Hjemmeeksamen i IN2120:

Access control in distributed networks

Kandidatnr: 15362

Universitet i Oslo

Høst 2019

1. Innledning

I denne oppgaven skal jeg ta for meg tilgangskontroll innen distribuerte nettverk. Motivasjonen til å skrive om dette temaet er at tilgangskontroll spiller en stor rolle innen informasjonssikkerhet. Ingen organisasjoner har et ønske om at uvedkommende skal få tilgang til sensitiv og viktig informasjon om sin bedrift.

Jeg skal ta for meg hva tilgangskontroll egentlig er og deretter hva et distribuert -nettverk og -system er. Videre skal jeg ta for meg hva det innebærer å ha tilgangskontroll i distribuerte nettverk, og deretter analysere noen forskningsartikler basert på dette.

Problemstillingen jeg skal ta utgangspunktet i denne oppgaven er,

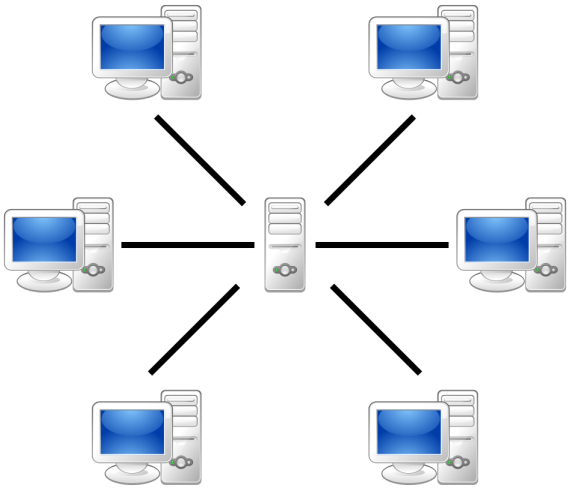
Hvorfor spiller tilgangskontroll en stor rolle for å opprettholde sikkerheten av sensitiv informasjon i et distribuert nettverk?

2. Distribuert nettverk og distribuert system

Før jeg skriver hva egentlig et distribuert nettverk er, vil jeg aller først definere begrepene distribusjon og nettverk. Distribusjon betyr generelt å fordele/ å utdele. I følge snl.no så fordeles begrepet distribusjon i to deler; markedsføring og transportere ("distribusjon – Store norske leksikon," n.d.). Innen informatikk, vil den sistnevnte delen være til mer nytte for definisjonen for distribuert nettverk , siden et distribuert nettverk handler om å transportere data gjennom ulike nettverk. Hvor for eksempel vi skal sende data fra nettverk A som er kilden til nettverk B som er destinasjonen.

Et nettverk er et system av samhandlende komponenter. Sammen med begrepet distribuert kan man definere et distribuert nettverk som et datanettverk som avhenger av flere kilder. Disse kildene kommuniserer gjennom komplekse datamaskiner, også kalt for noder. Dette medfører til datakommunikasjon mellom ulike stasjonære maskiner, lokale nettverksservere, region servere, webservere og andre type servere. Generelt er hensikten med et distribuert nettverk er å koordinere bruken av delte ressurser eller en kommunikasjonstjeneste for brukere. (Praveen Balda, 2015)

Mens et distribuert system er et system hvor flere maskiner er er sammenhengende av et nettverk(Maymi & Harris, 2018). Alle maskinene samarbeider effektivt som en enhet, så et distribuert nettverk er en sammenkoblingen av alle disse maskinene som transporterer data i mellom seg. Det finnes mange ulike distribuerte nettverk, og en av dem er klient/server nettverk arkitekturen. Hvor det hele baserer seg på at en klient vil hente data fra en server. Mange organisasjoner tar i bruk denne type arkitektur hvor ansatte får tak i data relatert til sitt arbeid fra en server, men denne serveren kan også inneholde sensitiv informasjon for organisasjonen, derfor er det utrolig viktig å kunne ha en streng adgang til denne serveren.



Figur 1: Eksempel Klient/server arkitekturen (Contributors to Wikimedia projects, 2008)

2.1. Nettverkssikkerhet

I dagens samfunn har de fleste organisasjoner, et nettverk for å kunne utføre datakommunikasjon mellom nodene i deres nettverket. Men dette fører også til å bli utsatt for angrep. Derfor er nettverkssikkerhet ganske viktig å ha i fokus.

Innen nettverkssikkerhet så er det to hovedområder;

Kommunikasjonssikkerhet: handler om sikkerheten av data som blir overført i et nettverk mellom sluttbrukere og organisasjoner (Gruschka, 2019). Siden sikkerheten av transportering av data er utrolig viktig, så har det blitt utviklet flere ulike sikkerhetsprotokoller for ulike formål (Gruschka 2019):

- Integritet, autentisering og konfidensialitet
- nøkkelutveksling
- e-voting
- secret sharing

Det finnes mange flere formål, også kalt for sikkerhetstjenester enn de nevnte, men en smart kombinasjon av disse 4 sikkerhetstjenestene kan bidra til å forhindre seg mot angrep i overførings fasen mellom to maskiner.

Innen informasjonssikkerhet er man aldri 100% forsikret mot angrep. Derfor er sikkerhet av data alltid under utvikling og forbedring. Et eksempel på dette er utviklingen av Transport Layer Security (Jøsang, 2019a).

Perimeter security: handler om å beskytte nettverket til organisasjonen for uautorisert tilgang (Jøsang, 2019b). Det er veldig viktig å ha en ledelse av IT-sikkerhet i en organisasjon, siden det gir en verdi til organisasjonen. Disse er noen enkelte fordeler med å fokus på IT-sikkerhet; (Jøsang, 2019e)

- tillit fra kunder, partnere, investorer, og ansatte
- forbedret rykte
- blir konkurransedyktige
- forbedring og redusering av tap
- får større verdi hos aksjonærene

Dette er de fordelene som bidrar til en økning av verdien til organisasjonen, det fjerde punktet er veldig viktig å sette fokus i en organisasjon på ut i fra mitt perspektiv, såkalt risikohåndtering.

Risikohåndtering bidrar til å avdekke trusler, sårbarheter og risiko, og deretter bruker virkemidler til å redusere risiko på et akseptabelt nivå (Jøsang 2019). Grunnbasen for informasjonssikkerhet, er å vite hva risikoen er, for da vet man hvor i nettverket eller systemet det er nødvendig med ekstra sikkerhet . For eksempel hvis en organisasjon som ikke har en ledelse som tar hånd om risikohåndtering, og velger å satse på å utvikle en brannmur for å forbedre sikkerheten sin, uten å vite om det faktisk er nødvendig. Dette medfører jo til tap av store summer organisasjonen har brukt på utviklerne og hele prosessen på det.

3. Hva er tilgangskontroll?

Tilgangskontroll er en sikkerhetsfunksjon som bidrar til å beskytte delte ressurser og data mot uautorisert tilgang (Brose, 2011). Tilgangskontroll er et begrep innen flere domener, men innen informatikk er det mer fokus på at en uautorisert person ikke skal få tilgang til data som er konfidensiell, derfor er autentifikasjon av brukere i et nettverk eller et system veldig viktig.

Formålet med tilgangskontroll er å kunne opprettholde sikkerhetstjenester som konfidensialitet og integritet av data ressurser, slik at det skal forhindre at disse data ressursene ikke blir brukt på en uautoriserte måte. For å definere forskjellen på autorisert og uautorisert tilgang, så lager man en tilgangskontroll polise (access control policy). Denne polisen er en beskrivelse av til tillatt og nektet tilgang i et system. (Brose, 2011)

3.1. Ulike mekanismer

Det finnes to type tilgangskontroll, hvor den ene er fysisk tilgangskontroll og den andre er logisk tilgangskontroll. Jeg skal skrive mest om den sistnevnte. Innen logisk adgang kontroll har vi fire ulike typer som er definert punktvis under (Jøsang, 2019f). Det finnes fire ulike modus for tilgang i systemer som forteller om hvilke tilstander enkelte brukere av systemer har tilgang til de ulike objektene. Disse er: lese (r), skrive (w), eksekvere (x) og append (a) (Jøsang 2019). Disse blir brukt flittig i tilgangskontroll lister og matriser som definerer hvem (subjekter) som har tilgang til hva (objekter).

- **Discretionary Access Control (DAC)** har fokus på tilgangs autorisasjon som er spesifisert og opprettholdes basert på navn/identitet av objekter og subjekter. Det blir brukt en tilgangskontroll liste (access control list) for å kunne spesifisere hvem som har tilgang til det objektet.

	O1
S1	r,w
S2	r
S3	-
S4	r,w

	O2
S1	-
S2	-
S3	x
S4	x

	O3
S1	x
S2	r
S3	-
S4	x

	O4
S1	r
S2	r,w
S3	-
S4	x

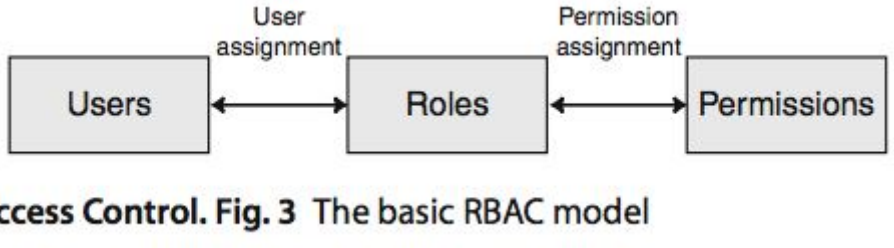
Figur 2: Eksempel på Access control list (Jøsang, 2019f)

Columns→ ↓Rows		Object names			
		O1	O2	O3	O4
Subject names	S1	r,w	-	x	r
	S2	r	-	r	r,w
	S3	-	x	-	-
	S4	r,w	x	x	x

Figur 2: Eksempel på Access control matrix (Jøsang, 2019f)

- **Mandatory access control (MAC)** er en tilgangskontroll som baserer seg på begrense muligheten for at ressurseier ikke kan endre eller velge hvem som kan få tilgang til ressursene. Tilgangs autorisasjonen er spesifiser på med sikkerhetsetiketter: klassifiseringsnivå av objekter, og sikkerhetsklarering av subjekter.

- **Role-Based Access Control (RBAC)** har fokus på å tildele roller til brukere av system, en bruker får tilgang til et objekt basert på stillingen sin. Rollene blir tildelt basert på stillingen, så brukeren får adgang basert på autoritet og ansvar. Et viktig punkt å huske er at objekter bryr seg om brukeren rolle og ikke selve brukeren.



Access Control. Fig. 3 The basic RBAC model

Figur 4: En enkel role based access control (Brose, 2011)

- **Attribute-Based Access Control (ABAC)** er en generalisering av de tre ovenfor. ABAC spesifiserer og godkjenner tilganger basert på poliser kombinert med attributter som bruker- ressur- og kontekst-attributter.

4. Tilgangskontroll i distribuerte nettverk

Distribuerte systemer har alltid vært under utvikling, og denne utviklingen har ledet til flere ulike teknologier, som peer-to-peer nettverk (P2P), tjenesteorientert arkitektur (SOA), web service og nettsky (Lázár, 2014). På grunn av økningen på mengden av utvekslet og publisert informasjon om disse teknologien, så har den mest vanskeligste oppgaven vært å kunne administrere disse teknologiene, med tanke på sikkerhet (Lázár, 2014).

Selv om utvikling av slike systemer har gitt oss nye teknologier som blir brukt flittig, så er det viktig å ha fokus på sikkerheten av dataressurser i slike systemer. Som nevnt over så har informasjon om slike teknologier blitt publisert, som videre fører til at enkelte personer kan bare søke opp på nettet og vite hvordan disse teknologiene fungerer. Derfor er det viktig å kunne ha enda mer avansert og hemmelig måte for at en organisasjon skal kunne sende sensitive data fra A til B, på en sikker måte. Slik at en uautorisert person ikke skal få tak i denne sensitive dataen som blir sendt over i et nettverk.

4.1. ABAC (Attribute-Based Access Control)

Å dele informasjon innen service-orientert miljø fører til skremmende sikkerhetsutfordringer. På den ene siden kreves det at dataen blir tilgjengelig for alle de som trenger den dataen, og på den andre siden må organisasjoner beskytte sensitiv data og konfidensiell informasjon slik at kun autoriserte personer kan hente og manipulere ressursene (Yuan & Tong, 2005). Å få til en god balansering av disse to, så har det blitt utviklet en rekke standarder for å kunne administrere dette (Yuan and Tong 2005). Et av disse har vært XACLM (XML Access Control Markup Language) som definerer et språk for å uttrykke tilgangskontroll attributter og poliser som er implementert i XML, og en behandlingsmodell som beskriver hvordan man evaluerer tilgang (Yuan & Tong, 2005).

XACLM terminologi er en nødvendighet for nettverk som tar i bruk ABAC for å kunne uttrykke alle mulige attributter og verdiene til attributtene. Men en ulempe med å ta i bruk en ABAC er at man må implementere tilgangskontroll polisene i formen av XACLM og det krever mer sammensetningen av ontologier i forhold til de tradisjonelle tilgangskontrollene (DAC, MAC, RBAC) (Jøsang 2019) . I tillegg kreves det politisk justering og lovlige avtaler ved å ta i bruk ABAC i distribuerte miljøer. Men i forhold til ulempene ved å ta bruk en ABAC så er fordelen at det er mer fleksibel i forhold til de tradisjonelle tilgangskontrollene, og er en passende tilgangskontroll i distribuerte miljøer. I tillegg kan man bruke alle type autorisasjon poliser kombinert med ubegrenset antall av attributter (Jøsang 2019).

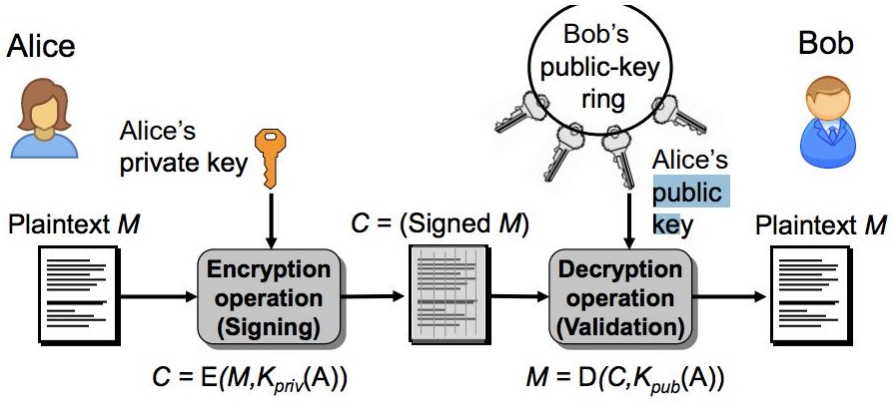
4.2. Kryptografi

Kryptografi handler om å gjemme informasjon, selv om kryptografi har vært et sentralt verktøy for å kunne sende hemmelige meldinger tvers over et nettverk, så har det vært under utvikling siden 500 f.Kr. Derfor blir kryptografi definert som vitenskapen av hemmelig skriving, med fokus på å skjule betydningen av budskapet av meldingen (Jøsang, 2019d). Kryptografi kan sørge for disse fire sikkerhetstjenestene kommer i nytte (Jøsang, 2019d):

- **Konfidensialitet:** dataen blir uleselig for enheter som ikke har den passende kryptografiske nøkkelen.
- **Dataintegritet:** enheter med riktige kryptografiske nøkler kan bekrefte at dataene er riktige og uendret
- **Autorisering:** enhetene som kommuniserer kan være sikre på at enhetene er dem de hevder å være.
- **Digital signering:** gir bevis på data opprettelsen verifiseres fra tredjepart.

Innen distribuerte nettverk så blir kryptografiske algoritmer tatt i bruk for å overføre elektrisk data over internettet slik at tredjeperson ikke skal få lese dataene.

PKI (Public Key Infrastructure) er et rammeverk for kryptering og cybersikekrhet som beskytter kommunikasjon mellom server og klientene (“How Does PKI Work | Venafi,” n.d.). PKI fungerer med en offentlig nøkkel og en privat nøkkel, hvor disse nøklene blir brukt for en digital signering for begge parter (Jøsang, 2019d). Figur 5 viser en enkel digital signering mellom to parter.



Figur 5: Et eksempel på en enkel digital signering (Jøsang, 2019d)

I offentlige sektorer blir det brukt standarder for PKI. Difi tar i bruk standarden som er vist i figur 6. I følge Difi bidrar standarden til en effektiv forbindelse med elektronisk kommunikasjon med og i offentlig sektor. For Difi er PKI er en nyttig og nødvendig funksjonalitet for at offentlig sektor skal tilby innbyggerne digitale tjenester. Dette gir Difi en sikkerhet om at innbyggerne er den vedkommende gir seg for å være, samtidig som at sensitiv informasjon ikke kommer til en uautorisert person ("PKI (Public Key Infrastructure) - Kravspesifikasjon | Difi," n.d.-a).

Figur 6: en standard for Bruksområdet gjelder elektronisk kommunikasjon med og i offentlig sektor("PKI (Public Key Infrastructure) - Kravspesifikasjon | Difi," n.d.-b)

5. Konklusjon

I denne oppgaven har jeg tatt for meg ulike tilgangskontroller som blir brukt for sikkerheten av dataressurser i et distribuert nettverk. Jeg har skrevet om de ulike tilgangskontrollene som blir tatt i bruk i praksis, hvor jeg konkluderer at ABAC (atributt basert tilgangskontroll) er mer flittig brukt i forhold til de tradisjonelle tilgangskontrollene. ABAC er også mer tilpasset for distribuerte miljøer og bidrar til å få en sikkerhet over dataressurser i nettverket (Yuan and Tong 2005).

Tilgangskontroll spiller en stor rolle for å opprettholde sikkerheten av data i et distribuert nettverk, siden det bidrar til å få en oversikt over hvem som har tilgang til enkelte objekter i et nettverk, og hvilke funksjoner enkelte har muligheten å gjøre med objektet.
I tillegg så er det også veldig viktig å kunne kryptere meldinger som blir sendt tvers over nettverket, slik at meldingene blir holdt konfidensielt.

Det finnes mange flere sikkerhetstjenester for å beskyttet seg mot angrep i en organisasjon, for eksempel konfidensialitet så kan det oppstå ulike angrep som informasjonstyveri, en ansatt utgir for å være en autentisert person i organisasjonen og får tilgang til sensitiv informasjon om organisasjonen. Innen integritet så kan angrep som data og system korrupsjon og tap av ansvarlighet oppstå, og for dette finnes det mange sikkerhetskontroller som kryptering, hashing, digital signering, autentisering, tilgangskontroll… osv (Jøsang, 2019c). Derfor er det viktig med ulike sikkerhetskontroller for å forsikre seg om at informasjonen blir kun tilgjengelig for autentiserte personer.

6. Referanser

Brose, G. (2011). *Encyclopedia of Cryptography and Security* (S. J. Henk C. A. van Tilborg, ed.). Springer Science+Business Media,.

Contributors to Wikimedia projects. (2008, November 11). Client-server. Retrieved November 2, 2019, from Wikimedia Foundation, Inc. website: https://simple.wikipedia.org/wiki/Client-server#/media/File:Server-based-network.svg

distribusjon – Store norske leksikon. (n.d.). Retrieved October 24, 2019, from Store norske leksikon website: https://snl.no/distribusjon

Gruschka, N. (2019, September 12). Network Security. Retrieved October 30, 2019, from UiO.no website: https://www.uio.no/studier/emner/matnat/ifi/IN2120/h19/lectures/in2120-2019-l04-netsec.pdf

How Does PKI Work | Venafi. (n.d.). Retrieved November 3, 2019, from https://www.venafi.com/education-center/pki/how-does-pki-work

Jøsang, A. (2019a, August). *Course Info + IS Concepts*. Retrieved from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h19/lectures/in2120-2019-l01-intro-basics.pdf

Jøsang, A. (2019b, August). *Lecture 1 - Basic concepts in information security*. Retrieved from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h19/lectures/in2120-2019-l01-intro-basics.pdf

Jøsang, A. (2019c, August). *Lecture 1 - Basic concepts in information security*. Retrieved from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h19/lectures/in2120-2019-l01-intro-basics.pdf

Jøsang, A. (2019d, August). *Lecture 02 - Cryptography*. Retrieved from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h19/lectures/in2120-2019-l02-crypto.pdf

Jøsang, A. (2019e, September). *Lecture 05 - Information Security Management - Human Factors for Information Security*. Retrieved from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h19/lectures/in2120-2019-l05-isman-humfact.pdf

Jøsang, A. (2019f, October). *Lecture 10 - Identity and Access Management*. Retrieved from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h19/lectures/in2120-2019-l10-iam.pdf

Lázár, K. A. (2014). A Computational Model of XACML–Based Access Control Management in Distributed Networks. *Language, Life, Limits*, pp. 265–274. https://doi.org/10.1007/978-3-319-08019-2_27

Maymi, F., & Harris, S. (2018). *CISSP All-in-One Exam Guide, Eighth Edition*. McGraw-Hill Education.

PKI (Public Key Infrastructure) - Kravspesifikasjon | Difi. (n.d.-a). Retrieved November 3, 2019, from https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/pki-public-key-infrastructure-kravspesifikasjon

PKI (Public Key Infrastructure) - Kravspesifikasjon | Difi. (n.d.-b). Retrieved November 3, 2019, from https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/pki-public-key-infrastructure-kravspesifikasjon

Praveen Balda, S. M. G. (2015). Security Enhancement in Distributed Networking. *Computer Science and Information Technology*. Retrieved from

https://ijcsmc.com/docs/papers/April2015/V4I4201599a43.pdf
Yuan, E., & Tong, J. (2005). Attributed based access control (ABAC) for Web services. *IEEE International Conference on Web Services (ICWS'05)*. https://doi.org/10.1109/icws.2005.25