Cross Domain Solutions – äärimmäisen turvallista selaamista

Uusi järjestelmäratkaisu turvallisuus- ja puolustussektorille

Cross Domain Solutions – äärimmäisen turvallista selaamista ja lataamista

Cross Domain Solutions (CDS) -mallit ja -järjestelmät tarjoavat ratkaisun eri turvallisuusvyöhykkeiden välillä tapahtuvaan tiedonsiirtoon.

Turvallisuus- ja puolustussektorin viranomaiset joutuvat usein siirtämään tietoa eri tietoturvavyöhykkeillä olevien päätelaitteen välillä. Tällöin arkaluonteisen informaation tietoturva saattaa vaarantua.

Yksi haasteista on ollut julkisesta verkosta ladatun tiedon siirtäminen korkeamman tietoturvaluokan välineisiin. Se on vaatinut hidasta, manuaalista työtä. Nyt ongelmaan on ratkaisu: Cross Domain Solutions (CDS) -järjestelmät on kehitetty eri tietoturvavyöhykkeiden välillä tapahtuvaan turvalliseen tiedonsiirtoon.

Helppokäyttöinen ja turvallinen

CDS tarjoaa helppokäyttöisen ja korkean tietoturvan ratkaisun loppukäyttäjille ilman erillistä koulutustarvetta. Ainoa osaamisvaatimus on selaimen käyttö. Työasemaan tai älypuhelimeen asennetaan oma selain, mutta ilman selaimen haavoittuvuusrajapintaa, koska varsinainen selainprosessi pyörii CDS-laitteiston uhrautuvan puolen prosessorissa, joka on eristetty puhtaalta puolelta.

Jokaiselle käyttäjälle on varattu kaksi prosessoria, joten järjestelmän tehokkuus säilyy vakiona tilanteesta riippumatta. Prosessoreina käytetään mobiilipuhelimista tuttuja siruja. Vaikka selauslaitteisto sisältää satoja prosessoreja, on sen rakentaminen kustannustehokasta.

Transformaatioiden, eristämisen, siirtorakenteiden ja tarvittavien kontrollien käyttö teknisessä ratkaisussa huomioi myös nollapäivähaavoittuvuudet. Nollapäivähaavoittuvuus tarkoittaa tietoturva-aukkoa, jolle tuotteen valmistaja ei ole tehnyt korjausta. Integroidun CDS-ratkaisun turvallisuus on rauta-, ohjelmisto- ja arkkitehtuuripohjaista. Sitä ei ole mahdollista ohittaa.

Suomen viranomaisten luokitellut tietoturvavyöhykkeet

Tietoturvavyöhyke tai -alue on tietojärjestelmien muodostama kokonaisuus eli ympäristö, joka on luotu tietoturvasäännöstöjen määrittämien ohjeiden ja luokitusten mukaan. Ympäristössä tieto tallennetaan ja käsitellään siten, että salassa pidettävä tieto pysyy suojattuna. Tahaton tai tahallinen tiedon väärinkäyttö tai siirtäminen voidaan estää. Näistä tietoturva-alueista käytetään useasti englanninkielistä nimitystä *enclave*.

KATAKRI on tietoturvallisuuden auditointityökalu viranomaisille ja *VAHTI* on julkisen hallinnon digitaalisen turvallisuuden johtoryhmän ohjesivusto. Ne määrittävät tietoturvavaatimuksia ja toimivat usein kriteeristöinä, kun luokiteltuja työskentelyvälineitä, järjestelmiä ja ympäristöjä rakennetaan, käytetään ja auditoidaan.

Suomessa viranomaisten luokiteltuja ympäristöjä on kolme tasoa:

TL II – SALAINEN
TL III – LUOTTAMUKSELLINEN
TL IV – KÄYTTÖ RAJOITETTU

Ympäristöt on tehty yleensä itsenäisiksi, eristetyiksi tietoturvavyöhykkeiksi. TL II -taso on vyöhykkeistä suojatuin ja eristetyin.

CDS:n käytöllä merkittävin hyöty saavutetaan TL II- ja TL III- tasoille luokitelluissa ympäristöissä, koska niissä on korkeat vaatimukset eri tietoturva-alueiden väliseen tiedon selaamiseen, käyttöön ja lataamiseen.

Näin Cross Domain Solutions toimii

Asiantuntijana Timo Seppälä, Fujitsu Finland

Turvallinen selausteknologia

Turvallinen selaus on varmistettu erillisellä laitteistolla, jossa jokaiselle käyttäjälle on varattu kaksi prosessoria. Ne muodostavat noodin. Selaus perustuu eristämiseen (isolation) ja eheyden varmistamiseen (verification).

Alemman puolen prosessori suorittaa sivun ja toimii käytännössä selaimena. Se tekee sivusta tietovirran, joka dekoodataan puhtaalle, ylemmälle puolelle. Saatu tietovirta prosessoidaan puhtaan puolen prosessorilla ja kompressoidaan laitteistopohjaisella, sisäänrakennetulla videopakkauksella. Se lähetetään työasemassa tai esimerkiksi Android-laitteessa olevaan selainsovellukseen. Sama toimenpide tehdään äänelle.

Paluukanava, eli hiiren ja näppäimistön painallus, on yksisuuntainen ja eristetty käytettävään laitteistoon. Kun käyttäjän istunto päättyy, prosessin noodi pyyhitään laitteistosta.

Myös videoita voidaan toistaa vastaavasti. Video tuodaan käyttäjälle turvallisella pikselivirralla, joka on raakapakattu bittikartta. Vaikka alemman puoleinen siru vaarantuisi, suoratoistoon päätyy vain video siitä, mitä alemman puolen siru näkee. Tällöin virukset tai haittaohjelmat eivät voi siirtyä alemmalta puolelta ylemmälle.

Jos selaimessa olisi tietoturva-aukko, kyseinen selausprosessi pyörisi eristämisen ansiosta vain alemman, uhrautuvan puolen sirulla. Näin ollen ylempi, puhdas puoli ei saastu. Työasemassa olevaa selainta muistuttava sovellus vastaanottaa vain data- tai videovirtaa, eikä siis esimerkiksi suoritettavaa HTML5-koodia.

Jos alemman puolen noodi saastuu, on yhden käyttäjän sivun tai kuvan laatu huono.

Turvallinen latausteknologia ja -prosessi

CDS-järjestelmän lataustuotteiden avulla tiedostoja voi ladata turvallisesti selauslaitteiston alemman puolen kautta ylemmälle tasolle, aina työasemaan asti. Tätä varten selauslaitteistoon on tehty integraatio-ohjelmisto ja työasemaan asennettava integraatiokirjasto. Ne osallistuvat tiedostojen siirto- ja puhdistusprosessiin (extract-verify-build, EVB).

Kun käyttäjä selaa turvallisella selauksella esimerkiksi nettisivuja ja käynnistää latauksen (download), se onnistuu aivan kuten normaalilla selaimella. Alemman puolen vastaanottava tiedonsiirtopalvelin (receiver) vastaanottaa tiedostoja laajennuksen avulla selauslaitteesta ja käynnistää extract-vaiheen prosessista. Kyseinen palvelin purkaa informaation tiedostosta ja muuntaa sen sisäiseen transformaatiorakenteeseen.

Jos tiedostoon olisi piilotettu haittaohjelma, se putoaisi pois, koska odottamattomasta tiedoston sisällön rakenteesta ei haeta informaatiota. Tässä vaiheessa myös poistetaan tietorakenteissa olevat mahdolliset haittaohjelmat jäsentämällä rakenteet alimmalle tasolle. Siirrettäväksi otetaan vain tiedoston uudelleenrakentamiseen tarvittava informaatio.

Varmennus ennen siirtämistä

Transformoitu tiedosto välitetään tarkistuslaitteistolle (verifier), jossa se varmennetaan ennen siirtämistä ylemmän tietoturvaluokan välittävälle palvelimelle (transmitter). Verify-vaiheessa tarkistetaan, että tiedoston sisäinen esitys on oikein jäsennelty ja että siirtämiseen käytettyä protokollaa noudatetaan.

Tarkistuslaitteisto sisältää elektroniset diodit tietovirran ohjaamiseksi. Logiikkayksikkö tekee itsenäisen vahvistusvaiheen, joka estää hyökkääjiä kohdistamasta haavoittuvuuksia muun muassa verkkoliitännän laiteohjelmistoihin, protokollapinoon tai sisältöön.

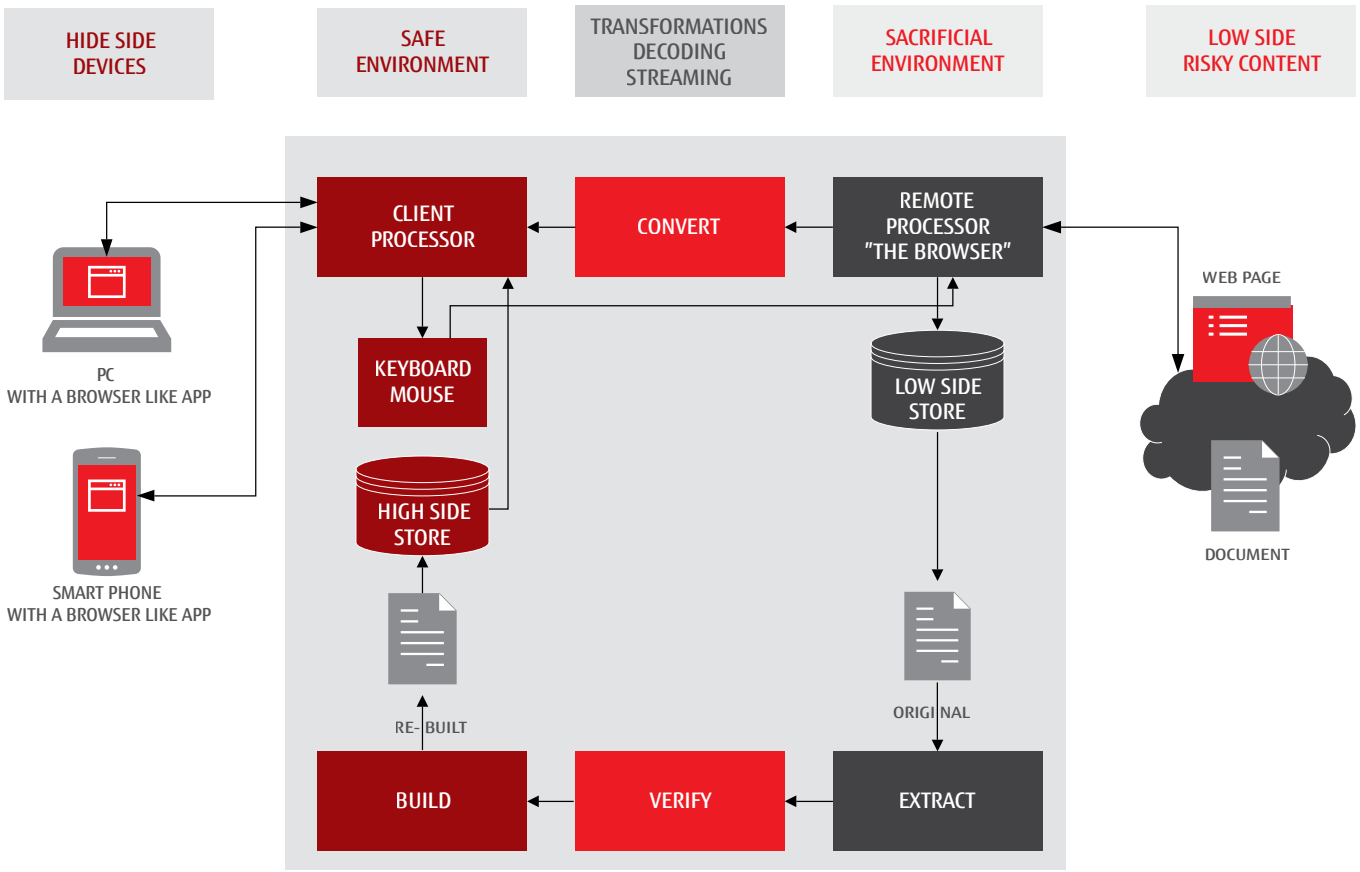
Välittävä palvelin rakentaa build-vaiheessa esimerkiksi Word- tai PDF-tiedoston uudelleen ja siirtää sen tiedonvaihtopalvelimen kautta ja työasemaan asennetun integraatiokirjaston avulla käyttäjän tallennettavaksi.

Kaikkia alemman puolen tiedostoja pidetään ”saastuneina”. Puhdaskaan tiedosto ei siirry ylemmälle puolelle ilman EVB-prosessia. Tuettuja tiedostomuotoja on kymmeniä, mukaan lukien yleisimmät kuvatiedostomuodot.

Latausteknologian avulla voidaan välittää myös XML- ja JSON-struktuureja, kun niille on tehty skeema. Tuntematon tiedostomuoto, jolla ei ole aktiivista käsittelijää, ei siirry. Tuntemattomista ja saastuneista tiedostoista tulee ilmoitus käyttäjälle.

> Integroidun CDS-ratkaisun turvallisuus on rauta-, ohjelmisto- ja arkkitehtuuripohjaista. Sitä ei ole ole mahdollista ohittaa.

Cross Domain Solutionsin toimintaperiaate



Esimerkkejä CDS-käyttötapauksista

Selaus alemmalle tasolle – Access CDS (browse down)

CDS-käyttötapauksia on useita. Selaus alemmalle tasolle -käyttötapaustyyppi mahdollistaa alemman tietoturvaluokan tietojen selaamisen ja käsittelyn korkean tietoturvaluokan työskentelyvälineellä. Tätä tyyppiä voi hyödyntää myös samassa tietoturvaluokassa olevissa järjestelmissä, jos ne ovat esimerkiksi eri organisaatioiden palveluja.

Access CDS (browse down) -käyttötapauksen ansiosta päätelaitteiden lukumäärää voidaan vähentää, koska se mahdollistaa netin selaamisen korkean tietoturvallisuuden työasemalta.

Yhdensuuntainen tiedonsiirto – Transfer CDS (uni-directional)

Ratkaisu koostuu yhdensuuntaisesta datavirtauksen ohjauksesta. Datavirran ympärillä on tietojenkäsittelykomponentteja. Manuaalisista haittaohjelmistojen tarkistusprosesseista voidaan luopua, eikä tietoa tarvitse kirjoittaa uudestaan. Siirrettävä data säilyy puhtaana.

Haluatko lisätietoja?
Ole hyvä ja ota yhteyttä:

Harri Koski
Business Development Director,
Defence and Security
Kehitysjohtaja, Puolustus- ja turvallisuus

Fujitsu Finland Oy
Mob: +358 (40) 9202460
Email: harri.koski@fujitsu.com
Web: www.fujitsu.com/fi