
Authorization (Access control)

Identify

- Assets – (inventory system, asset management)
- Potential threats – (threat modeling, risk assessment)

Prevent

- Block attacks – (authentication, access control, encryption, firewall)
- Reduce vulnerabilities – (static/dynamic code analysis, software updates, vulnerability penetration testing)

Detect

- When an incident happens or shortly after – (monitoring systems, logs, malware scan, intrusion detection systems, integrity checksums/hashes, digital signatures)

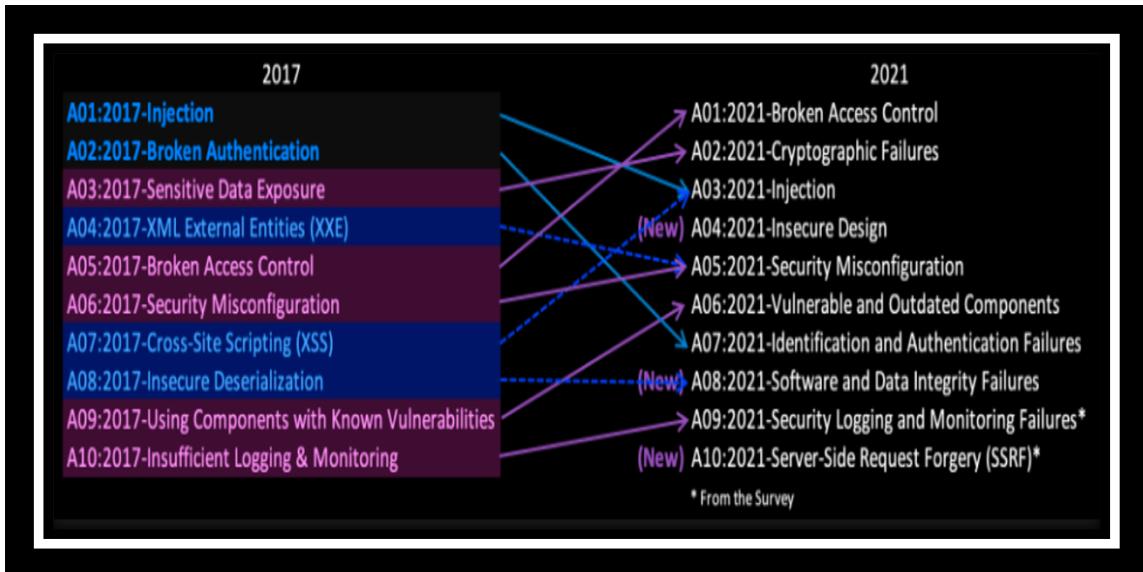
Respond

- Be able to respond to stop attacks and prevent further damage – (intrusion prevention systems, shutting down and rebuilding the system)

Recover

- Correct copy of the data can be reloaded from backup

Når et system vet hvem en bruker er gjennom autentisering, vil autorisasjon være hvordan systemet bestemmer hva brukeren kan gjøre. Eks er user eller root, student eller lærer.



Hvorfor autorisering er viktig er også knyttet opp med personopplysningsloven hvor det er lovpålagt å sikre tilgang til informasjon.

Personopplysningsloven

- **Lovpålagt å sikre tilgang til informasjonen**
 - Artikkels 32. Sikkerhet ved behandlingen
 - Art. 32 EU. General Data Protection Regulation (GDPR). Security of processing

Art. 32 GDPR

Lov om behandling av personopplysninger (personopplysningsloven)

EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforskrift) [PVF, GDPR]

KAPITTEL IV Behandlingsansvarlig og databehandler

Avsnitt 2 Personopplysningssikkerhet

Artikkels 32. Sikkerhet ved behandlingen

1. Med det har henvi til den tekniske teknologien, personopplysningslovene og bestemmelser om, omfang, formål og sammenhengen med annen. Lært risikoen av varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og frihet, skal den behandlingsansvarlige og databehandleren gjennomføre spesielle tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med henvis til risikoen, herunder blant annet, at etter hva som er egnet,

- a) prosess for personvern og kryptering av personopplysninger
- b) en sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -prosesse
- c) en gjenopprettelig tilgang til opplysningene i tilfelle dersom det oppstår en teknisk eller teknisk hendelse
- d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingsens tekniske og organisatoriske sikkerhetsnivå er.

2. Ved utviklingen av egnet sikkerhetsnivå skal det samtidig tas hensyn til risikene forbundet med behandlingen, samtidig som følge av utviklet eller jobbdrevet teknologi, lag, endring eller ikke-autorisert tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

3. Overhodelet av godkjente tilhører som nevnt i artikkels 40 eller en godkjent verifiseringsmekanisme som nevnt i artikkels 42 kan brukes som et faktor til å påvirke til krasjene i nr. 11 denne artikkelen er oppfylt.

4. Den behandlingsansvarlige og databehandleren skal tilrette bla. til å sikre at enhver trykk person som handlar for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, beholder samme opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre utspesifisert eller medvetsstilles nøyaktig net krever at vedkommende gjør dette.

Personopplysningsloven - Artikkels 32. Sikkerhet ved behandlingen

Sikkerhetsloven:

The screenshot shows a slide with a blue header bar containing the text "Sikkerhetsloven". Below this, a large white box contains a bullet point: "► Lovpålagt å sikre tilgang til Skjermingsverdige informasjon/informasjonssystemer". To the right of this box is a vertical sidebar with legal text. At the top of the sidebar is the title "Lov om nasjonal sikkerhet (sikkerhetsloven)" and "Kapittel 6. Informasjonssystemsikkerhet". Below this are two sections: "§ 6-1. Skjermingsverdige informasjonssystemer" and "§ 6-2. Beskyttelse av skjermingsverdige informasjonssystemer". The text in these sections discusses the protection of sensitive information systems, mentioning obligations for companies to protect such systems and the state's role in identifying them. At the bottom of the sidebar, a red link reads "Sikkerhetsloven - § 6-2.Beskyttelse av skjermingsverdige informasjonssystemer".

UTFORDRINGER MED AUTORISERING

Som datamaskiner blir bedre forstått og mer økonomiske, bringer hver dag nye anvendelser. Mange av disse nye anvendelsene innebærer både lagring av informasjon og samtidig bruk av flere individer. For de anvendelsene der ikke alle brukere skal ha identisk myndighet, trengs det en ordning for å sikre at datamaskinsystemet implementerer den ønskede myndighetsstrukturen.

SECURITY DESIGN PRINCIPLES

I artikkelen "The protection of information in computer systems" fra 1975:

Saltzer og Schroeder var de første til å foreslå «Sikkerhetsdesign prinsipper»:

1. Økonomi i mekanismen
 - Hold designet så enkelt og lite som mulig ("Kompleksitet er fienden til sikkerhet").
2. Feilsikre standardinnstillinger / Sikre standardinnstillinger
 - Basert tilgangsbeslutninger på tillatelse i stedet for utelukkelse ("Nekt med mindre det er uttrykkelig autorisert").
3. Fullstendig mediering
 - Hver tilgang til hvert objekt må sjekkes for godkjenning.
4. Åpen design
5. Psykologisk akseptabilitet
6. Minst privilegium

- Hver programvare og hver bruker av systemet skal operere med det minste settet med privilegier som er nødvendig for å fullføre oppgaven.

7. Skillelse av plikter

- To eller flere betingelser må oppfylles før tilgang skal tillates.

8. Minst felles mekanisme

- Minimer mengden av mekanismen som er felles for mer enn én bruker og avhengig av alle brukere. Minimer avhengigheter og alt slik at hvis tilgang til en del av systemet nås, er det like vanskelig å få tilgang til mer i systemet.

LEAST PRIVILEGE

Dette prinsippet hevder at en bruker eller et program kun burde få utdelt de privilegiene som trengs for at jobben kan gjøres. Man bør ikke ha tilgang eller autoritet til det som er irrelevant for en selv.

SEPARATION OF DUTY

Sikkerhets prinsipp som brukes til å formulere fler-person kontroll policier, som krever at to eller flere personer er ansvarlige for å fullføre en oppgave eller et sett med oppgaver som henger sammen. Hensikten med dette prinsippet er å demotivere svindel ved å dele ansvar og autoritet for en handling eller oppgave over flere personer, som derfor kan minske risikoen for fare.

ACCESS CONTROL

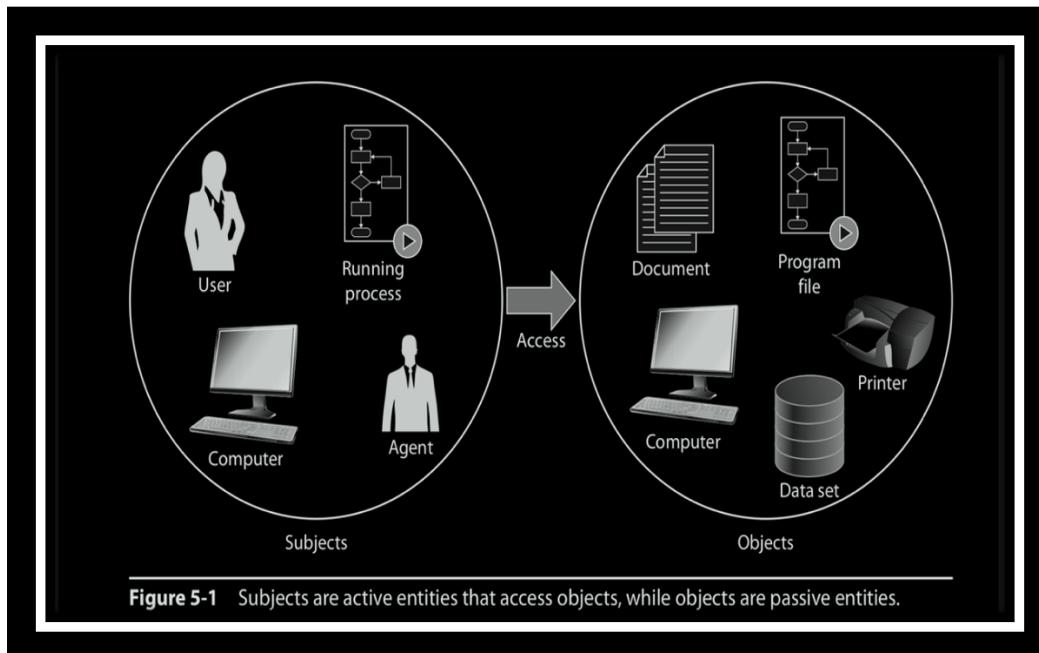
Hvordan kan vi sikre at autorisasjon kun utdeles til legitime brukere?

Gjennom access control som er en mekanisme til å beskytte ressurser/eiendeler.

Det grunnleggende designet for tilgangskontroll-systemet består av:

- Subject:
 - Som er en aktiv entitet som forespør tilgang til et objekt eller data i systemet
- Object:
 - Som er et passivt komponent som inneholder informasjon eller nødvendig funksjonalitet som trengs for å beskytte mot uautorisert bruk
- Access:

- Som er informasjonsflyten mellom subjekt (bruker, prosess, maskin) og objekt (fil, mappe, database og nettverk).



ACCESS CONTROL MODELS

En tilgangskontroll-modell er et rammeverk som definerer hvordan subjekter får tilgang til objekter. Det finnes flere typer av disse:

i. **Mandatory access control (MAC)**

Brukes mest I miljøer der det kreves høy/streng sikkerhet slik som i militæret.

MAC er en tilgangskontroll-service som styrker en sikkerhets-policy på å sammenlikne (A) security labels, noe som indikerer hvor sensitivt eller kritisk systemressurser er, med (B) sikkerhets clearances, noe som indikerer at system entiteter er gode nok til å ha tilgang til ressursene det er snakk om.

Dette heter obligatorisk tilgangskontroll fordi en entitet har ingen tilgang uten grunn til andre deler av ressurser eller systemer.

ii. **Discretionary Access Control (DAC)**

Brukes mest av operasjonssystemer (Linux, Windows and Mac/Unix)

iii. **Role-based access control (RBAC)**

Brukes mest av applikasjoner (databases, web applications)

iv. Attribute-Based Access Control(ABAC)

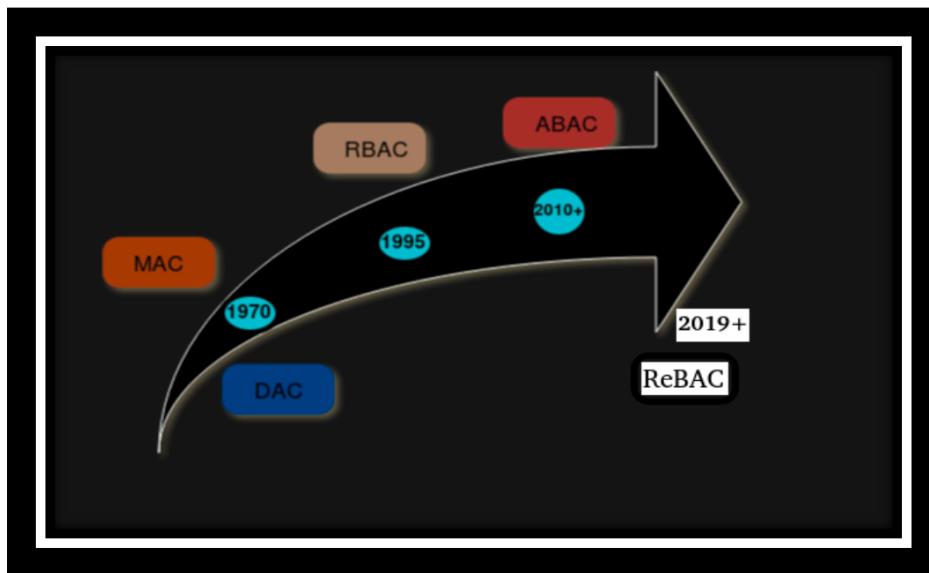
ABAC er en ny tilgangskontroll modell siden 2010+ fra NIST

ABAC er ennå ikke implementert i operasjonssystemer eller av mange applikasjoner

v. Relationship Based Access Control (ReBAC)

ReBAC er en ny modell fra 2019 basert på Zanzibar - Google's Consistent, Global Authorization System

ReBAC er ennå ikke implementert i operasjonssystemer eller av mange applikasjoner



Role-Based vs Attribute-Based vs Relationship-Based

RBAC – bruker roller som er tagget til brukere. Titler tagget til roller.

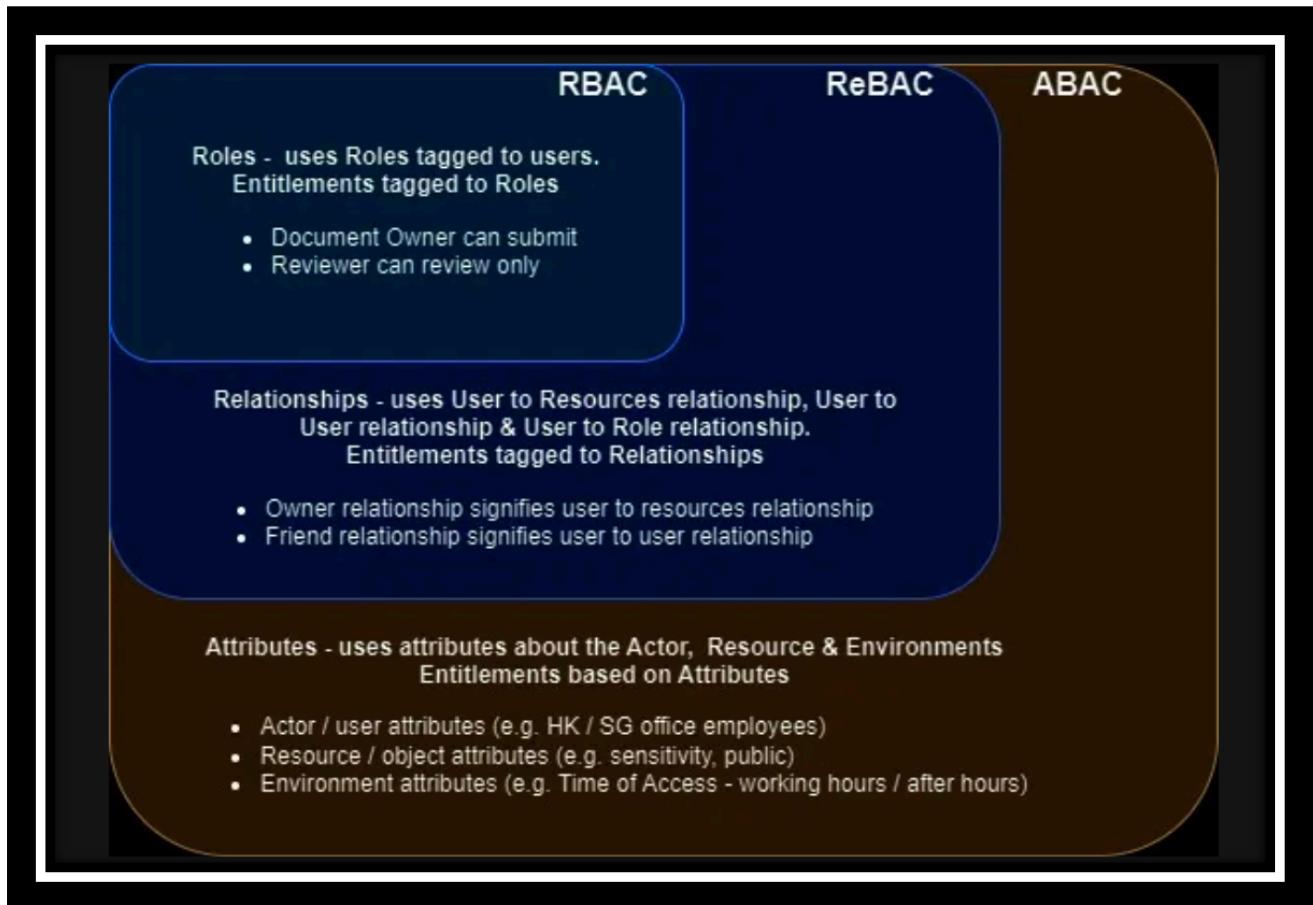
- Document eier kan leve
- En som er reviewer kan bare reviewe

ReBAC – titler tagget til forhold

- Eier forhold signifies bruker til ressurs forhold
- Venn forhold signifies bruker til bruker forhold

ABAC – titler basert på attributter

- Skuespiller / bruker attributter (HK / kontor ansatte)
- Ressurser / objekt attributter (sensivitet, offentlig)
- Miljø attributter (time of access – arbeidstimer / after hours)



MER OM MAC

MAC er en sikkerhetsstrategi som limiterer evnen til en individuell ressurs eiere til å tillate, eller nekte, tilgang til ressurs objekter i et filsystem. Tilgang (access) er definert av en sentral autoritet (policy) og er obligatorisk. MAC kontrollerer tilgang basert på et sett med klassifikasjoner som indikerer hvor sensitivt eller kritisk system ressurser er (f eks topp hemmelig, hemmelig, confidential og klassifisert) som infører hvem som fyller kravene på tilgang til ressursene det er snakk om.

I tillegg til klassifikasjoner bruker MAC et subset med kategorier som kalles sikkerhetsnivåer (f eks topp hemmelig, hemmelig, confidential og klassifisert).

Alle ressurser som trenger å sikres får en label som sier hvilken klassifikasjons-nivå du trenger og hvilket nivå med sikkerhet som den burde ha. MAC brukes mest av operasjonssystemer som behøver høy/streng sikkerhet.

MER OM DAC

De fleste operasjonssystemer, inkludert Linux, bruker tilgangskontroll basert på DAC. DAC kontrollerer tilgang til ressurser ved å begrense tilgang basert på identiteten til subjektet (eieren) og grupper. Eieren av en ressurs har valg bestemmende autoritet over hvem andre som kan ha tilgang til ressursen. I andre ord kan vi si at eieren bestemmer rettighetene til andre.

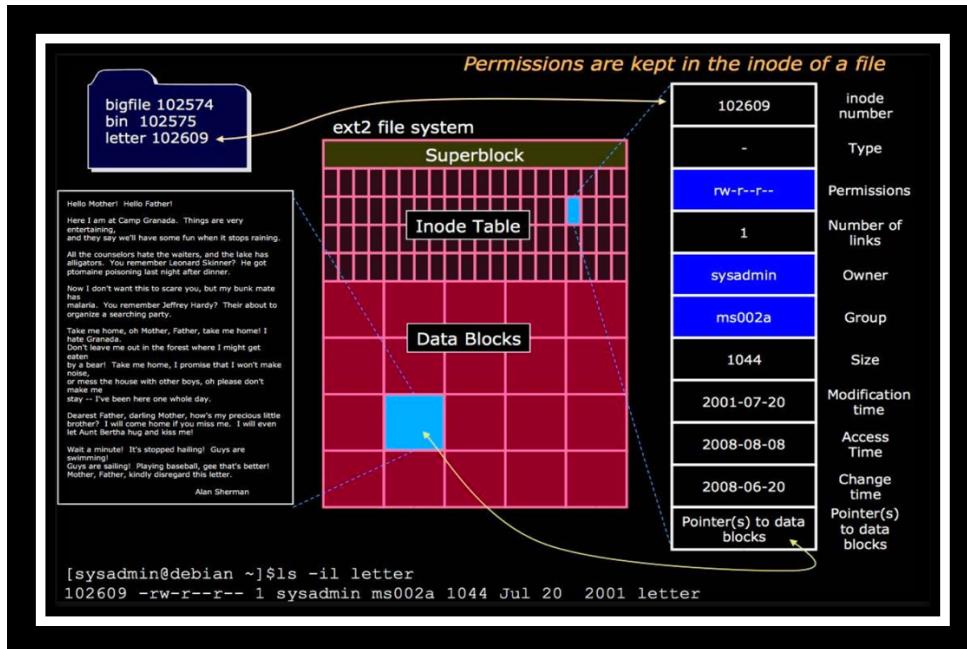
Hvordan kontrollerer tilgang til ressurser (filer og mapper) i DAC?

Gjennom tilganger. Hvilke tilganger kan vi sette? Read, write og execute. Hvem er det disse gjelder? Eier, gruppe og alle andre.

```
msysadmin@ismail:~/itpe3100/Lecture-5$ ls -l
total 44
drwxrwxr-x 2 msysadmin itpe3100 4096 okt. 10 09:39 auth
drwxrwxr-x 2 msysadmin itpe3100 4096 okt. 10 09:38 dir1
drwxrwxr-x 2 msysadmin itpe3100 4096 okt. 10 09:38 dir2
-rw-rw-r-- 1 msysadmin itpe3100 6 okt. 10 09:40 fil1.txt
-rw-rw-r-- 1 msysadmin itpe3100 48 okt. 10 09:40 fil2.txt
-rw-rw-r-- 1 msysadmin itpe3100 12 okt. 10 09:40 fil3.txt
-rw-rw-r-- 1 msysadmin itpe3100 17119 okt. 10 09:26 lec5.tex
```

Permissions Owner Group

Under er det filsystemer og inode (OS administrativt overblikk).



Under er det inode informasjon:

```
msysadmin@ismail:~/itpe3100/Lecture-5$ ls -li fil2.txt
280813 -rw-rw-r-- 1 msysadmin itpe3100 48 okt. 10 09:40 fil2.txt
msysadmin@ismail:~/itpe3100/Lecture-5$ stat fil2.txt
  File: 'fil2.txt'
  Size: 48          Blocks: 8          IO Block: 4096   regular file
Device: 802h/2050d  Inode: 280813      Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/msysadmin)  Gid: ( 1001/itpe3100)
Access: 2016-10-10 09:38:05.230760513 +0200
Modify: 2016-10-10 09:40:32.098756165 +0200
Change: 2016-10-10 09:44:09.970749715 +0200
 Birth: -
```

Filrettigheter i binær:

Decimal	Binary
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

The permissions on letter are `rw-r--r--` or 644
 owner has read and write
 group has only read
 others have only read

`110 (binary) = 6 (decimal)`
`100 (binary) = 4 (decimal)`

inode number	102609
Type	-
Permissions	<code>rw-r--r--</code>
Number of links	1
Owner	sysadmin
Group	ms002a
Size	1044
Modification time	2001-07-20
Access Time	2008-10-15
Change time	2008-10-15
Pointer(s) to data blocks	

LESE 4

SKRIVE 2

KJØRE 1

ACCESS CONTROL LIST (ACL)

Tilgangskontroll med ACL gir oss muligheten til å dynamisk endre rettigheter til eiere, brukere og grupper, og uten ACL kan en fil eller mappe kun ha en eier eller en gruppe som eier. Det vil ikke uten ACL være mulig å arve rettigheter.

I Linux brukes kommandoene `setfacl` og `getfacl` til å se på og sette ACL-er:

1. `getfacl` kommandoen viser filens nåværende ACL
2. `setfacl` kommandoen modifiserer eller setter den

Filer med ACL-er opprettholder deres originale mode bits, men “consistency is automatically enforced, and the two sets of permissions can never conflict”.

FILRETTIGHETER FØR OG ETTER ACL

```
debian:/adm1# setfacl -d -m g:ms002a:rwx,g:sysadmin:rx students
debian:/adm1# getfacl students
# file: students
# owner: root
# group: root
user::rwx
group::r-x
group:ms002a:rwx
mask::rwx
other::r-x
default:user::rwx
default:group::r-x
default:group:sysadmin:r-x
default:group:ms002a:rwx
default:mask::rwx
default:other::r-x
```

Format	Example	Sets permissions for
user::perms	user::rw-	The file's owner
user:username:perms	user:trent:rw-	A specific user
group::perms	group::r-x	The group that owns the file
group:groupname:perms	group:staff:rwx	A specific group
other::perms	other::---	All others
mask::perms	mask::rwx	All but owner and other ^a

UTFORDRINGER MED DAC OG ACL

Det er noen utfordringer med DAC og ACL:

- Når noe endrer seg, for eksempel rettighetene til en bruker, da må system administrator gå gjennom alle filene som brukeren har tilgang på, legge til eller fjerne rettigheter.

Sikkerhets featurene er ikke spesifikke nok og mangler en måte for å styrke den minste privilegien på.

- Alle programmer som kjøres av en bruker har tilgang på alt brukeren har tilgang på.
 - o Så hvis brukeren har evnen til å slette dems egen musikk bibliotek, kan en VCL spiller også slette dem.
 - o Hvis en bruker kan lese dems egne bank eller skattefiler, kan flash-plugins i FireFox også.

MER OM RBAC

- Tilgangskontroll-modell proposed i 1992
- Presentert som et alternativ for MAC og DAC
- En viktig feature i RBAC er at all tilgang er allokkert gjennom roller

RBAC er en form for identitets-basert tilgangskontroll hvor system entities er identifisert og kontrollert er funksjonelle posisjoner i en organisasjon eller en prosess. Administratorer deler ut tilgang til roller som det trengs for å utføre funksjoner i systemet. Administratorer utdeler individuelt identiteter til roller.

MER OM RBAC

- I. RBAC kontrollerer tilgang til ressurser basert på utdelte roller i en organisasjon.
- II. En rolle kan sees på som en samling av oppgaver, en person eller en gruppe mennesker som kan gjøre noe i en organisasjon.
- III. Tilgangen er snettalt kontrollert av en sikkerhets policy som er definert av management.
- IV. RBAC kan ha eller utføre noen discretionary eller mandatory elementer
 - a. RBAC er mest brukt av applikasjoner som databaser og webapplikasjoner

Eksempler på roller i Canvas: student, lærer, foreleser, TA, kurs-designer og observatør.

BEGRENSNINGER VED RBAC

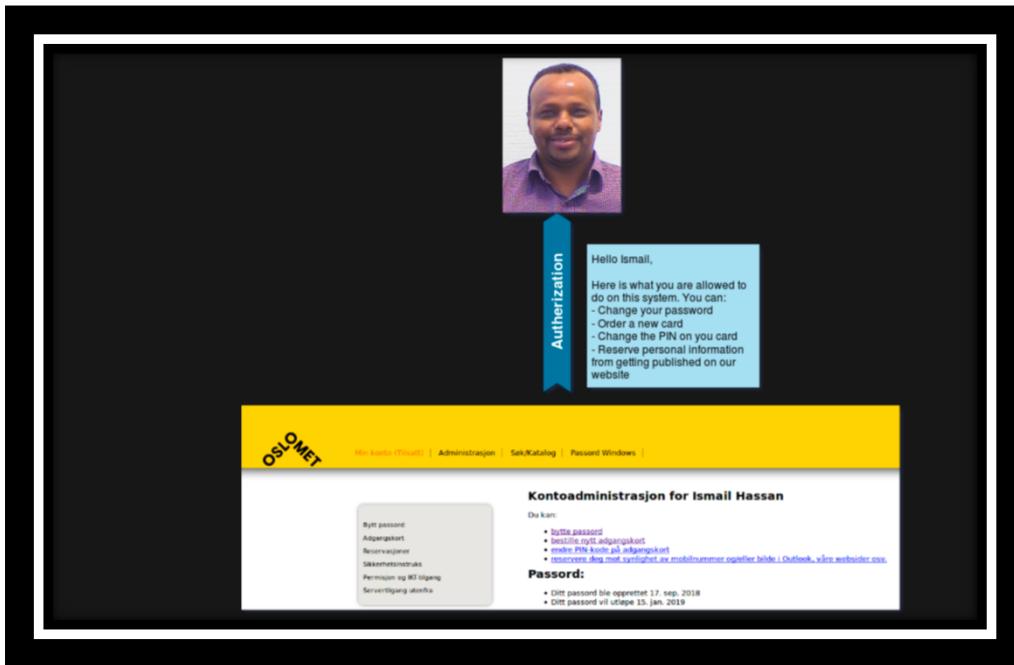
- RBAC antar at alle rettigheter som trengs for en jobb kan være «neatly encapsulated». Faktisk, har rolle ingenør blitt en vanskelig oppgave.
 - o Utfordringen for RBAC er konflikten mellom trengselen for en sterk sikkerhet og enklere adminstrasjon. For sterkere sikkerhet er det bedre for hver rolle å være spesifikk og dermed ha flere roller per bruker. For enklere adminstrasjon er det bedre å ha færre roller å håndtere.
- The least privilege condition er ofte vanskelig eller dyrt å oppnå fordi det er vanskelig å skreddersy tilgang basert på varierte attributter.
 - o Brukere kan lett akkumulere roller som leder til flere tilganger enn det de egentlig trenger, noe som er brudd på least privilege condition
- RBAC har begrenset støtte for «separation of duty controls»
 - o I RBAC, prosessen for å lage en ny rolle, endre en rolle og muligens slette en rolle, er veldig kritisk. Separation of duty er derfor en utfordring hvis en ikke er forsiktig når rollene utdeles.
- RBAC har skalerbarhet problemer ofte referert som role explosion
 - o Mange organisasjoner hevder at maximum 10 roller per ansatt er grensen og alt over vil lede til rolle eksplosjon.

ACCESS CONTROL TECHNIQUES AND TECHNOLOGIES

Når en organisasjon har bestemt for typen access control modell de vil ha, må de da identifisere teknologiene og teknikkene tilgjengelig for å støtte access control modellen.

Det er ulike access controls og teknologier for å støtte de ulike modellene:

- Constrained user interfaces (begrenset brukergrensesnitt)
 - o Det er tre hovedtyper av begrenset brukergrensesnitt: menu, shell and database views
 - o Begrensende brukergrensesnitt begrenser brukernes tilgangsevner ved å ikke tillate dem å be om visse funksjoner eller informasjon, eller å ha tilgang til spesifikke systemressurser.



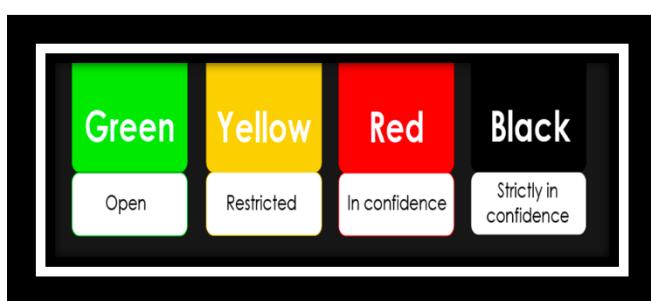
- Capability table
 - o Spesifiserer tilgangsrettigheter for et spesifikt subjekt til spesifikte objekter
 - o Spesifiserer rettigheter et subjekt har relatert til objekter
 - o Capability table er ulikt ACL fordi subjektet er bundet til capability table, hvor objektet er bundet til ACL
 - o Capability corresponds to the subject's row in the access control matrix

Capability Table for the subject Larry			
File 1	File 2	File 3	File 4
Read	Read, write	Read	Read, write
Capability Table for the subject Bob			
File 1	File 2	File 3	File 4
Full control	Full control	Full control	No access

- Access control list
 - o Liste over subjekter som har legitim tilgang til visse objekter og dems type autorisasjon
 - o ACL er brukt i flere OS, applikasjoner og ruter konfigurasjoner.
 - o De er lister med subjekter som er autorisert for å ha tilgang til spesifikke objekter, og de definerer nivå over autorisasjon tillat.
 - o Autorisering kan være spesifikt til et individ, gruppe eller rolle.
 - o ACL-er mapper verdier fra access control matric til objektet.

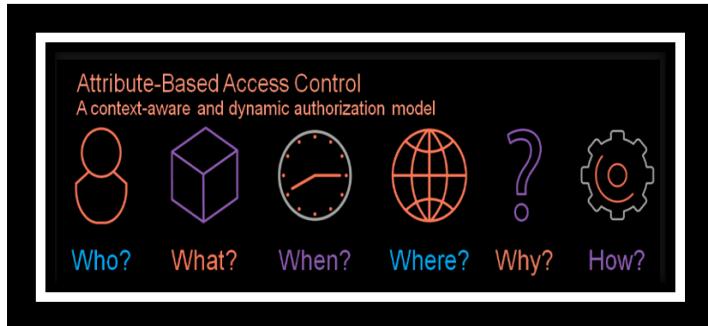
User	File1
Diane	Read and execute
Katie	Read and execute
Chrissy	Read, write, and execute
John	Read and execute

- Access control matrix
 - o Er en tabell med subjekter og objekter som indikerer hvilke handlinger subjekter kan utføre på hvilke objekter
 - o Se bildet under punktene
- Content-dependent access control
 - o Tilgang til objekter bestemt av innholdet (eks: unntatt fra offentligheten)



- Context-dependent access control
 - o Situational access (eks: statefull firewall)

- Tilgangsbeslutninger basert på konteksten til en samling av informasjon heller enn på sensiviteten til dataene
- Et system som bruker kontekstavhengig tilgangskontroll og «gjennomgår situasjonen» og så tar en avgjørelse



FORHOLD MELLOM ACM, CAPABILITY OG ACL

Access Control Matrix					
	Subject	File 1	File 2	File 3	File 4
Capability	Larry	Read	Read, write	Read	Read, write
	Curly	Full control	No access	Full control	Read
	Mo	Read, write	No access	Read	Full control
	Bob	Full control	Full control	Full control	No access

Capability = row in matrix
ACL = column in matrix

ACL

Tabellen er en access control matrix. Hver rad er capability og er knyttet til subjektet.

Hver kolonne er en ACL.

KLASSIFIKASJON AV INFORMASJON

- Informasjon må være prosessert og lagret i et lovlig og sikkert vis
- Retningslinjer burde være forberedt for hvordan informasjon burde være klassifisert basert på hva som trengs med tanke på beskyttelse etter risikovurdering
- Klassifisering av informasjon i Norge:
 - Lov om nasjonal sikkerhet (sikkerhetsloven)

- Klassifisering av informasjon og informasjonssikkerhet (UNIT)

KLASSIFISERING AV INFORMASJON I FORHOLD TIL SIKKERHETSLOVEN

The diagram illustrates the classification of information according to the Security Act. It features a central text box with a quote from the act, followed by four colored boxes representing different classification levels: BEGRENSET (blue), KONFIDENSIELL (orange), HEMMELIG (green), and STRENGT HEMMELIG (red). Each level is accompanied by its corresponding legal basis:

BEGRENSET Int. sikkerhetsloven §§ 5-3 og 5-4 jf. offentleglova § 13	KONFIDENSIELL Int. sikkerhetsloven §§ 5-3 og 5-4 jf. offentleglova § 13	HEMMELIG Int. sikkerhetsloven §§ 5-3 og 5-4 jf. offentleglova § 13	STRENGT HEMMELIG Int. sikkerhetsloven §§ 5-3 og 5-4 jf. offentleglova § 13
--	--	---	---

Source: NSM – Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon

I FORHOLD TIL UH SEKTORENS SEKRETARIAT FOR INFORMASJONSSIKKERHET

The diagram illustrates the classification of information according to the Security Act, similar to the one above. It includes a quote from the classification handbook and detailed descriptions of each level:

Konfidensialitetskasser
Konfidensialitetskassene beskriver grad av beskyttelse som kreves for informasjon.

Eksempler på informasjon hvor konfidensialiteten er viktig er helseopplysninger, eksamsoppgaver for de er gitt og forskningsresultater som ikke er publisert. Det er definert fire klasser for konfidensialitet. De tre lavest klassene Åpen og Fortrolig er de som oftest vil bli brukt. Kassene Fortrolig og Strengt fortrolig er harmonisert med Sikkerhetsinstruksen.

- **Åpen (Grunn):** Informasjon kan være tilgjengelig for alle uten særskilte tilgangsrettigheter.
- **Intern (Gul):** Eksempler på slik informasjon er en web-side som presenterer en avdeling eller enhet som legges åpent ut på internett eller studiematerialiell for et enne eller kurs som ligger åpent, men som er merket med en gitt lisens eller opphavsrett.
- **Intern (Gul):** Informasjonen må ha en viss beskyttelse og kan være tilgjengelig for både eksterne og interne, med kontrollerte tilgangsrettigheter. Benyttes dersom det vil kunne forårsake en viss skade for institusjonen, eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende.
- **Fortrolig (Rød):** Eksempler på slik informasjon er enkelte arbeidsdokumenter, informasjon som er unntatt offentlighet, personopplysninger, karakterer, store studentarbeider, eksamsbesvarelser, forskningsdata og -arbeider.
- **Fortrolig (Rød):** Benyttes hvis det vil forårsake skade for offentlige interesser, institusjonen, enkeltperson eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende. Informasjonen skal ha de stengste tilgangsrettigheter.

Hvis man har behov for et fjerde og høyere nivå for konfidensialitet kan man bruke klassen

- **Strengt fortrolig (Sort):** Gi øvre avgrensning mellom den og Fortrolig. Strengt fortrolig benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, institusjonen, enkeltperson eller samarbeidspartner at informasjonen blir kjent for uvedkommende. Informasjonen skal ha de stengste tilgangsrettigheter.

Eksempler på slik informasjon er informasjon om personer som har adressesperrere kode 7 eller som har behov for annen særlig beskyttelse og svært konfidensielle forskningsdata og -arbeider.

Noen institusjoner har informasjon som skal beskyttes etter beskyttelsesinstruksen eller sikkerhetsloven. Se kapittel 3 Standarder, lover og forskrifter for mer informasjon.

