Opgave 1: Fundamental concepts (5 punten)

Een computersysteem wordt besmet met spyware in de vorm van een keystroke logger waarmee eavesdropping wordt gepleegd. Is dit erop gericht om de confidentialiteit, de integriteit of de availability van het computersysteem aan te vallen? Licht uw antwoord toe.

Opgave 2: Access control (5 punten)

Wat zijn de voor- en nadelen van access control met behulp van access control lists?

Opgave 3: Elementary cryptography (15 punten)

a. (5p) Het Vigenèrecijfer is een polyalfabetisch substitutiecijfer. Gebruik dit cijfer (eventueel met behulp van onderstaand tableau) om de klare tekst 'ddosattack' te vercijferen waarbij de sleutel 'pinda' wordt toegepast. Hoe luidt de cijfertekst?

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

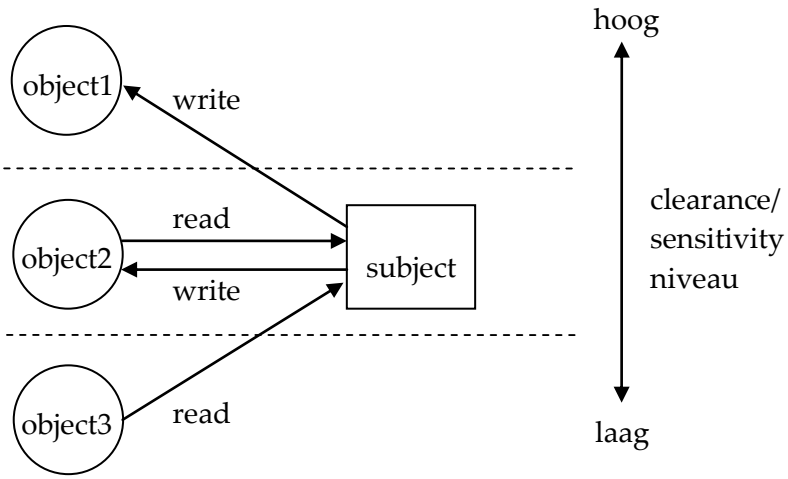
b. (5p) Publieke-sleutel-cryptografie kan worden toegepast om een bericht te voorzien van een digitale handtekening. Hoe genereert de afzender van het bericht deze digitale handtekening, en hoe kan de ontvanger van het bericht de digitale handtekening verifiëren?

c. (5p) Het Diffie-Hellmanprotocol kan worden toegepast om een geheime sleutel uit te wisselen? Hoe kan een man-in-the-middle-aanval dit ondermijnen?

Opgave 4: Operating systems security (15 punten)

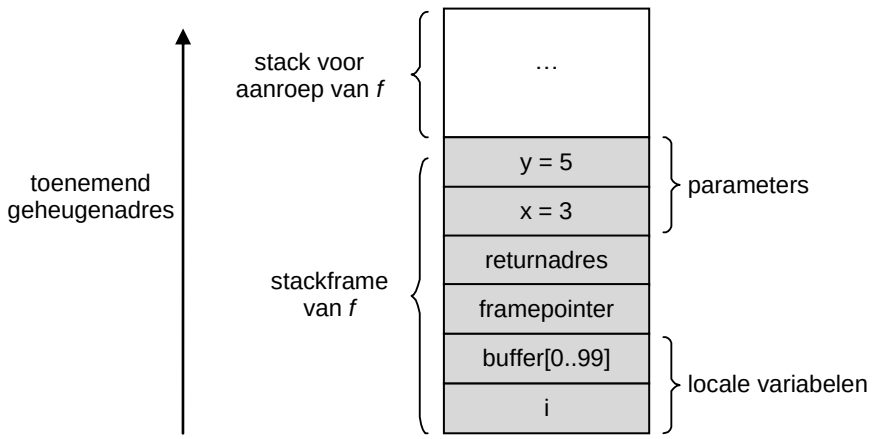
a. (5p) In de file permissie van een bestand dat programmacode bevat, kan het setuid-bit worden gezet. Wat is het doel van dit setuid-bit? Geef ook een voorbeeld waarin dit setuid-bit zinvol toegepast wordt.

b. (5p) Een subject mag objects (bv. documenten) lezen en schrijven volgens onderstaande figuur.



Leg uit of deze figuur in overeenstemming is met het Bell-LaPadula-model of het Biba-model.

c. (5p) In onderstaande figuur wordt de stack van een C-programma weergegeven na aanroep van een functie *f*. In deze functie wordt de gebruiker gevraagd om via het toetsenbord een reeks karakters in te tikken, die in het array *buffer* worden opgeslagen.



Leg uit hoe de gebruiker kwaadaardige code kan injecteren (bestaande uit 150 bytes) en ervoor kan zorgen dat deze code vervolgens ook wordt uitgevoerd.

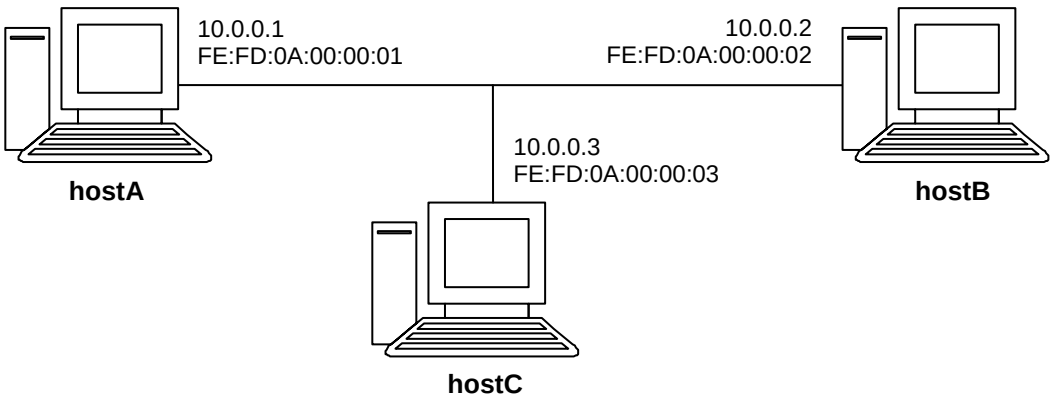
Opgave 5: Malware (10 punten)

a. (5p) Wat is een polymorphic virus en hoe kan een virusscanner zo'n polymorphic virus detecteren?

b. (5p) Hoe kunnen cryptografische hashfuncties worden ingezet om systeembestanden te beschermen tegen malware?

Opgave 6: Network security (25 punten)

a. (5p) Onderstaande figuur toont een netwerk waarop hostA, hostB en hostC zijn aangesloten. In de figuur worden de IP-adressen en MAC-adressen van de gebruikte netwerkinterfaces vermeld.



Op een bepaald moment is de inhoud van ARP-tabellen op deze hosts als volgt.

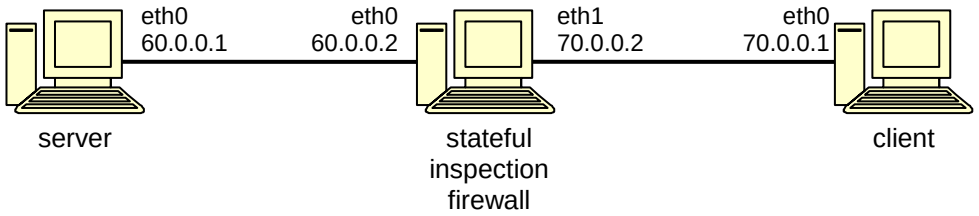
ARP-tabel van hostA:	10.0.0.2	FE:FD:0A:00:00:02
	10.0.0.3	FE:FD:0A:00:00:02
ARP-tabel van hostB:	10.0.0.1	FE:FD:0A:00:00:01
	10.0.0.3	FE:FD:0A:00:00:03
ARP-tabel van hostC:	10.0.0.1	FE:FD:0A:00:00:02
	10.0.0.2	FE:FD:0A:00:00:02

Vindt er een man-in-the-middle-aanval plaats? Licht uw antwoord toe.

b. (5p) Hoe verloopt een blind injection aanval met behulp van TCP sequence prediction?

c. (5p) Hoe kunnen SYN cookies helpen om een SYN flood attack te vermijden?

d. (5p) Onderstaande figuur toont een netwerk in het virtuele lab. De stateful inspection firewall filtert de communicatie tussen de server en de client en is met behulp van de tool iptables geïmplementeerd.



Onderstaande figuur toont de configuratie van de firewall.

```
Chain INPUT (policy DROP)
Num  target   prot   in    out    source      destination
1    ACCEPT   all    lo    *      0.0.0.0/0   0.0.0.0/0

Chain FORWARD (policy DROP)
Num  target   prot   in    out    source      destination
1    ACCEPT   all    eth1  *      0.0.0.0/0   0.0.0.0/0
2    ACCEPT   all    eth0  *      0.0.0.0/0   0.0.0.0/0  state RELATED,ESTABLISHED
```

Wat is het doel van rule 2 in de forward chain?

e. (5p) Waarom moet rekening gehouden worden met de base-rate fallacy bij het interpreteren van de false-alarm rate van een intrusion detection system?

Opgave 7: Web security (5 punten)

Hoe kan een aanvaller SSL-stripping toepassen om gebruik van HTTPS tussen een webserver en een client te omzeilen?

Opgave 8: Database security (5 punten)

Access control permissies in een database kunnen via grants van de ene aan de andere gebruiker worden doorgegeven. De onderstaande figuur toont toekenningen voor een privilege P en bijbehorende timestamps.

Grantor	*Grantee*	*Privilege*	*Timestamp*
Bob	*Carol*	*P*	*1*
Bob	*Alice*	*P*	*2*
Carol	*Ted*	*P*	*3*
Ted	*Charles*	*P*	*4*
Alice	*Ted*	*P*	*5*
Ted	*Diana*	*P*	*6*
Charles	*Camilla*	*P*	*7*

Welke gebruikers raken hun privilege kwijt wanneer Alice haar toekenning aan Ted intrekt op timestamp 5?

--- einde ---