

TENTTI 17.12.2018

KYBERTURVALLISUUS I: PERUSTEET, TIE-30151

Marko Helenius

Tentissä ei saa käyttää oheismateriaalia eikä laskinta. Vastaa selkeästi. Huomaa, että viimeinen viides tehtävä on toisella sivulla.

(6 pistettä/tehtävä)

Tehtävä 1

Mikä on? (lyhyt määrittely riittää)

- a) lohkosalaus
- b) kertakirjautuminen
- c) AES
- d) HMAC
- e) toistohyökkäys
- f) varmenne

Tehtävä 2

Piirrä käsitekartta liittyen käytettävään tietoturvaluuteen. Käsittele ainakin ongelmia, hyötyjä sekä käytettävyyden ja tietoturvaluuden ristiriitoja.

Tehtävä 3

Piirrä kuva, josta selviää mahdollisimman hyvin, miten julkisen avaimen salaus toimii.

Tehtävä 4

Tee esimerkki hyvästä salasanasta ja sen muodostamisesta. Tämä salasana pitää muistaa ainakin osin ulkoa. Perustele, miksi salasana on hyvä.

Tehtävä 5

Trafi joutui sulkemaan ajokorttitietojen hakupalvelun, josta näki ajokorttitiedot: ajokortin myöntämisaika, voimassaoloaika ja ajokorttiluokka (minkä tyyppisiä ajoneuvoja haltija saa ajaa), mahdollinen taksinkuljettajan voimassaolon päättymisen päivämäärä. Jos henkilöllä ei ollut ajo-oikeutta, myös tämä tieto oli saatavilla. Hakuja pystyi tekemään henkilötunnuksen ja paikkakunnan tai nimen ja paikkakunnan yhdistelmällä. Yksi ongelma oli, että tiedoista pystyi päättelemään syntymäajan ja tämän jälkeen henkilötunnuksen pystyi jäljittämään kokeilemalla, sillä manuaalisten hakujen määrää ei rajoitettu. Palvelussa oli kuitenkin ns. Captcha-suoja, jonka tarkoitus on estää automatisoidut haut.

EU:n tietosuoja-asetus (GDPR) on välittömästi voimassa voimaantulon päivämäärästä lähtien ja poikkeaa siten EU:n direktiivistä. EU:n asetukset ohittavat kansallisen lainsäädännön mahdollisissa ristiriitatilanteissa. GDPR jättää kuitenkin tilaa paikalliselle lainsäädännölle. Oletamme, että ajokorttitietojen julkisuus on laillista, kunhan henkilötunnusta ja osoitetietoja ei voi päätellä. Miten Trafin kaltainen palvelu ajokorttitiedoista Internetissä pitää järjestää, jotta se noudattaa GDPR:ää ja kansallista lainsäädäntöä? Ota tarkasteluun mukaan paitsi palvelun puutteet myös muut lainsäädännölliset vaatimukset. Ota erityisesti huomioon GDPR:n eri vaatimukset.