Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

Del 8: IAM – Identitets- og tilgangshåndtering

Oppgave 1: IAM-begreper

a. Gi en kort forklaring på følgende begreper knyttet til identitetshåndtering.
   (i) Entitet
   (ii) Identitet
   (iii) Bruker-ID (identifikator, entydig navn)
   (iv) Digital identitet
   (v) Autentikator
b. Forklar kort hva som menes med begrepet "identitets- og tilgangshåndtering" IAM.

Løsningsforslag

a. Begrepenes betydning:
(i) Entitet: en person, organisasjon, aktør, system, prosess etc.
(ii) Identitet: et sett attributter for en entitet i et domene.
(iii) Bruker-ID (identifikator, entydig navn): et attributt som (entydig) peker på en identitet i et identitetsdomene/navnerom.
(iv) Digital identitet: identitet med attributter som representeres digitalt på en måte som er egnet for prosessering i datasystemer.
(v) Autentikator: Privat (hemmelig) element (informasjon, egenskap eller enhet) som gjør at brukeren kan bevise rettmessig eierskap av en bruker-ID
b. **Identitets- og tilgangshåndtering** er et fagområde i informasjonssikkerhet som fokuserer på teknologier som skal sørge for at kun de rette personer får tilgang til rette ressurser til rett tid for de rette grunnene.

Oppgave 2: Silo-modell og føderert modell

a. Beskriv kort silo-modellen for identitetshåndtering.
b. Beskriv fordeler og ulemper ved silo-modellen.
c. Beskriv generelt den føderterte modellen for identitetshåndtering.
d. Beskriv fordeler og ulemper ved den føderterte modellen.

Løsningsforslag

a. I silo-modellen er tjenestetilbyder (SP) og autentiseringstjener (IdP) samme entitet, slik at tjenestetilbyder ikke bare tilbyr tjenester, men også autentiserer hver bruker.
b. Fordeler og ulemper ved silo-modellen:
    - Fordeler for SP: enkelt å sette opp, lave oppstartskostnader,
      Fordeler for bruker: potensielt godt personvern fordi SP ikke lett kan dele brukerdata med andre.
    - Ulemper for SP: På lang sikt høye kostnader ved forvaltning av autentisering, vanskelig for SP å garantere sterk sikkerhet ved autentisering, SP går glipp av mulighet til å samle inn informasjon om brukere fra IDP (og andre SP-er)
      Ulemper for bruker: Identitetsoverlast for brukere, dårlig brukervennlighet
c. I den føderterte modellen er tjenestetilbyder (SP) og autentiseringstjener (IdP) ulike entiteter, slik at SP kun tilbyr tjenester, mens IdP gjør jobben med å autentisere brukere.
d. Fordeler og ulemper ved føderering:
    - Fordeler for SP: Bedre skalerbarhet for autentisering på lang sikt, enklere å oppnå sterk sikkerhet for autentisering fordi det gjøres av IdP (som antas å ha stor kompetanse), mulighet for å samle inn mer informasjon om brukere.
      Fordeler for bruker: Bedre brukervennlighet fordi samme bruker-ID og autentikator kan benyttes for mange ulike tjenester.
    - Ulemper for SP: Initiell kompleksitet for å opprette føderering med IdP-er.
      Ulemper for bruker: Potensielt angrep på personvern fordi SP-er og IdP-er lett kan dele informasjon med hverandre, potensiell avhengighet av noen få IdP-er for tilgang til mange SP-er.

Oppgave 3: ABAC – Attributtbasert tilgangskontroll

Attributtbasert tilgangskontroll, eller ABAC (Attribute-Based Access Control) er en fleksibel modell for tilgangskontroll.

a. Nevn fire kilder for attributter i ABAC.
b. Forklar hvordan DAC kan implementeres med ABAC.
c. Forklar hvordan MAC kan implementeres med ABAC.
d. Forklar hvordan RBAC kan implementeres med ABAC.

Løsningsforslag

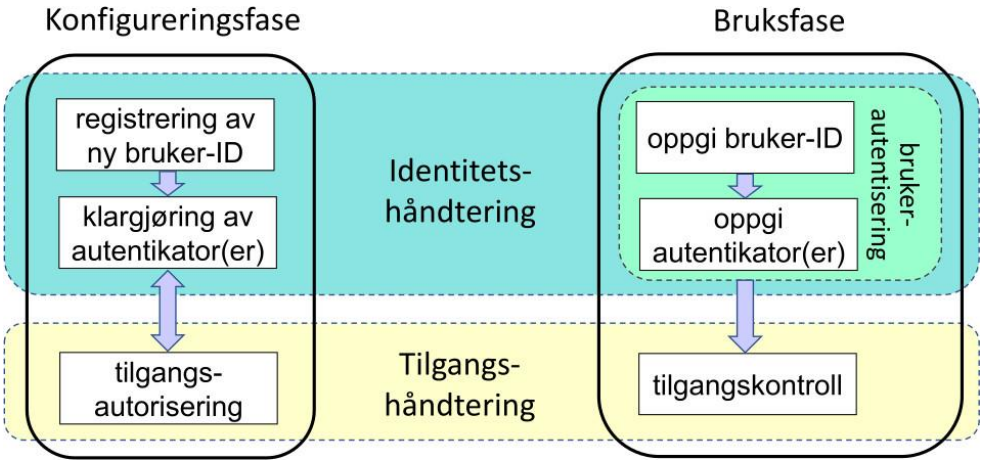
a. Typer attributter: i) Subjekt-attributter, ii) Objekt-attributter, iii) Kontekst-attributter, iv) Forespørselsattributter. I tillegg kommer policyer (regler for å ta beslutning om tilgang) som tar attributtene som input.
b. Definer brukeridentitet som subjekt-attributt og ressursidentitet som objekt-attributt. Policyen er simpelthen en ACL.
c. Definer sikkerhetsklarering som subjekt-attributt, og sikkerhetsgradering som objekt-attributt. Policyen kan f.eks. være MAC basert på Bell-LaPadula-modellen.
d. Definer rolle-proxyene (objekter fra brukers perspektiv og subjekter fra ressursens perspektiv. Deretter kan det defineres attributter (identiteter eller labeler) for brukere, roller og ressurser. Til slutt defineres policy (DAC eller MAC) for brukers tilgang til roller, og policy (DAC eller MAC) for rollers tilgang til ressurser.

Oppgave 4: IAM faser og trinn

a. Tegn et diagram av IAM i form av to faser, med et sett med trinn, og angi hvilke trinn som tilhører identitetshåndtering (Identity Management) og hvilke trinn som tilhører tilgangshåndtering (Access Management).
b. *Autorisering* er et essensielt begrep i ISO 27000 sine definisjoner av konfidensialitet, integritet og tilgjengelighet. Dessverre blir autorisering ofte beskrevet på en måte som er inkonsistent med ISO 27000. Gi en (i) konsistent (riktig) og (ii) inkonsistent (feilaktig) tolkning av begrepet autorisering relatert til de to fasene i IAM.

Svarforslag

a. Diagrammet for IAM er nedenfor.



b. Tolkninger av autorisering:

(i) Den korrekte og konsistente meningen av autorisering er "å spesifisere tilgangspolicy" som skjer under konfigurasjonsfasen.

(ii) Den feilaktige og inkonsistente, men dessverre vanlige, bruken av begrepet autorisering er "at systemet gir tilgang" som faktisk er tilgangskontroll og som skjer under bruksfasen.

Oppgave 5: Sentralisert og distribuert ID-føderering

Føderert identitetshåndtering kan ha sentralisert eller distribuert autentisering, og kan ha sentralisert eller distribuert navnerom. Finn typiske eksempler på forskjellige ordninger for føderert identitetshåndtering som brukes, og se hvor de passer inn tabellen nedenfor, og forklar på hvilken måte de er sentralisert eller distribuert. Vurder e, g, Aadhaar (Indias «unique identity»), det tyske eID, Eduroam, FEIDE, ID-porten, HelseId, europeisk eID, internett-IdP-ene facebook/google/twitter/apple/microsoft, og andre som du kommer på.

	Sentralisert navnerom	Distribuert navnerom
Sentralisert autentisering		
Distribuert autentisering		

Løsningsforslag

Figuren nedenfor kategoriserer ulike ordninger for føderert identitetshåndering.

Kategori av føderering	Sentralisert navnerom	Distribuert navnerom
Sentralisert autentisering	Tysk eID, AADHAAR	FEIDE, eduroam
Distribuert autentisering	ID-porten, altinn, HelseID	Google, Microsoft, twitter, fb, Apple, Europeisk eID

Se forklaring på s.191 i læreboka.

Oppgave 6: Kommersiell og militær tilgangshåndtering

a. Hvilke modeller for tilgangskontroll er tradisjonelt brukt i
   i. Kommersielle systemer
   ii. Militære systemer
b. Hvilket er det viktigste sikkerhetsmål som MAC (Bell-LaPadula) støtter?
c. Gi et eksempel på et anvendelsesområde der MAC (Bell-LaPadula) er hensiktsmessig.
d. Forklar kort følgende sikkerhetsprinsipper i Bell-LaPadula:
   (i) «No read up» (simpel security property: SS),
   (ii) «No write down» (Star property: *)
e. Anta at en bruker har sikkerhetsklarering STRENGT HEMMELIG. Hvordan kan brukeren redigere (lese og skrive) et dokument som har en lavere sikkerhetsgradering, f.eks. HEMMELIG?

Løsningsforslag

a. Tradisjonell bruk av modeller for tilgangskontroll
   i) Kommersielle systemer bruker DAC
   ii) Militære systemer bruker både DAC og MAC
b. Konfidensialitet
c. Militære
d. BLP-prinsippene er
   (i) SS-Property betyr «no read up». Anta at brukeren ber om lesetilgang. Da vil SS-property kreve at brukerens sikkerhetsklarering er minst like høy som objektets sikkerhetsgradering.
   (ii) *-Property betyr «no write down». Anta at brukeren ber om skrivetilgang til et objekt. *-property krever at brukerens sikkerhetsklarering er lik eller lavere enn objektets sikkerhetsgradering.
e. En bruker med sikkerhetsklarering STRENGT HEMMELIG kan velge et lavere aktuelt klareringsnivå for økten når hen logger inn. Hvis brukeren velger aktuelt klareringsnivå HEMMELIG kan hen redigere dokumenter merket HEMMELIG.

Oppgave 7: Distribuert tilgangsstyring

a. Hva var internettindustriens motivasjon for å utvikle OAuth-standarden?
b. Hvordan kan OAuth benyttes for tilgangsstyring for tilgang mellom virksomheter inne en sektor, f.eks. for tilgang til pasientdata innen helsesektoren.

Løsningsforslag

a. Internett-industrien så behovet for utveksling av brukerdata mellom ulike tjenestetilbydere der samme bruker er kunde. For å implementere praktiske ordninger for denne type utveksling av brukerdata mellom ulike internett-tjenester var nødvendig å utvikle en felles standard for hele industrien. Denne standarden fikk navnet OAuth, og er standardisert av IETF (Internet Engineering Task Force).
b. I helsesektoren er det behov for utveksling av helsedata mellom institusjoner (sykehus, legekontor, patologilaboratorier osv.). Det ville være upraktisk om to og to institusjoner måtte lage en egen ordning seg imellom. Med OAuth kan det lages en generell ordning med en eller flere sentraliserte autoriseringstjenere som lar helseinstitusjoner definere og håndheve tilgangspolicyer seg imellom.