Java 2 Enterprise Edition tietoturvamalli

Valtteri Rahkonen

30.9.2002

Hajautetut sovellukset vaativat usein järjestelmätason palveluita, kuten transaktion hallintaa, tietoturvaa, yhteyksien hallintaa ja tietokantayhteyksiä. Java 2 Enterprise Edition (J2EE) on SUN:in kehittämä alusta, joka on tarkoitettu helpottamaan hajautettujen sovellusten kehittämistä. J2EE:n ensimmäinen versio julkaistiin joulukuussa 1999, ja nykyinen versio on 1.3. Tässä seminaarityössä tutustutaan J2EE:n tarjoamiin tietoturvapalveluihin.

J2EE:n tietoturvallisuus koostuu turvallisesta suoritusympäristöstä JVM (Java Virtual Machine), työkaluista ja palveluista, joiden avulla sovelluksien kehittäjät pystyvät kehittämään turvallisia sovelluksia. Suoritusympäristön turvallisuus saavutetaan muistinhallinan kautta. JVM eristää nimiavaruudet toisistaan, suorittaa muistinhallinan ja lisäksi tutkii puskurin ylivuototapauksia automaattisesti.

J2EE tarjoaa tietoturvapalveluita autentikaatioon, oikeuksien määrittämiseen ja viestiliikenteen salaamiseen. Käyttäjän autentikaatio voidaan suorittaa käyttäjätunnuksella ja salanalla tai X509 sertifikaatilla. Autentikaation avulla määritellään mihin oikeusryhmään käyttäjä kuuluu, eli mitä sovelluksen komponentteja käyttäjä saa käyttää.

Sovellukselle määritellään tietoturvapolitiikka, jossa määrätään käyttäjäryhmät ja näiden ryhmien oikeudet sovelluksen komponenteille. Eri käyttäjäryhmillä voi olla eri tasoisia oikeuksia komponentteihin. Osa käyttäjistä voi esimerkiksi lukea tietoja, mutta ainoastaan järjestelmän ylläpitäjä saa muokata niitä.

J2EE tarjoaa oikeuksien määrittelyn myös komponenteille. Yksinkertaisimmillaan sovellus eristetään "hiekkalaatikkoon", jolla rajoitetaan sovelluksen suoritusoikeuksia. Perinteisesti rajoitetuilta sovelluksilta estetään pääsy mm. paikalliselle kovalevylle ja estetään uusien verkkoyhteyksien avaaminen. Sertifikaattien ja sovellusten allekirjoitusten avulla on mahdollista toteuttaa luotettuja sovelluksia, joiden rajoitustasoa säädetään tietoturvapolitiikan perusteella.

Tietoturvamanagerin (Security Manager) vastuulla on tietoturvapolitiikan hallinta. Tietoturvapolitiikka määritellään politiikka tiedostoilla. Tietoturvapoliikka määrittelee suoritettavan koodin oikeudet, kun se on suorituksessa. Kun sovellus haluaa suorittaa koodia, joka vaatii oikeuksia hiekkalaatikon ulkopuolelta, tietoturvamanageri välittää pyynnön oikeuksien hallinnolle (Access Controller). Päätös oikeuksien sallimisesta riippuu suoritettavan luokan oikeuksista tietoturvapoliikassa.

Java tarjoaa tiedon salaukseen joukon luokkia, jotka koottu JCE:hen (Java Cryptography Extension). JCE:n salauspalvelut ovat rajoitettuja johtuen Yhdysvaltojen hallituksen vientirajoituksesta. Sen vuoksi JCE tarjoaa mahdollisuuden lisätä salauspalveluita. JCE:n lisäksi tarjolla on JSSE (Java Secure Socket Extension), joka tarjoaa kehittäjille SSL (Secure Socket Layer) ja TLS (Transport Layer Security) toiminnot. JCE ja JSSE olivat aikaisemmin erillisinä paketteina, mutta uusimpaan Java versioon ne ovat integroitu mukaan.

J2EE sisältää tietoturvatyökalun tietoturvapolittiikan hallintaan. Lisäksi tarjolla on työkalut sertifikaattien tekoon ja hallintaan sekä sovellusten allekirjoittamiseen.

Lähteet

1 The Source for JavaTM Technology
`http://java.sun.com/`

2 JavaTM 2 Platform Security Architecture
`http://java.sun.com/j2se/1.4.1/docs/guide/security/spec/security-spec.doc.html`

3 JavaTM 2 Enterprise Edition Developer's Guide
`http://java.sun.com/j2ee/sdk_1.2.1/techdocs/guides/ejb/html/DevGuideTOC.html`

4 Developing Enterprise Applications
`http://citeseer.nj.nec.com/491812.html`

5 Ger Mulcahy
J2EE and .Net Security
`http://www.owasp.org/downloads/J2EEandDotNetsecurityByGerMulcahy.pdf`