Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 10: Identitets- og tilgangshåndtering

Spørsmål 1

a. Gi en kort forklaring på følgende begreper knyttet til identitetshåndtering.
   (i) Entitet.
   (ii) Identitet.
   (iii) Navn (identifikator).
   (iv) Digital identitet
b. Forklar kort hva som menes med begrepet "identitets- og tilgangshåndtering" eller IAM (Identity and Access Management).

Spørsmål 2

a. Nevn fasene av IAM
b. Hva betyr *identifisering* fra brukerens side, og fra tjenestetilbyderens side?
c. Beskriv korrekt (konsistent) og feilaktig (inkonsistent) mening av begrepet *autorisering*.

Spørsmål 3

a. Beskriv kort silo-modellen for identitetshåndtering.
b. Beskriv fordeler og ulemper ved silo-modellen.

Spørsmål 4

Federert identitetshåndtering kan ha sentralisert eller distribuert authentisering, og kan ha sentralisert eller distribuert navnerom, og kan i tillegg ha en sentralisert mellomnode/broker. Finn typiske eksempler på forskjellige federerte systemer for identitetshåndtering som brukes på Internet, 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»), Eduroam, Facebook Connect, FEIDE, Google +, ID-porten, HelseId, og andre som du kommer på.

	Sentralisert navnerom	Distribuert navnerom
Sentralisert autentisering		
Distribuert autentisering		

Spørsmål 5

SAML angir to forskjellige protokollprofiler for federert autentisering.

a. Forklar kort de to protokollprofilene.
b. Hvilken profil er **ikke** basert på videresending av sikkerhetstoken (krypto-token) via klient-nettleseren? Er dette en fordel? Hvorfor/hvorfor ikke?

Spørsmål 6

a. Definer kort begrepet identitetsbasert tilgangskontroll, eller «discretionary access control» (DAC), i henhold til TCSEC.
b. Definer kort begrepet labelbasert tilgangskontroll (MAC), eller «mandatory access control» i henhold til TCSEC.
c. Hvilke modeller av tilgangskontroll er vanligvis brukt i

(i) Kommersielle systemer
(ii) Militære systemer

Spørsmål 7

Bell-LaPadula-modellen (BLP) er en formell sikkerhetsmodell for et systems tilgangskontroll basert på både informasjonens klassifiseringsnivå og identiteter.

a. Hvilken er den viktigste sikkerhetstjenesten som Bell-LaPadula støtter?
b. Gi et eksempel på et anvendelsesområde der Bell-LaPadula er hensiktsmessig.
c. Beskriv kort følgende sikkerhetsprinsipper i Bell-LaPadula:
    (i) simpel security property (SS),
    (ii) Star property (*)

Spørsmål 8

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

a. Nevn 4 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.

Spørsmål 9

Hvilken betydning har XACML for implementering av ABAC-systemer ?