8 Assignment (10+2 Points)

Hinweis:	Abgabe in $\{2, 3, 4\}$-er Gruppen.
Abgabe:	**17.06.2017, 23.59**
Email:	Betreff “[Compsec] Ex 8’
	(bitte nur .pdf oder .txt, kein .doc, .jpeg, etc)
	Source code: bitte inkl. `signify` Signatur

Exercise 25 (HRU Model (Access Control Matrix) (**4 Points**))**.**
In class we modeled the primitive actions `create subject` s, `destroy subject` s and `enter` r `into` s, o using preconditions and postconditions. Model the remaining primitive actions

1. `create object` o,
2. `destroy object` o, and
3. `delete` r `from` s, o

in the same way. **Solution:**

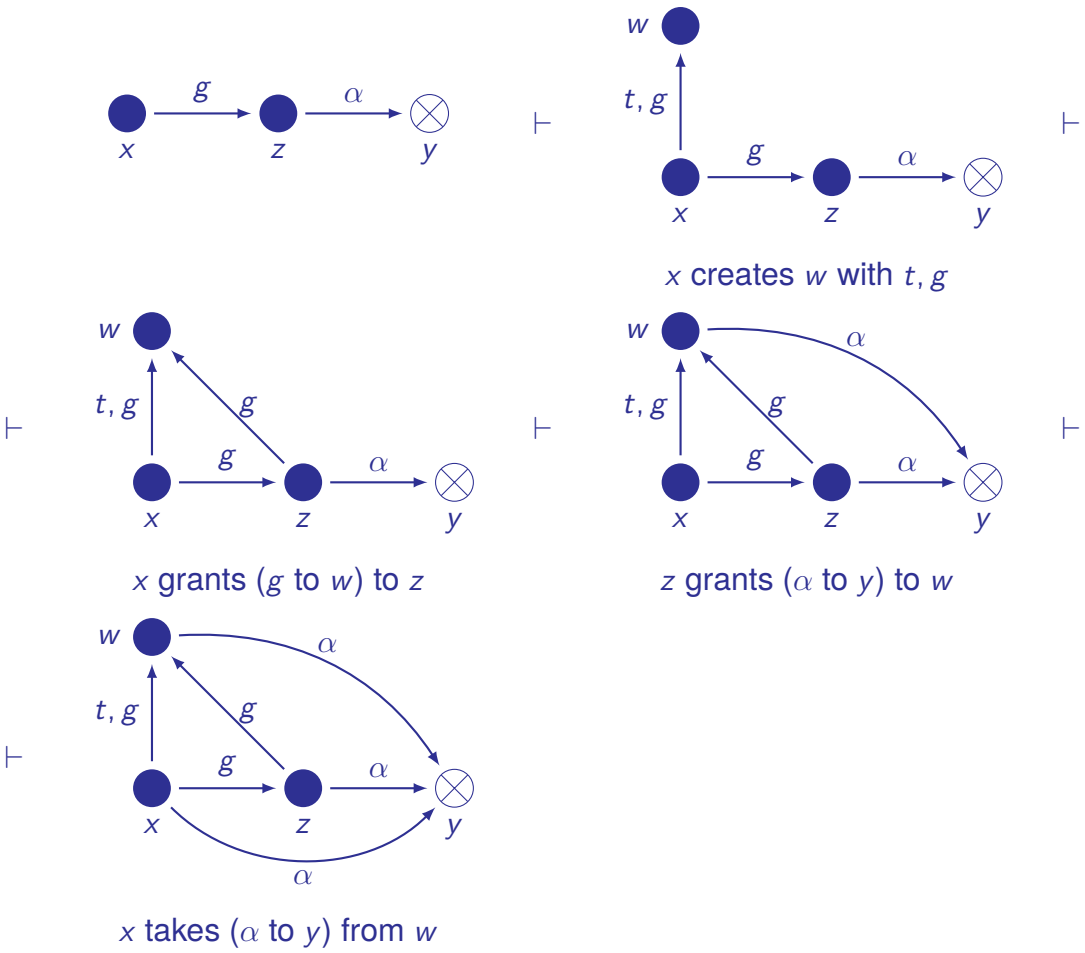
$$\frac{o \notin O \qquad \texttt{create object } o}{O' = O \cup \{o\}, S' = S}$$
$$s' \in S, o' \in O \Rightarrow M'(s', o') = M(s', o')$$
$$s' \notin S \Rightarrow M'(s', o') = \emptyset$$
$$o' \notin O \Rightarrow M'(s', o') = \emptyset$$

$$\frac{o \in O, o \notin S \qquad \texttt{destroy object } o}{O' = O \setminus \{o\}, S' = S}$$
$$s' \in S, o' \in O' \Rightarrow M'(s', o') = M(s', o')$$
$$s' \notin S' \Rightarrow M'(s', o') = \emptyset$$
$$o' \notin O' \Rightarrow M'(s', o') = \emptyset$$

$$\frac{s \in S, o \in O, r \in R \qquad \texttt{delete } r \texttt{ from } s, o}{S' = S, O' = O}$$
$$M'(s, o) = M(s, o) \setminus \{r\}$$
$$s \neq s', o \neq o' \Rightarrow M'(s', o') = M(s', o')$$

Exercise 26 (Take-grant protection model (**3 Points**))**.**
Prove that, in the Take-Grant Protection Model, it holds that:

Solution:



Exercise 27 (Case study μ-`shout` (v): Firewall Rules (**3 Points + 1 Bonus**))**.**
We used privilege dropping and a chroot in Exercise 22 to limit the amount of damage an attacker can do on our system once μ-shout is exploited. We now want to limit the amount of damage an attacker can do to *other* systems. For

example: your μ-shout server could be used as part of a botnet in a denial of service attack.

Have a look at OpenBSDs firewall documentation in `pf.conf(5)` and `pfctl(8)`. Configure your firewall so that

- any blocked communication will be logged
- incoming connections are only allowed to
  - port 22 (ssh).
  - to your `ushoutd` daemon running as the `_ushoutd` user
- no outgoing connections are allowed

Bonus: You may want to update your server and/or install new packages once in a while. Add rules that allow the installation of new packages and syspatch.

Solution:

```
block in log
# allow ssh (port 22)
pass in proto tcp to port 22
# allow _ushoutd daemon on any port
pass in proto tcp user _ushoutd

block out log
# package installs and system updates are privilege
# separated, makeing use of these two users:
pass out proto {udp,tcp} user _pkgfetch
pass out proto {udp,tcp} user _syspatch
```

Exercise 28 (Keeping your systems secure (**Bonus: 1 Points**))**.**
Are there any new vulnerabilities for your Debian or OpenBSD system since last week (10.06.2016 at 23.59)? If so: state one, **name the programming mistake**, decide if you are affected or not, and report if there are any known work-arounds or patches.