



Network and Computer Security

Practical Arrangements

Prof. dr. ir. Eli De Poorter

■ Opleidingsonderdeel

- Beveiliging van netwerken en computers
- 6 studiepunten

■ New teacher, new slides

- In other words: new course
- Mistakes might be present
 - ▶ Grammar, spelling, unclarities, (hopefully not) content
 - ▶ Feel free to report these to me or using the subforum on Minerva
 - ✓ Feedback is always appreciated and will never be held against you!

■ Cursus

- Slides + notepages
- English slides
 - ▶ but Dutch course and examination

■ Minerva

- Slides under /documents
- Additional materials and links

■ Reference book

- William Stallings, “**Cryptography and Network Security, principles and practices**”, 6th (international) edition, Prentice Hall, 2010;
ISBN-13: 9780137056323
 - ▶ Not mandatory
 - ▶ Website: <http://williamstallings.com/Cryptography/>
 - ✓ Useful for errata and additional resources
 - ▶ Older editions (3rd, 4th, and 5th) can still be used
 - ▶ Not mandatory

■ Class hours

- **Theory**

- ▶ Friday, from 10:30 to 12:30, room B4016

- **Labo sessions**

- ▶ Wednesday, from 09:30 to 12:30
- ▶ Normally meant for exercises
- ▶ Also used for company visit and test

■ Literature

- Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, “**Handbook of Applied Cryptography**”, CRC Press, 2001, ISBN 0-8493-8523-7
 - ▶ Rather mathematical approach of cryptography (and somewhat older)
 - ▶ Freely available in pdf format at <http://cacr.uwaterloo.ca/hac/>

■ Literature

- Matt Bishop, “**Computer Security: Art and Science**”, Addison Wesley, Pearson Education, 2003, ISBN-13: 978-0-201-44099-7
 - ▶ A true reference about security (1136 p.)
 - ▶ Also deals with aspects of security policy

■ Software

- Software allowing you to experiment with encryption

- PGP

- ▶ <http://www.gnupg.org>

- ✓ The GPL version

- ▶ <http://www.openpgp.org/>

- OpenSSL

- ▶ <http://www.openssl.org>

- ▶ TLS & SSL + generic toolsets

- CrypTool

- ▶ <http://www.cryptool.org/en/>

- ▶ Educative cryptography software

■ Samenstelling

- **theorie (semesterexamen): 50%**
- **labo: 50%**
 - ▶ alleen raadpleging handleidingen en geselecteerde bronnen
 - ▶ voorbereiding
 - ▶ permanente evaluatie (voorbereiding, activiteiten, verslag)
 - ▶ 1 test (9/12/2014)

■ Minimumvereisten

- **7/20 voor zowel theorie als labo!**

■ Theorie examen

- **Schriftelijk (niet mondeling)**
- **Tekenen voor akkoord**

■ Teacher

- Prof. dr. ir. Eli De Poorter
- E-mail: eli.depoorter@intec.ugent.be
- Information Technology Department
- Gaston Crommenlaan 8, 9050 Gent (Ledeberg)
- Room 2.09b
- Meer info: <http://www.ibcn.intec.ugent.be/route.html>

■ Labo assistants

- Pieter-Jan Maenhaut, PieterJan.Maenhaut@UGent.be
- Wim Van Den Breen, Wim.VanDenBreen@UGent.be