



## Beveiliging van netwerken en computers (E765003)

Cursusomvang (nominale waarden; effectieve waarden kunnen verschillen per opleiding)

Studiepunten 6.0      Studietijd 170 u      Contacturen 60.0 u

Aanbodssessies en werkvormen in academiejaar 2018-2019

A (semester 1)	Nederlands	hoorcollege	24.0 u
		practicum	36.0 u

Lesgevers in academiejaar 2018-2019

De Poorter, Eli	TW05	Verantwoordelijk lesgever
Van Den Breen, Wim	TW05	Medelesgever

Aangeboden in onderstaande opleidingen in 2018-2019

	stptn	aanbodssessie
<a href="#">Master of Science in de industriële wetenschappen: informatica</a>	6	A

Onderwijstalen

Nederlands

Trefwoorden

computernetwerken, beveiliging, cryptografie, authenticatie, Computerwetenschappen (P170), Informatica (P175), Computertechnologie (T120)

Situering

De studenten kennen de belangrijkste concepten van geheimhouding en authenticatie, ze kennen de toepassingen ervan op de verschillende netwerklagen, ze kennen de verschillende niveaus en manieren hoe een netwerk en computers kunnen beveiligd worden. Ze kennen van al deze concepten zowel de theoretische achtergrond en de algoritmen evenals de toepassingen en zijn in staat om servers en netwerkdevices in een grotere netwerkconfiguratie te beveiligen.

Inhoud

Algemene begrippen. Conventionele en publiekesleutel encryptie. Sleutelbeheer en sleuteluitwisseling. Authenticiteit en handtekeningen. Toepassingen: X.509 certificaten, PGP, S/MIME, PKI, IPSec, SSL en TLS, SET. Firewalls. Systeembeveiliging. Blockchains.

Begincompetenties

**Strikte volgtijdelijkheid :**

Met succes gevolgd hebben van het opleidingsonderdeel 'Computernetwerken II' (E761031) of de erin beoogde competenties op een andere manier hebben verworven (strikte volgtijdelijkheid zoals vastgelegd in de Curriculumregels van de Faculteit Ingenieurswetenschappen en Architectuur, zie <http://www.ugent.be/ea/nl/faculteit/diensten/studentenadministratie/curriculum.htm>)

**Adviserende begincompetenties:**

Een server in unix kunnen opzetten en beheren, een netwerk kunnen opzetten en configureren, Competenties zoals in detail beschreven in Besturingssystemen I en II.

Eindcompetenties

- 1 De belangrijkste concepten en functies van geheimhouding en authenticatie kennen en begrijpen.
- 2 De toepassingen van geheimhouding en authenticatie kunnen instellen op een werkende netwerk- en computerconfiguratie.
- 3 De verschillende niveaus en manieren hoe een netwerk en computers kunnen beveiligd worden, kennen en begrijpen.
- 4 Servers en netwerkdevices in een grotere netwerkconfiguratie te beveiligen.

Creditcontractvoorwaarde

Toelating tot dit opleidingsonderdeel via creditcontract is mogelijk mits gunstige beoordeling van de competenties

#### Examencontractvoorwaarde

Dit opleidingsonderdeel kan niet via examencontract gevolgd worden

#### Didactische werkvormen

Hoorcollege, practicum

#### Toelichtingen bij de didactische werkvormen

Hoorcollege (24u), practicum (36u; aanwezigheid verplicht; opzetten en beveiligen van servers en netwerkconfiguraties, al dan niet in groep), zelfstudie (110u)

#### Leermateriaal

Slides (ENG), notitiepaginass (ENG), referentiewerken, tutorials op internet.

#### Referenties

##### Books

William Stallings, "Cryptography and Network Security, principles and practices", 6th (international) edition, Prentice Hall, 2010; ISBN-13: 9780137056323

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 2001, ISBN 0-8493-8523-7

Matt Bishop, "Computer Security: Art and Science", Addison Wesley, Pearson Education, 2003, ISBN-13: 978-0-201-44099-7

##### Websites

- <https://crypto.stackexchange.com/>
- <http://www.gnupg.org>
- <http://www.openssl.org>
- <http://www.cryptool.org/en/>

#### Vakinhoudelijke studiebegeleiding

De lesgevers zijn ter beschikking voor extra uitleg tijdens de labo's, voor of na de theorielessen en eventueel op andere ogenblikken na afspraak, al dan niet via e-mail.

#### Evaluatiemomenten

periodegebonden en niet-periodegebonden evaluatie

#### Evaluatievormen bij periodegebonden evaluatie in de eerste examenperiode

Schriftelijk examen

#### Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode

Schriftelijk examen

#### Evaluatievormen bij niet-periodegebonden evaluatie

Participatie, vaardigheidstest, verslag

#### Tweede examenkans in geval van niet-periodegebonden evaluatie

Examen in de tweede examenperiode is niet mogelijk

#### Toelichtingen bij de evaluatievormen

Theorie: mondeling examen met schriftelijke voorbereiding (50%).

Labo's: permanente evaluatie via testen en afgeven van opdrachten en verslagen (50%).

#### Eindscoreberekening

De beoordeling en het tot stand komen van de eindquotatie van opleidingsonderdelen gebeurt via het wiskundige gemiddelde volgens de toegekende coëfficiënten. Indien op één van de onderscheiden delen 7 of minder op 20 wordt behaald, wordt er afgeweken van de berekende eindscore indien deze 10 of meer is en haalt de student een 9/20.