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?
- Rowhammer! Hardware Rootkit! Put on your tinfoil hats! ✗
  (could be, but there is a simpler explanation)
- Okay, it’s the assumptions:
- Error in the model

It is ‘formally verified’, how can it be unsound?

- Proof? ✓ (Isabelle)
- Does the soundness theorem really mean what we think it means? ✓ (trust me)
- Unrealistic assumptions ✓ (checked)
- What else?
- Rowhammer! Hardware Rootkit! Put on your tinfoil hats! ✗
  (could be, but there is a simpler explanation)
- Okay, it’s the assumptions:
- Error in the model ✗

Model: Filtering Behavior

$$\textsc{Skip}\ \frac{}{\Gamma, \gamma, p \vdash \langle [],\ t \rangle \Rightarrow t}$$

$$\textsc{Accept}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Accept})],\ ? \rangle \Rightarrow \checkmark}$$

$$\textsc{Drop}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Drop})],\ ? \rangle \Rightarrow \times}$$

$$\textsc{Reject}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Reject})],\ ? \rangle \Rightarrow \times}$$

$$\textsc{NoMatch}\ \frac{\neg\ \text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ a)],\ ? \rangle \Rightarrow ?}$$

$$\textsc{Decision}\ \frac{t \neq ?}{\Gamma, \gamma, p \vdash \langle rs,\ t \rangle \Rightarrow t}$$

$$\textsc{Seq}\ \frac{\Gamma, \gamma, p \vdash \langle rs_1,\ ? \rangle \Rightarrow t \qquad \Gamma, \gamma, p \vdash \langle rs_2,\ t \rangle \Rightarrow t'}{\Gamma, \gamma, p \vdash \langle rs_1 :::\ rs_2,\ ? \rangle \Rightarrow t'}$$

$$\textsc{Log}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Log})],\ ? \rangle \Rightarrow ?}$$

$$\textsc{Empty}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Empty})],\ ? \rangle \Rightarrow ?}$$

$$\textsc{CallResult}\ \frac{\text{matches } \gamma\ m\ p \qquad \Gamma, \gamma, p \vdash \langle \Gamma\ c,\ ? \rangle \Rightarrow t}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Call}\ c)],\ ? \rangle \Rightarrow t}$$

$$\textsc{CallReturn}\ \frac{\text{matches } \gamma\ m\ p \qquad \Gamma\ c = rs_1 ::: (m',\ \texttt{Return}) :: rs_2 \qquad \text{matches } \gamma\ m'\ p \qquad \Gamma, \gamma, p \vdash \langle rs_1,\ ? \rangle \Rightarrow ?}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Call}\ c)],\ ? \rangle \Rightarrow ?}$$

Background ruleset $\Gamma : \mathit{chain\ name} \rightarrow \mathit{rule\ list}$

Model: Filtering Behavior

$$\textsc{Skip}\ \frac{}{\Gamma, \gamma, p \vdash \langle [],\ t \rangle \Rightarrow t}$$

$$\textsc{Accept}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Accept})],\ ? \rangle \Rightarrow \checkmark}$$

$$\textsc{Drop}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Drop})],\ ? \rangle \Rightarrow \times}$$

$$\frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Reject})],\ ? \rangle \Rightarrow \times}$$

$$\textsc{NoMatch}\ \frac{\neg\ \text{matches } \gamma\ m}{\Gamma, \gamma, p \vdash \langle [(m,\ a)}$$

$$\textsc{Decision}\ \frac{t \neq ?}{\Gamma, \gamma, p \vdash \langle rs,\ t \rangle \Rightarrow t}$$

$$\textsc{Seq}\ \frac{\Gamma, \gamma, p \vdash \langle rs_1,\ ? \rangle \Rightarrow t \qquad \Gamma, \gamma, }{\Gamma, \gamma, p \vdash \langle rs_1 :::$$

$$\textsc{Log}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Log})],\ ? \rangle \Rightarrow ?}$$

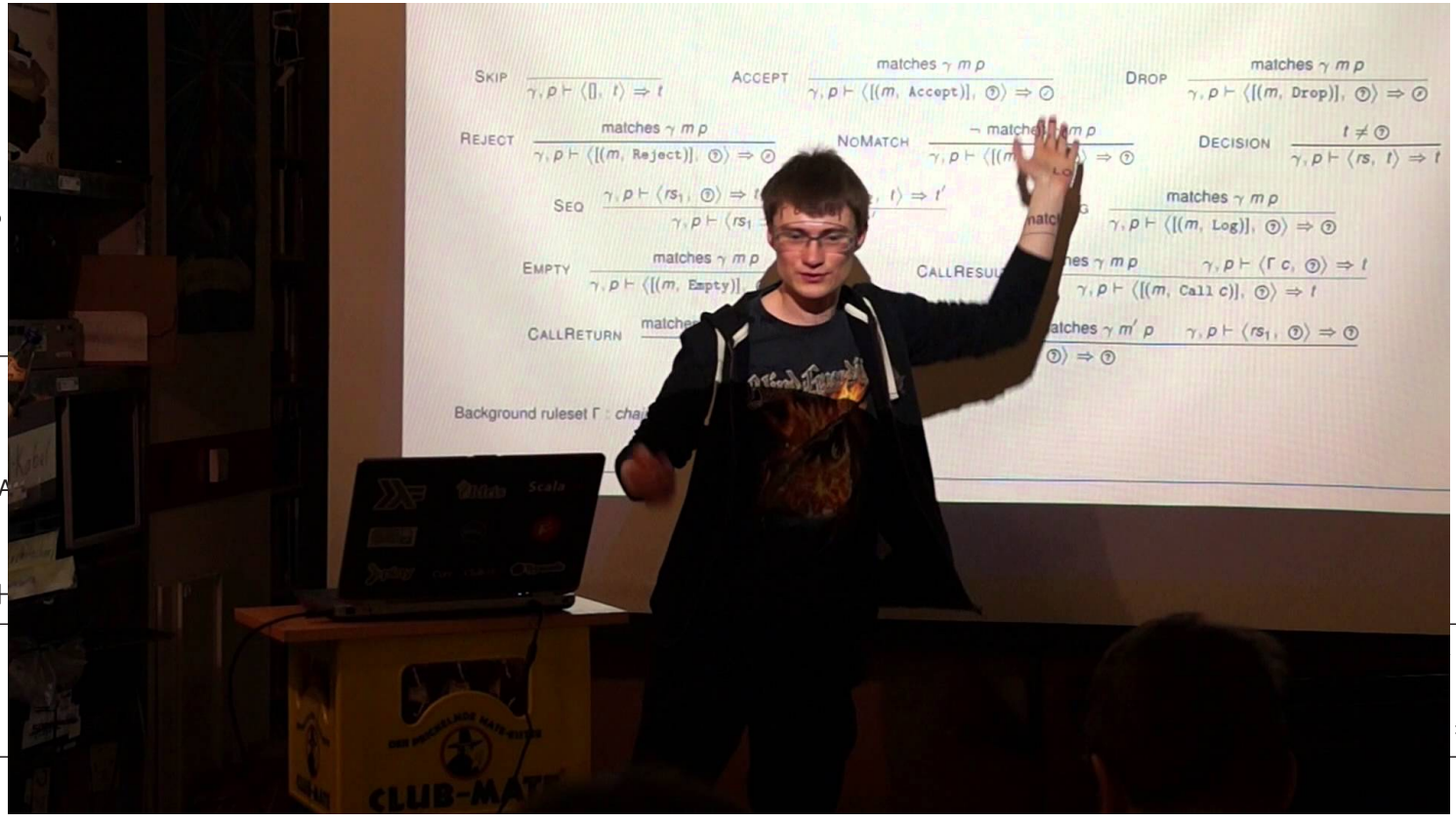
$$\textsc{Empty}\ \frac{\text{matches } \gamma\ m\ p}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Empty})],\ ? \rangle \Rightarrow ?}$$

$$\textsc{CallResult}\ \frac{\text{matches } \gamma\ m\ p \qquad \Gamma, \gamma, p \vdash \langle \Gamma\ c,\ ? \rangle \Rightarrow t}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Call}\ c)],\ ? \rangle \Rightarrow t}$$

$$\textsc{CallReturn}\ \frac{\text{matches } \gamma\ m\ p \qquad \Gamma\ c = rs_1 ::: (m',\ \texttt{Return}) :: rs_2 \qquad \text{matches } \gamma\ m'\ p \qquad \Gamma, \gamma, p \vdash \langle rs_1,\ ? \rangle \Rightarrow ?}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Call}\ c)],\ ? \rangle \Rightarrow ?}$$

Background ruleset $\Gamma : \mathit{chain\ name} \rightarrow \mathit{rule\ list}$

Model: Filtering Behavior



$$\textsc{Skip}\ \frac{}{\gamma, p \vdash \langle [],\ t \rangle \Rightarrow t} \qquad \textsc{Accept}\ \frac{\text{matches}\ \gamma\ m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Accept})],\ ? \rangle \Rightarrow \checkmark} \qquad \textsc{Drop}\ \frac{\text{matches}\ \gamma\ m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Drop})],\ ? \rangle \Rightarrow \times}$$

$$\textsc{Reject}\ \frac{\text{matches}\ \gamma\ m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Reject})],\ ? \rangle \Rightarrow \times} \qquad \textsc{NoMatch}\ \frac{\neg\ \text{matches}\ \gamma\ m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Reject})],\ ? \rangle \Rightarrow ?} \qquad \textsc{Decision}\ \frac{t \neq ?}{\gamma, p \vdash \langle rs,\ t \rangle \Rightarrow t}$$

$$\textsc{Seq}\ \frac{\gamma, p \vdash \langle rs_1,\ ? \rangle \Rightarrow ? \qquad \gamma, p \vdash \langle rs_2,\ t \rangle \Rightarrow t'}{\gamma, p \vdash \langle rs_1 \ldots}$$

$$\textsc{Empty}\ \frac{\text{matches}\ \gamma\ m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Empty})] \ldots}$$

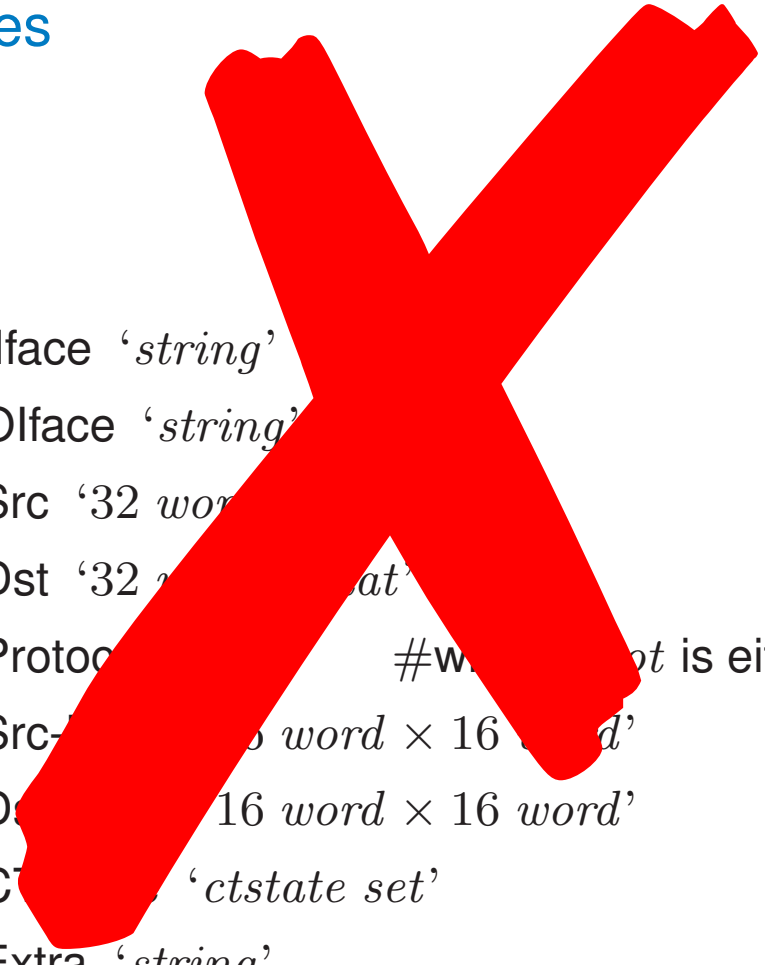
$$\textsc{CallReturn}\ \frac{\text{matches}\ \gamma\ m\ p \qquad \Gamma\ c = rs_1\ ::: (m',\ \texttt{Return}) :: rs_2 \qquad \text{matches}\ \gamma\ m'\ p \qquad \Gamma, \gamma, p \vdash \langle rs_1,\ ? \rangle \Rightarrow ?}{\Gamma, \gamma, p \vdash \langle [(m,\ \texttt{Call}\ c)],\ ? \rangle \Rightarrow ?}$$

Background ruleset $\Gamma : \mathit{chain\ name} \rightarrow \mathit{rule\ list}$

Model: Matching Features

datatype $primitive$ = IIface ‘$string$’
| OIface ‘$string$’
| Src ‘$32\ word \times nat$’
| Dst ‘$32\ word \times nat$’
| Protocol ‘$prot$’ #where $prot$ is either Any or $8\ word$
| Src-Ports ‘$16\ word \times 16\ word$’
| Dst-Ports ‘$16\ word \times 16\ word$’
| CT-State ‘$ctstate\ set$’
| Extra ‘$string$’

Model: Matching Features



datatype $primitive$ = IIface ‘$string$’
OIface ‘$string$’
Src ‘32 wo
Dst ‘32 at’
Protoc $\#w$ ot is either Any or $8\ word$
Src- $word \times 16$ d’
D $16\ word \times 16\ word$’
C ‘$ctstate\ set$’
Extra ‘$string$’

Model: Matching Features

datatype

There is no such things as ports!

Dst ‘$32\ word \times nat$’

Protocol ‘$prot$’ #where $prot$ is either Any or $8\ word$

Src-Ports ‘$16\ word \times 16\ word$’

Dst-Ports ‘$16\ word \times 16\ word$’

CT-State ‘$ctstate\ set$’

Extra ‘$string$’

Model: Matching Features

datatype

There is no such things as ports!

but there are TCP ports, UDP ports, SCTP ports, ...

Dst $'32\ word \times nat'$

Protocol $'prot'$ #where $prot$ is either Any or $8\ word$

Src-Ports $'16\ word \times 16\ word'$

Dst-Ports $'16\ word \times 16\ word'$

CT-State $'ctstate\ set'$

Extra $'string'$

Model: Matching Features

datatype

There is no such things as ports!

but there are TCP ports, UDP ports, SCTP ports, ...

Dst $'32\ word \times nat'$

Protocol $'prot'$ #where $prot$ is either Any or $8\ word$

Src-Ports $'8\ word'$ $'16\ word \times 16\ word'$

Dst-Ports $'8\ word'$ $'16\ word \times 16\ word'$

CT-State $'ctstate\ set'$

Extra $'string'$

Negating Matches on Ports

- `! (-p tcp --dport 80) -j ACCEPT`

Negating Matches on Ports

- `! (-p tcp --dport 80) -j ACCEPT`
- `! -p tcp -j ACCEPT`
  `-p tcp ! --dport80 -j ACCEPT`

Negating Matches on Ports

- `! (-p tcp --dport 80) -j ACCEPT`
- `! -p tcp -j ACCEPT`
  `-p tcp ! --dport80 -j ACCEPT`
- $\neg(tcp \wedge port80) = \neg tcp \vee (tcp \wedge \neg port80)$

Negating Matches on Ports

- `! (-p tcp --dport 80) -j ACCEPT`
- `! -p tcp -j ACCEPT`
  `-p tcp ! --dport80 -j ACCEPT`
- $\neg(tcp \wedge port80) = \neg tcp \vee (tcp \wedge \neg port80)$
- Dependent matches?

Negating Matches on Ports

- `! (-p tcp --dport 80) -j ACCEPT`
- `! -p tcp -j ACCEPT`
  `-p tcp ! --dport80 -j ACCEPT`
- $\neg(tcp \wedge port80) = \neg tcp \vee (tcp \wedge \neg port80)$
- Dependent matches?
- Match on ports, possibly get a match on protocols for free!

Negating Matches

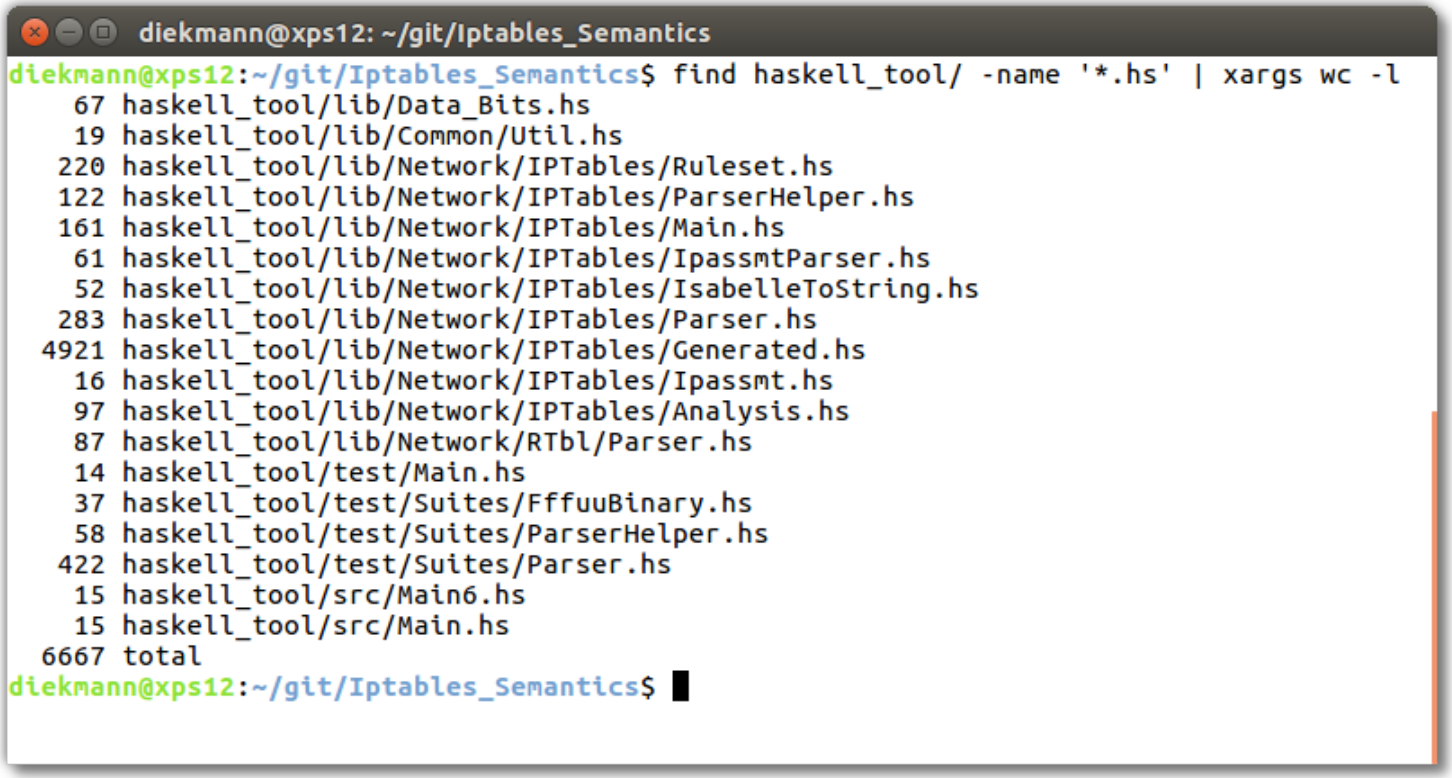
- `! (-p tcp -`
- `! -p tcp -j`
  `-p tcp ! --`
- $\neg(tcp \wedge port8$
- Dependent mat
- Match on ports,

Negating Matches on Ports

- `! (-p tcp --dport 80) -j ACCEPT`
- `! -p tcp -j ACCEPT`
  `-p tcp ! --dport80 -j ACCEPT`
- $\neg(tcp \wedge port80) = \neg tcp \vee (tcp \wedge \neg port80)$
- Dependent matches?
- Match on ports, possibly get a match on protocols for free!
- Common firewall research: just translate match expressions to SAT . . .

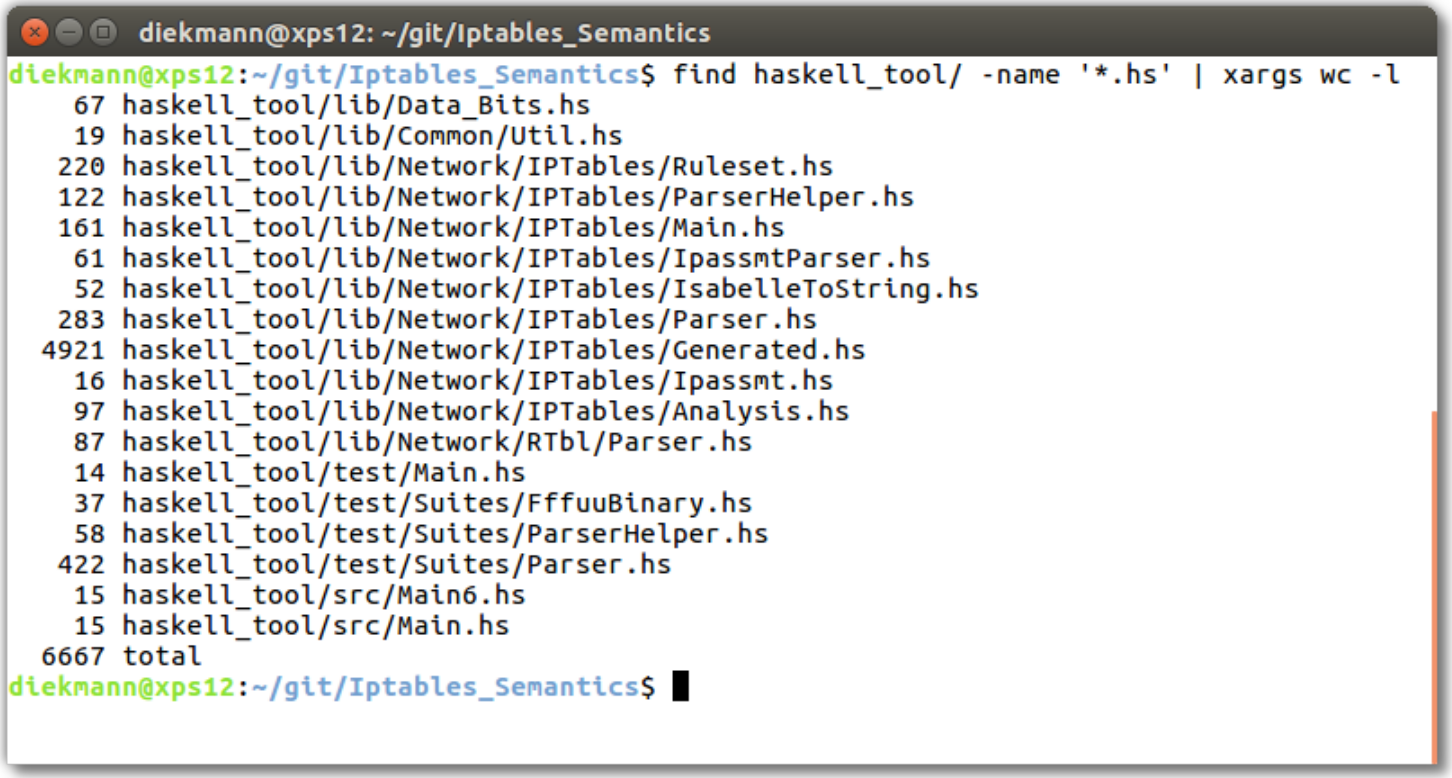
Fixing the Bug in the Code

- The error exists only in your head!



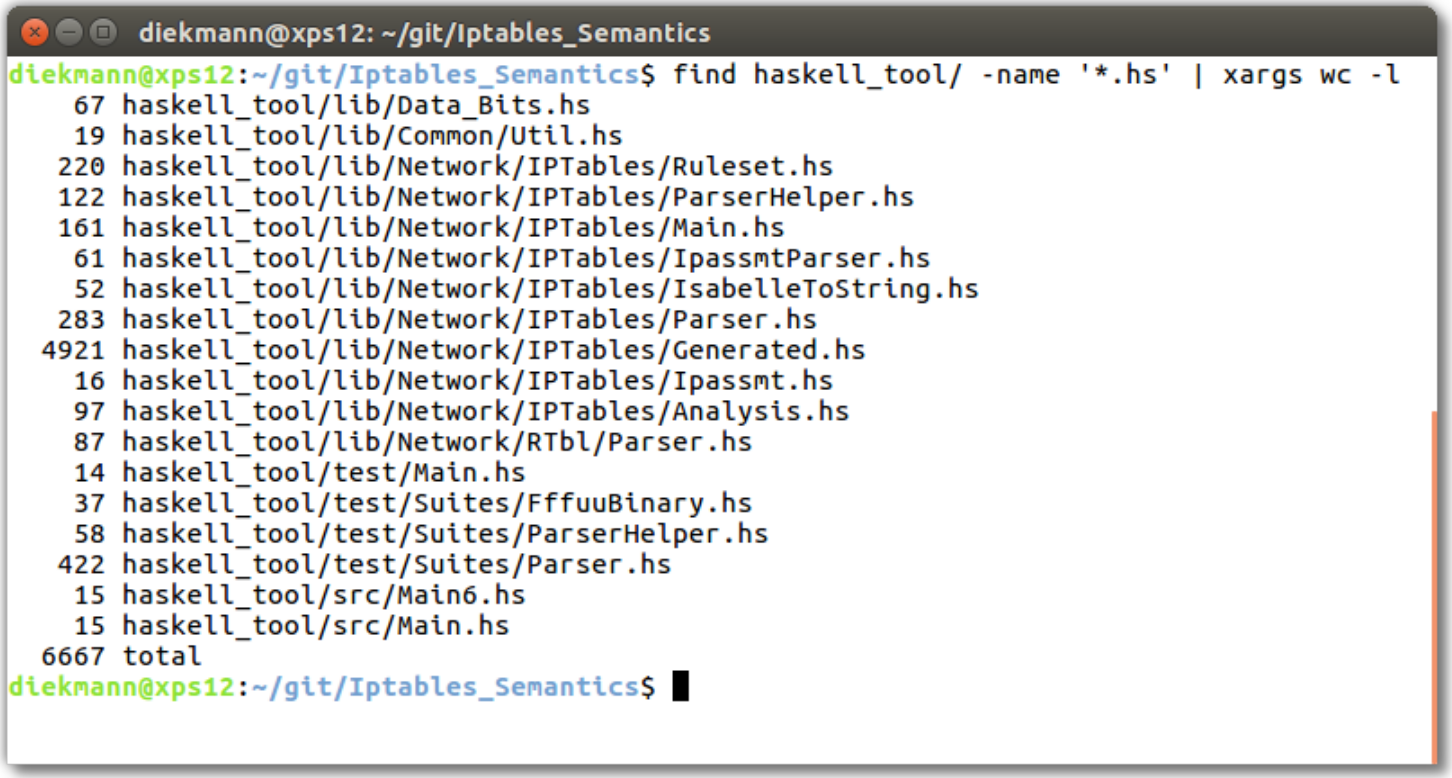
Fixing the Bug in the Code

- The error exists only in your head!
- May be repeated throughout the code . . .



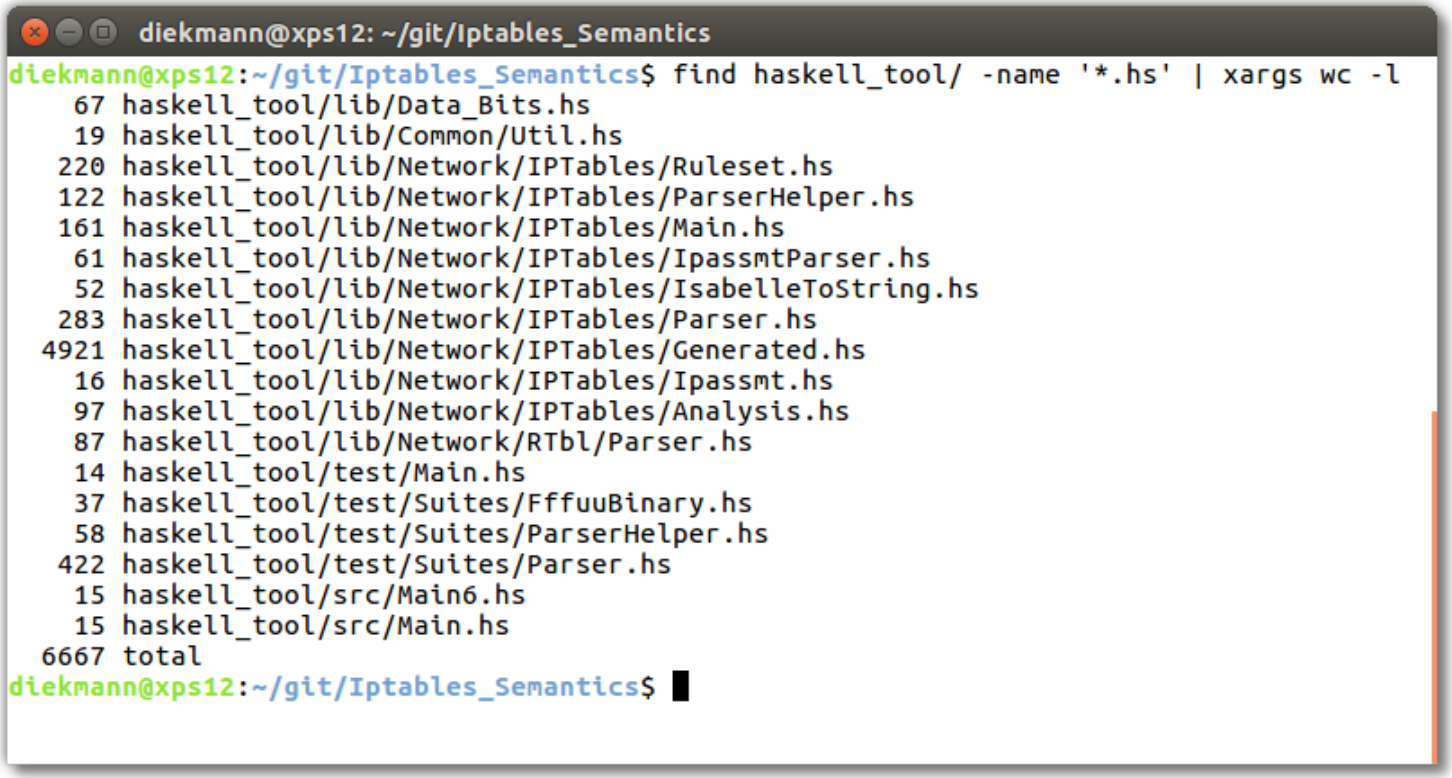
Fixing the Bug in the Code

- The error exists only in your head!
- May be repeated throughout the code . . .
- Fixing may cause odd side effects . . .
  - Normalization routines assume that once a primitive is normalized, another routine will not destroy that



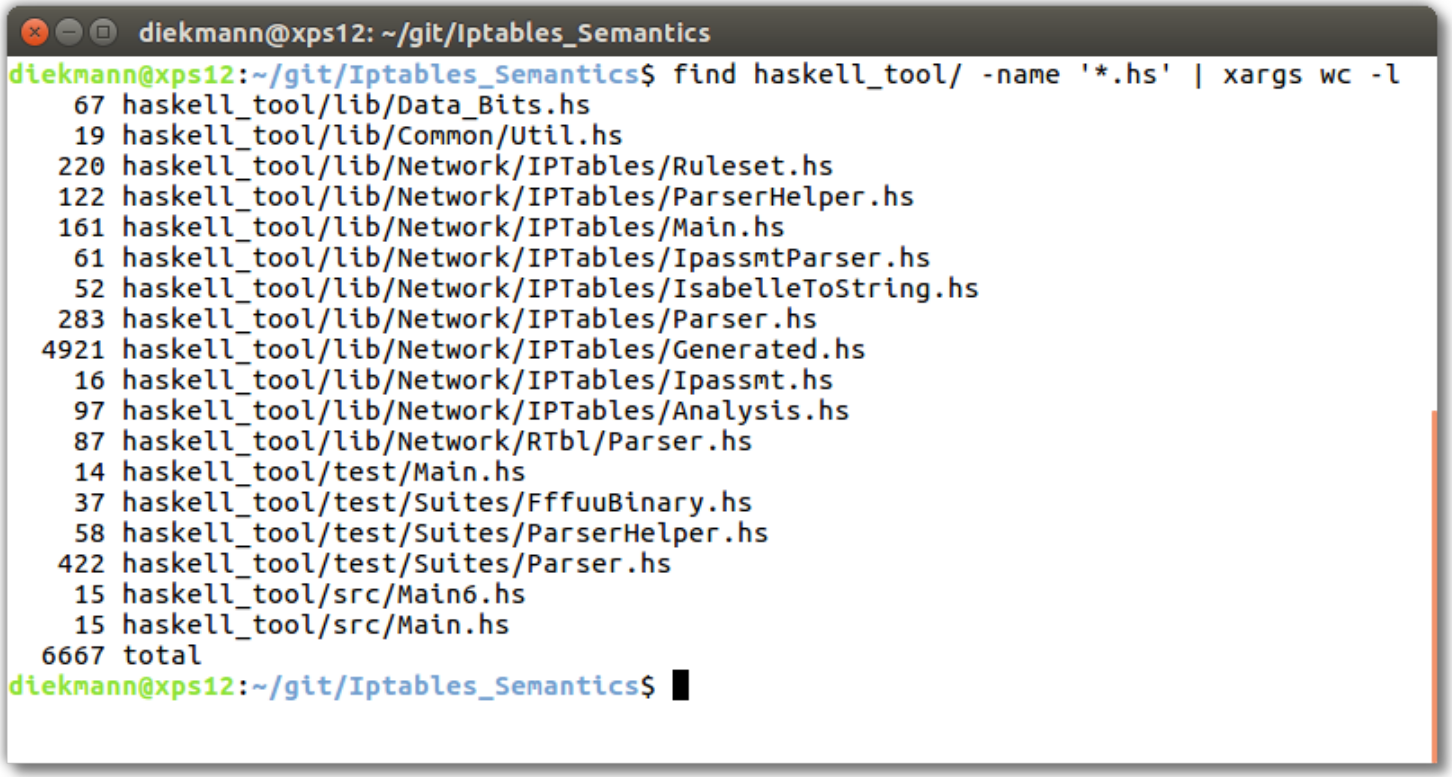
Fixing the Bug in the Code

- The error exists only in your head!
- May be repeated throughout the code . . .
- Fixing may cause odd side effects . . .
  - Normalization routines assume that once a primitive is normalized, another routine will not destroy that
- Almost impossible to get right!



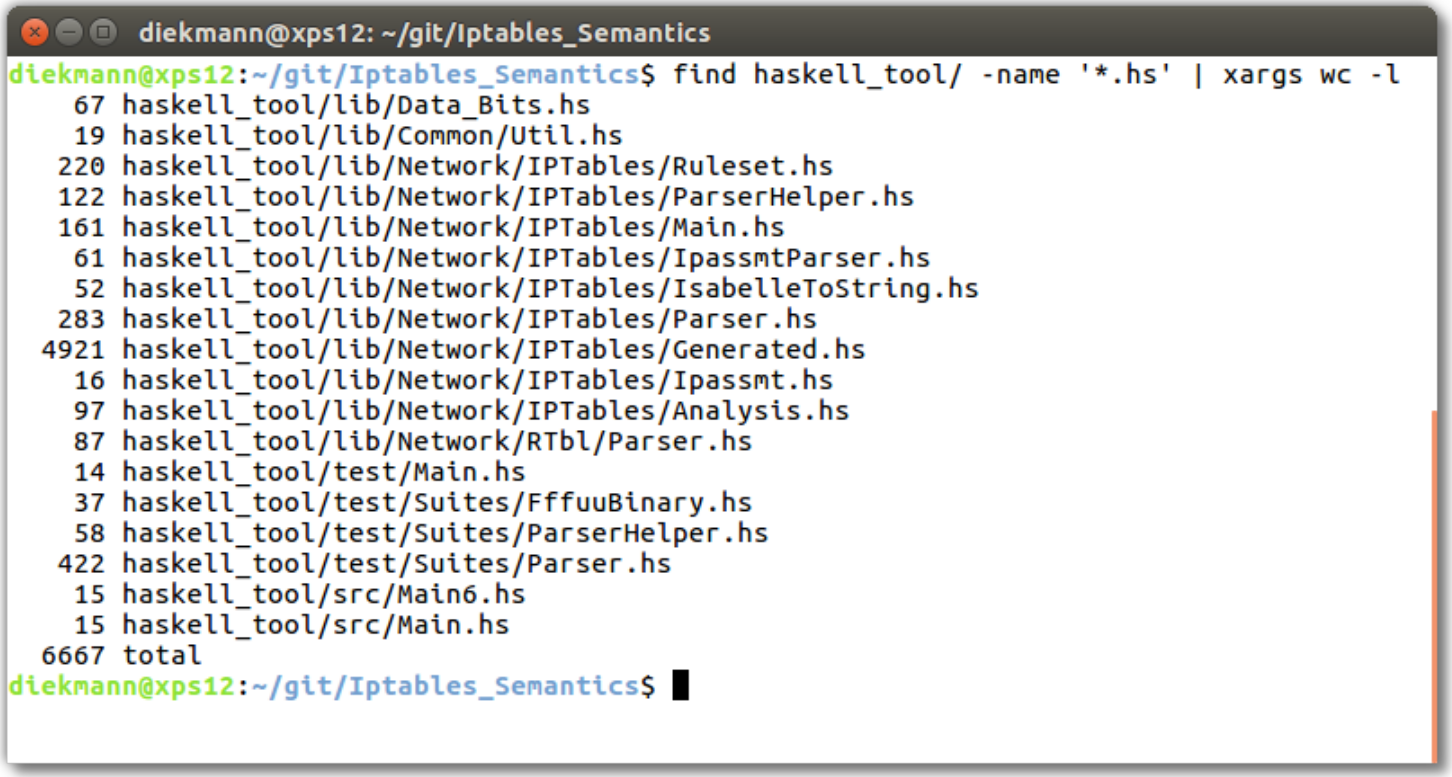
We don’t fix the Code!

- We fix the model!



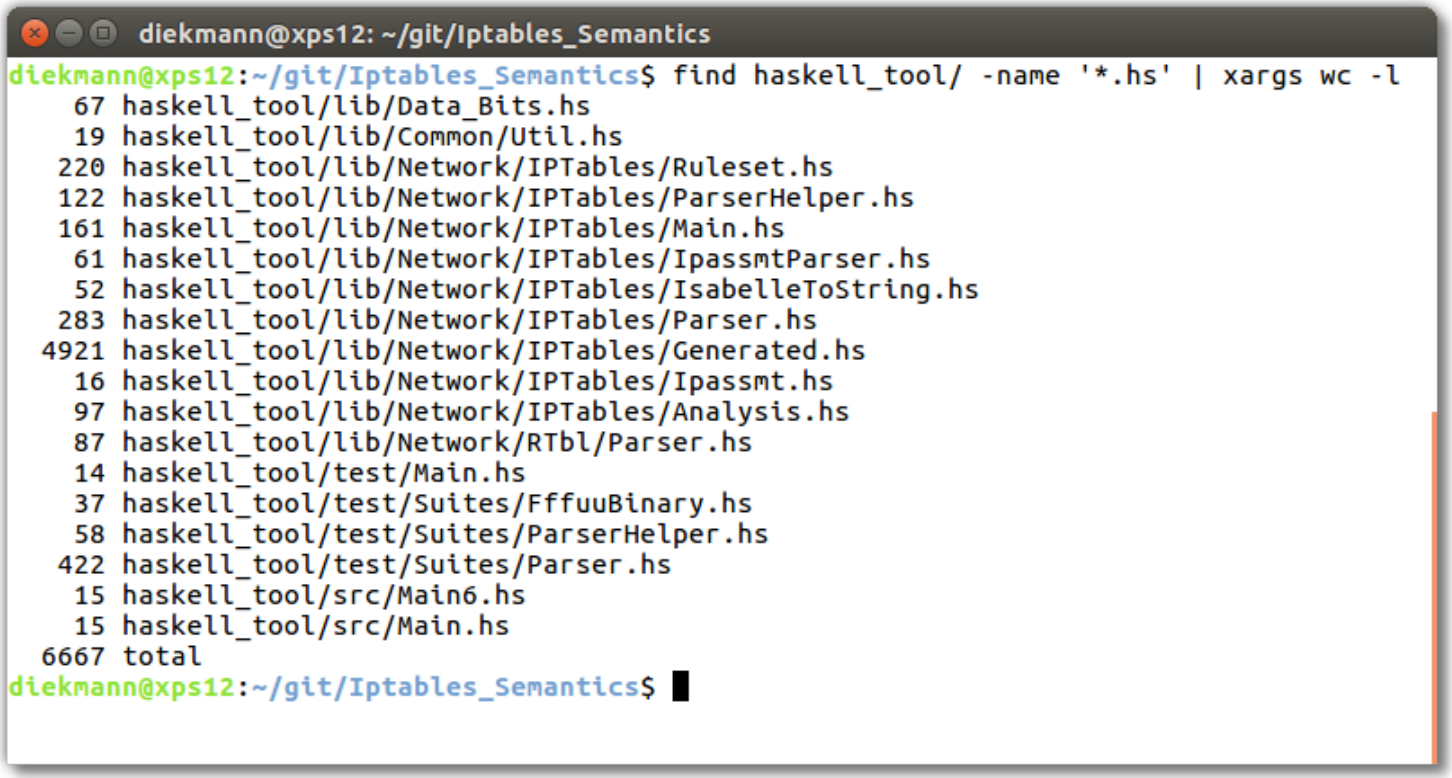
We don’t fix the Code!

- We fix the model! The semantics, the assumptions, . . .



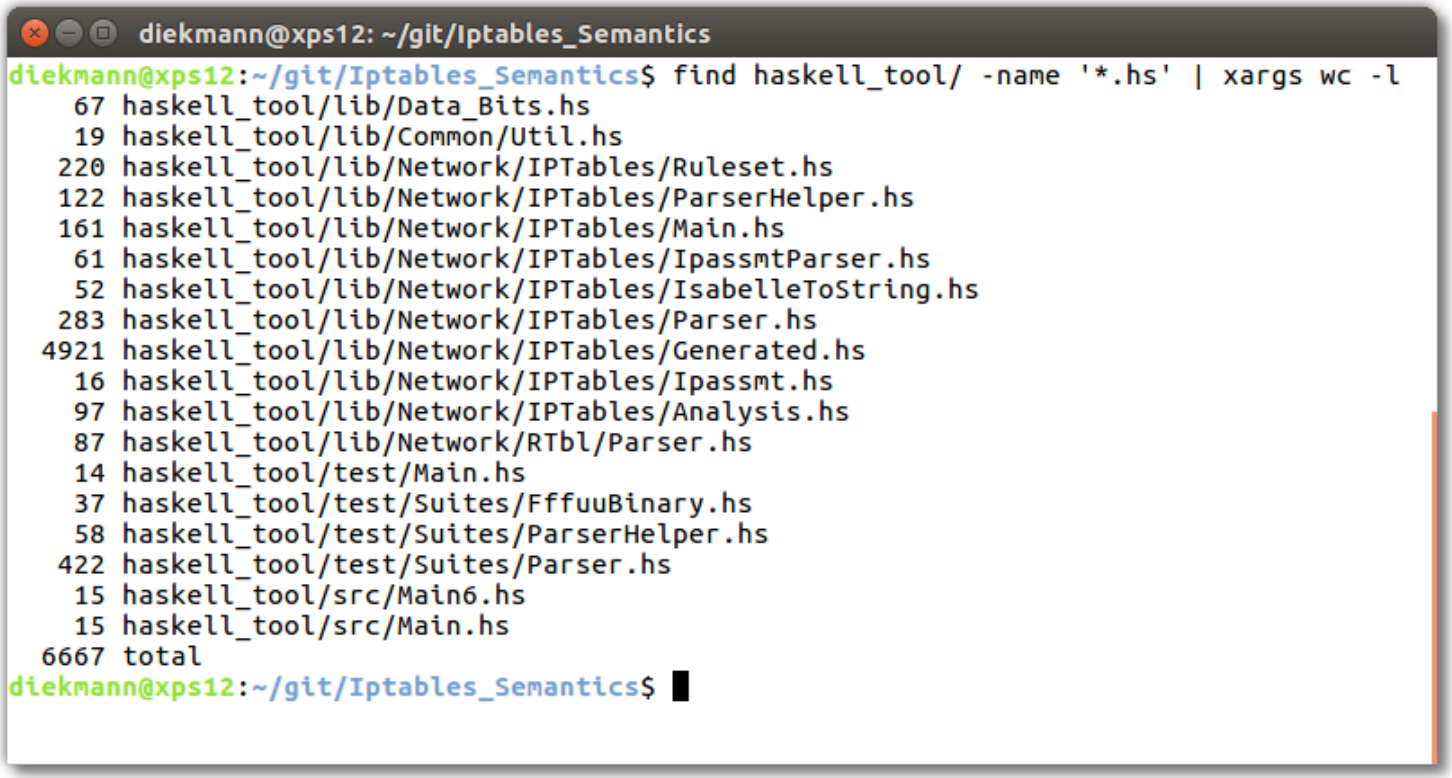
We don’t fix the Code!

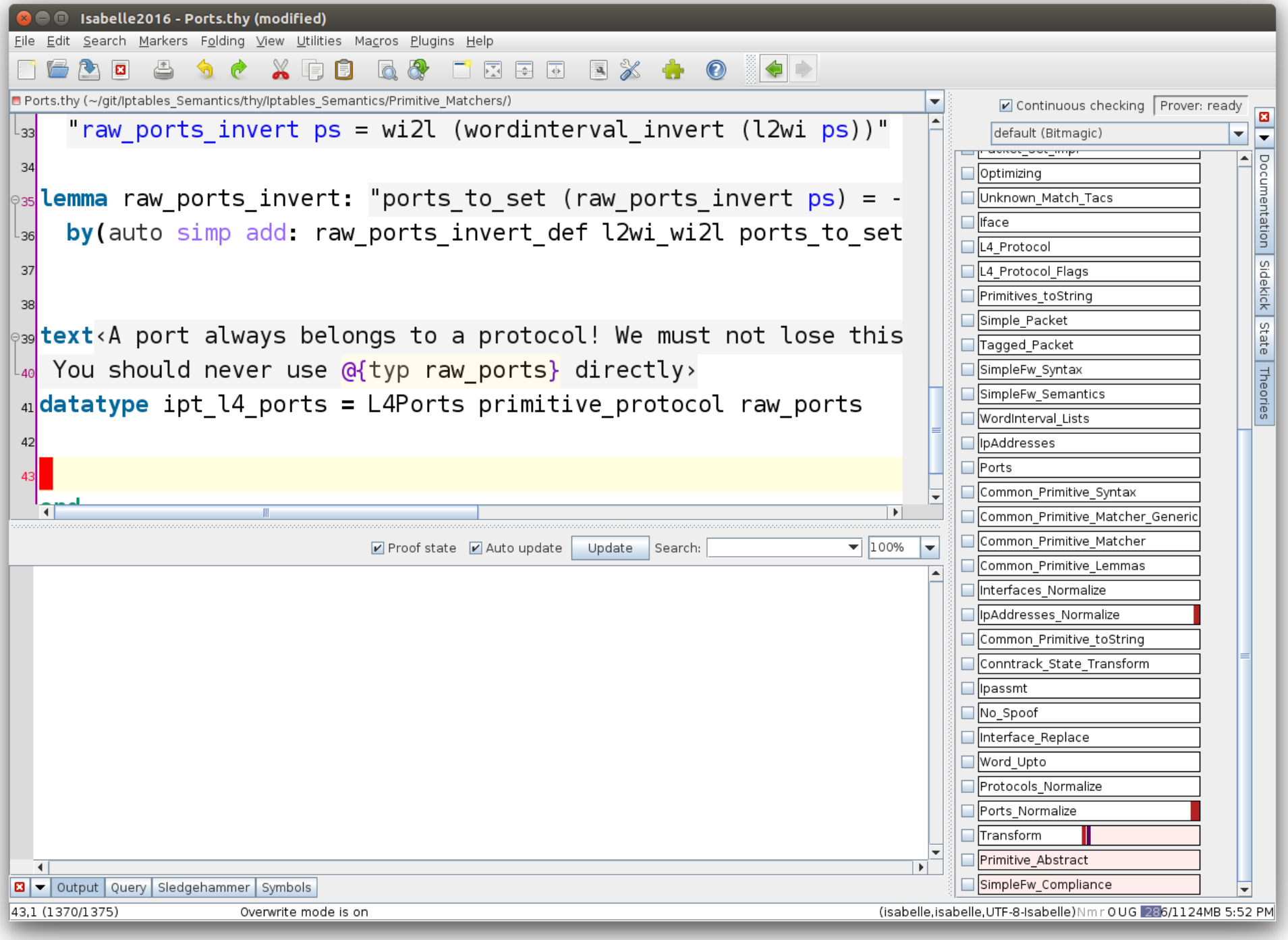
- We fix the model! The semantics, the assumptions, . . .
- You saw the `diff` before



We don’t fix the Code!

- We fix the model! The semantics, the assumptions, . . .
- You saw the `diff` before
- Proofs will fail $\longrightarrow$ we know exactly where we need to fix stuff!




Isabelle2016 - Ports.thy (modified)
File Edit Search Markers Folding View Utilities Macros Plugins Help
Ports.thy (~/git/Iptables_Semantics/thy/Iptables_Semantics/Primitive_Matchers/)
"raw_ports_invert ps = wi2l (wordinterval_invert (l2wi ps))"
lemma raw_ports_invert: "ports_to_set (raw_ports_invert ps) = -
by(auto simp add: raw_ports_invert_def l2wi_wi2l ports_to_set
text‹A port always belongs to a protocol! We must not lose this
You should never use @{typ raw_ports} directly›
datatype ipt_l4_ports = L4Ports primitive_protocol raw_ports
Proof state
Auto update
Update
Search:
100%
Output
Query
Sledgehammer
Symbols
Continuous checking
Prover: ready
default (Bitmagic)
Optimizing
Unknown_Match_Tacs
Iface
L4_Protocol
L4_Protocol_Flags
Primitives_toString
Simple_Packet
Tagged_Packet
SimpleFw_Syntax
SimpleFw_Semantics
WordInterval_Lists
IpAddresses
Ports
Common_Primitive_Syntax
Common_Primitive_Matcher_Generic
Common_Primitive_Matcher
Common_Primitive_Lemmas
Interfaces_Normalize
IpAddresses_Normalize
Common_Primitive_toString
Conntrack_State_Transform
Ipassmt
No_Spoof
Interface_Replace
Word_Upto
Protocols_Normalize
Ports_Normalize
Transform
Primitive_Abstract
SimpleFw_Compliance
Documentation
Sidekick
State
Theories
43,1 (1370/1375)
Overwrite mode is on
(isabelle,isabelle,UTF-8-Isabelle)
5:52 PM

Fixed Model

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:CHAIN - [0:0]
-A FORWARD -j CHAIN
-A CHAIN -p tcp -m tcp --sport 22 -j RETURN
-A CHAIN -p udp -m udp --dport 80 -j RETURN
-A CHAIN -j DROP
COMMIT
```

Simplified

```
DROP      udp  --  0.0.0.0/0    0.0.0.0/0   dports: 0:79
DROP      udp  --  0.0.0.0/0    0.0.0.0/0   dports: 81:65535
DROP      tcp  --  0.0.0.0/0    0.0.0.0/0   sports: 0:21
DROP      tcp  --  0.0.0.0/0    0.0.0.0/0   sports: 23:65535
ACCEPT    all  --  0.0.0.0/0    0.0.0.0/0
```