Grundlagen Informationsicherheit und Datensicherheit, Blatt 5

Lukas Baur, 3131138
Felix Bühler, 2973410
Marco Hildenbrand, 3137242

22. Dezember 2017

Problem 1: Firewalls with nftables

(a)

Router 1

```
nft add table ip filterRouter1
nft add chain ip filterRouter1 chain1 { \
   type filter hook input priority 0; policy drop; \
}
nft add rule ip filterRouter1 chain1 \
   ip saddr 4.2.0.3 ip daddr 10.0.0.6 tcp  sport >= 1024 tcp dport 3306 accept

nft add rule ip filterRouter1 chain1 \
    ct state != new ip saddr 10.0.0.6 ip daddr 4.2.0.3 tcp  sport 3306 tcp dport >= 1024 accept

nft add rule ip filterRouter1 chain1 \
    ip saddr 10.0.0.2 ip daddr 4.2.0.3 accept

nft add rule ip filterRouter1 chain1 \
    ct state != new ip saddr 4.2.0.3 ip daddr 10.0.0.2 accept

nft add rule ip filterRouter1 chain1 \
    ip saddr 10.0.0.2 meta oifname "eth1" accept

nft add rule ip filterRouter1 chain1 \
    ct state != new meta iifname "eth1" ip daddr 10.0.0.2 accept
```

Router 2

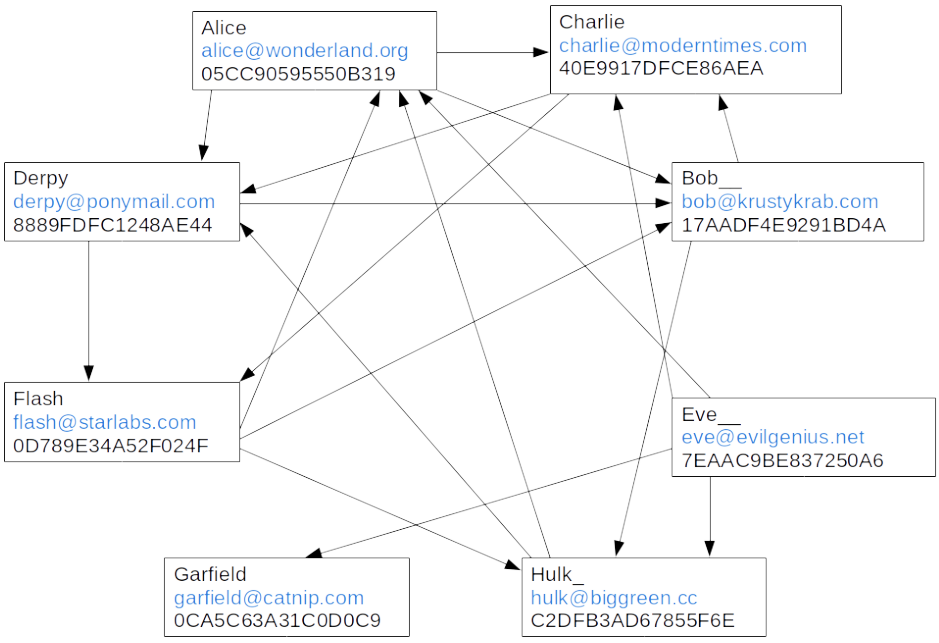
```
nft add table ip filterRouter2
nft add chain ip filterRouter2 chain2 { \
   type filter hook input priority 0; policy drop; \
}
nft add rule ip filterRouter2 chain2 \
    ip saddr 4.2.0.1 meta oifname "eth1" accept

nft add rule ip filterRouter2 chain2 \
    ct state != new meta iifname "eth1" ip daddr 4.2.0.1 accept

nft add rule ip filterRouter2 chain2 \
    meta iifname "eth1" ip daddr 4.2.0.3 tcp sport >= 1024 tcp dport 443 accept

nft add rule ip filterRouter2 chain2 \
    ct state != new ip saddr 4.2.0.3 meta oifname "eth1" tcp sport 443  tcp dport >= 1024 accept
```

Problem 2: Web of Trust and PGP

(a)

```
key 05CC90595550B319: public key "Alice <alice@wonderland.org>"
was signed by:
Flash <flash@starlabs.com>,
Hulk_ <hulk@biggreen.cc>,
Eve__ <eve@evilgenius.net>

key 17AADF4E9291BD4A: public key "Bob__ <bob@krustykrab.com>"
was signed by:
Alice <alice@wonderland.org>,
Derpy <derpy@ponymail.com>,
Flash <flash@starlabs.com>

key 40E9917DFCE86AEA: public key "Charlie <charlie@moderntimes.com>"
was signed by:
Bob__ <bob@krustykrab.com>,
Eve__ <eve@evilgenius.net>,
Alice <alice@wonderland.org>

key 8889FDFC1248AE44: public key "Derpy <derpy@ponymail.com>"
was signed by:
Hulk_ <hulk@biggreen.cc>,
Charlie <charlie@moderntimes.com>,
Alice <alice@wonderland.org>

key 7EAAC9BE837250A6: public key "Eve__ <eve@evilgenius.net>"
was signed by: none

key 0D789E34A52F024F: public key "Flash <flash@starlabs.com>"
was signed by:
Derpy <derpy@ponymail.com>,
Charlie <charlie@moderntimes.com>

key C2DFB3AD67855F6E: public key "Hulk_ <hulk@biggreen.cc>"
was signed by:
Eve__ <eve@evilgenius.net>,
Bob__ <bob@krustykrab.com>,
Flash <flash@starlabs.com>
```

```
key 0CA5C63A31C0D0C9: public key "Garfield <garfield@catnip.com>"
was signed by: Eve__ <eve@evilgenius.net>
```



(b)

Messages:

- msg0 good signature by Garfield $< garfield@catnip.com >$
- msg1 good signature by Hulk_ $< hulk@biggreen.cc >$
- msg2 bad signature by Flash $< flash@starlabs.com >$
- msg3 good signature by Derpy $< derpy@ponymail.com >$
- msg4 good signature by Eve__ $< eve@evilgenius.net >$

is Alice trustings:

- msg0 no
- msg1 yes, because of Alice $\rightarrow$ Bob$_{--}$ $\rightarrow$ Hulk$_{-}$
- msg2 yes, because of Alice $\rightarrow$ Derpy $\rightarrow$ Flash
- msg3 yes, because of Alice $\rightarrow$ Derpy
- msg4 no