9 Assignment (11+1 Points)

Hinweis:	Abgabe in $\{2, 3, 4\}$-er Gruppen.
Abgabe:	**24.06.2017, 23.59**
Email:	Betreff "[Compsec] Ex 9'
	(bitte nur .pdf oder .txt, kein .doc, .jpeg, etc)
	Source code: bitte inkl. `signify` Signatur

Exercise 29 (Chinese wall and Bell-La Padula model **(4 Points)**).
The following composition of objects in the BLP model was derived from a set of objects in the Chinese wall model according to [1]. Sketch the original composition of objects in the Chinese wall model.

1 & 0	(A,f)	2 & 0	(B,z)	3 & 0	(C,t)	4 & 0	(D,f)
5 & 0	(A,g)	6 & 0	(B,f)	7 & 0	(C,e)	8 & 0	(D,l)
9 & 0	(A,h)	10 & 0	(B,l)	11 & 0	(C,p)	12 & 0	(D,k)
13 & 0	(A,i)	14 & 0	(B,m)	15 & 0	(C,q)	16 & 0	(D,j)
(X_0, Y_0)							

[1] David F.C. Brewer and Dr. Michael J. Nash, *The Chinese wall security policy*, IEEE Symposium on Security and Privacy, 1989.

Exercise 30 (Undecidability of the general halting problem **(4 points)**).
Consider the representation of a Turing machine as a protection system as discussed in class.

- Specify the missing commands for the head moving right: $\delta(q, X) = (p, Y, R)$
- Given the access matrix below, show the matrix that results after the following two moves:
  1. $\delta(q, C) = (p, D, R)$
  2. $\delta(p, D) = (s, E, R)$

A	B	⇓ C	D	ϕ	...

A	*own*		
	B	*own*	
		C q	*own*
			D END

Exercise 31 (More Hello World (**1+2 Points**))**.**
Port your hello world program from exercise 18 to linux for your debian VM. Then consider the following C program:

```
char* hello = "hello_world!\n";
typedef void (*fn_ptr)(void);

void bar(void){
  printf("does not do anything\n");
}

void foo(void){
  char buffer[1024];
  fn_ptr func = bar;
  if(read(0, buffer, 1024) > 10)
    func = (fn_ptr) buffer;
  func();
}
int main(){
  foo();
  return 0;
}
```

Compile this program with `gcc -g -Wl,-z,execstack`. Then give an input string that does not crash this program and makes it print `hello_world!` in your debian VM.

Note: You are allowed to disable memory randomization in your debian VM (if needed) using `echo 0 | sudo tee /proc/sys/kernel/randomize_va_space`.

Exercise 32 (Keeping your systems secure (**Bonus: 1 Points**))**.**
Are there any new vulnerabilities for your Debian or OpenBSD system since last week (17.06.2016 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.