

Post-academic course

ICT Networking and Security

Scientific coordination

Prof. dr. ir. Eric Laermans

Prof. dr. ir. Ingrid Moerman

ir. Andy Van Maele

Department of Information Technology, Ghent University, IBBT

Part I: Communication networks

Module 1: Fixed networks

20, 22, 27 and 29 October, 10, 12 and 19 November 2011

Module 2: IPv6

17, 24 and 26 November 2011

Module 3: Wireless networks

1, 8, 15 and 17 December 2011

Module 4: Multimedia networks

12, 19, 21 and 28 January 2012

Part II: Security

Module 1: Security basics

22 and 29 March 2012

Module 2: Security applications

19 and 26 April, 3, 10, 24 and 31 May 2012

Module 3: Advanced security configuration

28 April, 5, 12 and 26 May and 2 June 2012

Module 4: Organizational Aspects

7 and 14 June 2012

Module 5: Legal aspects

21 June 2012

> With hands-on exercises!
> Possibility to follow
the theoretical lessons
via streaming video!

2nd edition



This programme allows
to obtain a certificate
granted by
Ghent University



Introduction

WHY THIS COURSE?

The world of communication networks has rapidly and thoroughly evolved in the last decades. We have gradually switched from traditional, fixed telephone networks, well controlled by clearly identified operators to mobile, pervasive, more open and ever more complex IP-based networks. The share of voice communication in total network traffic has dwindled, while the amount of data communication over IP-networks from new applications as the Web, streaming media, iDTV, etc. has steadily risen. Even within mobile networks, data communication is taking an ever larger share with smartphones using the latest UMTS-derived technologies. Today, these new data networks even compete with the older, more traditional networks for the telephone service, as Voice-over-IP has become a fierce competitor to the historical telephone operators. This course aims to present the underlying technologies of this relatively new reality.

As long as networks were tightly controlled by well-defined operators, attacks against those networks were sometimes possible, allowing the hacker to pass the bill of his communications to the victim of the hacking, but the amplitude of the attacks and their damage were generally rather limited. The openness of contemporary networks, especially IP-based networks, and the complexity and vulnerability of contemporary terminals (computers or advanced mobile devices), requires much more attention on the security of these networks. Attacks can come from anywhere, at any time. The attack could even originate from the terminal of the user itself in the form of some spyware, leaking precious information to the hacker who planted the piece of malware. Furthermore, as users and enterprises rely more and more on their network infrastructure to do business, the consequences of successful attacks have become more devastating.

The second objective of this course is to allow to understand which security functions and mechanisms exist, how they can be used and implemented to achieve acceptable secure communications.

WHO SHOULD ATTEND?

This course targets people with some technological background, although they don't need to be experts in ICT. The target audience of this course however is twofold: generalist and specialist. The generalist profile has a theoretical interest in ICT, and takes the course for conceptual knowledge. The specialist profile has both a theoretical and practical interest in ICT. The conceptual knowledge will be completed with hands-on training. For the latter, the specialist should have a basic knowledge of working on the Linux command line.

POST-ACADEMIC COURSE CERTIFICATE GRANTED BY GHEENT UNIVERSITY

This programme is part of Ghent University's post-academic courses.

To receive the certificate 'generalist' for Part I, one should at least attend module 1 and the theoretical sessions of modules 2, 3 and 4 of part I and succeed for the final exam. Participants who follow all the modules of part I and succeed for the final exam, will receive the certificate 'specialist' for Part I.

For the certificate 'generalist' of Part II, one should at least attend modules 1, 2, 4 and 5 of Part II and succeed for the final exam. To receive the certificate 'specialist' for Part II, one should attend modules 1, 2, 3 and 4 of part II and succeed for the final exam.

Course certificates are a personal merit: participants who aspire to a certificate cannot be replaced, others can.

Streaming video

There is the possibility to follow the theoretical sessions via streaming video. The lab sessions can't be followed by this method. For more information, please contact us. A demo of this method can be found on: <http://www.ivpv.ugent.be/networking>

Programme

Part I: Communication Networks

Module 1: Fixed Networks

The basis of most contemporary fixed networks is the TCP/IP protocol stack. The objective of this module is to discuss in more detail the several layers of this stack, starting with the application layer and ending with the data link layer. At the application layer, we shall deal with the most common protocols for Web (HTTP), e-mail (SMTP, POP), file transfer (FTP),... One level lower in the protocol stack, at the transport layer, we find the well known TCP and UDP. The transport layer itself relies on the underlying network layer, where the Internet Protocol (IP) is used. At this point routing and network management tools like OSPF, BGP, ICMP, NAT, DHCP,... will also be discussed. Finally, we end with the data link layer protocols such as Ethernet or PPP.

The theory from this module will be illustrated by a series of 4 lab sessions which will give the course members hands-on experience about the operation of basic IP applications, network protocols and basic network configuration.

Teacher: Andy Van Maele

Dates: Theory lessons on 20 and 27 October and 10 November 2011. Lab exercises on 22 and 29 October and 12 and 19 November 2011

Module 2: IPv6

Since long IPv6 is the successor of the IPv4 protocol, but IPv6 remained in the development phase as long as IPv4 addresses were still available. However, the last available class A networks have been assigned in February 2011.

Introducing IPv6 kicks off with the addressing of the new protocol, which now is notated in hexadecimal, and features some quite new concepts (IID, address scopes). Next to the addressing, the ICMPv6 protocol is tackled, covering new IPv6 concepts such as Neighbor Discovery, Duplicate Address Detection and Autoconfiguration.

As IPv4 will be used for many more years, an overview of transition mechanisms towards IPv6 will be presented.

This module will conclude with a case study on transition of an existing IPv4 network to an IPv6 enabled network.

The theory will be complemented by a lab session, where an IPv6 only network will be built, and interconnected to the existing IPv6 Internet.

Teachers: Gunter Van de Velde and Andy Van Maele

Dates: Theory lessons on 17 and 24 November 2011. Lab exercise on 26 November 2011

Module 3: Wireless Networks

Two different kinds of wireless networks will be dealt with in this module. On the one hand, we shall consider mobile communication systems relying on large cellular infrastructures, like GSM and UMTS. On the other hand, this module emphasizes on less "institutional" wireless technologies like WiMAX (wide area networks), WLAN (local networks), Bluetooth and Zigbee (personal area networks) and even RFID (tagging). The module will explain the basic concepts of wireless medium access and discuss the operating principles of the main wireless standards mentioned above. The theoretical part of this module will conclude with a use case study of the rollout of a WLAN in a professional environment.

The theory is further complemented by a lab session where experience will be acquired with the capabilities and configuration of WLAN.

Teachers: Francky Deleu, Piet Demeester and Ingrid Moerman

Dates: Theory lessons on 1, 8 and 15 December 2011. Lab exercise on 17 December 2011

Module 4: Multimedia Networks

The last module of this part about communication networks deals with multimedia networks and the specific network requirements multimedia implies. It is in this module that we shall discuss important concepts as quality of service (QoS), multicast and the nature of Internet traffic, which offers new possibilities that are unavailable in less advanced networks and are useful for the reliable transmission of multimedia data. Voice-over-IP will be considered as a typical multimedia application. Other, more advanced techniques such as SIP (used to support Voice-Over-IP), MPLS (used to support QoS),... will also be handled.

The theory is complemented by a series of 3 lab sessions where experience will be acquired with the nature of video traffic, by configuring a network to support QoS and with SIP.

Teachers: Chris Develder and Andy Van Maele

Dates: Theory lessons on 12 and 19 January 2012. Lab exercises on 21 and 28 January 2012

Modules 1 and 4 of Part I are supported by the reference book 'Computer networking – a top-down approach featuring the internet', 5th edition by J.F. Kurose and K.W. Ross (€ 56,71 incl VAT).

Module 3 of part I is supported by the reference book 'Mobile communications', 2nd edition by J. Schiller (€ 63,00 incl VAT).

The reference book for modules 1 and 2 of Part II is 'Cryptography and Network Security, Principles and Practices', 5th edition by W. Stallings (€ 63,00 incl VAT).

Reference books are billed directly by the bookshop.

Programme

Part II: Security

Module 1: Security Basics

What does information security mean? Which functions can be realized? Why do we need security? These are the questions that should be answered in the first session of this module.

The main basic objectives of information security are discussed: confidentiality, authentication, data-integrity, non-repudiation and availability. We shall show what may happen if insufficient measures are taken to achieve these properties and how people with bad intentions can undermine these objectives to gain an advantage. Besides these basic security concepts, this module also deals with the concrete basic mechanisms that can be used to achieve the desired security objectives. The basic principles of conventional and asymmetric encryption, hash functions, message authentication codes, time stamps, certificates, PKI,... are explained, without plunging into the mathematical details underlying these complex techniques. Biometric techniques will also be shortly discussed here, both with their advantages and their shortcomings.

Teacher: Eric Laermans

Dates: Theory lessons on 22 and 29 March 2012

Module 2: Security Applications

Once the basic building blocks are well understood, we shall try to understand how they are used to achieve security in communication networks, at the different levels of the protocol stack: at application layer (PGP, S/MIME, SSH,...), at the transport layer (TLS/SSL) or at the network layer (IPsec). Related to these secure protocols, we shall also explain how they can be used to create VPNs. The use of these cryptographic security techniques alone is not sufficient to guarantee the security of computer or communication systems. System security measures protection against malware and other intrusions are also essential. This is why we shall also discuss malware protection, firewalls and intrusion detection systems. And finally, as wireless networks are particularly open and vulnerable to attacks, we deal with the specific security measures for wireless networks: from the defective WEP to the improved WPA and WPA2.

This module concludes with two case studies: one about the rollout of security measures in a professional environment and one about the use of tokens for security.

Teachers: Eric Laermans, Dimitri Roman and Tim Stevens

Dates: Theory lessons on 19 and 26 April, 3, 10, 24 and 31 May 2012

Module 3: Advanced security configuration

To those who are already more familiar with ICT and security, this module is devoted to the more advanced practical aspects of information security. In a series of 4 lab sessions, hands-on experience will be obtained in advanced PC security, authentication services with a RADIUS server and advanced security aspects of wireless networks.

Teacher: Andy Van Maele

Dates: Lab exercises on 28 April, 5, 12 and 26 May and 2 June 2012

Module 4: Organizational aspects

Security is not just a matter of technology. The organizational aspects certainly are not less important. In this module, we shall see how information security can be organized within a company: how security policies are designed and implemented and how a company can respond to security incidents. Attention will also be given to the control and auditing of security policies, for which CobiT is an important standard.

Teacher: Marc Vael

Dates: Theory lessons on 7 and 14 June 2012

Module 5: Legal aspects

The security part of this course concludes with a module about the legal aspects of security. Which activities (hacking, identity theft,...) can be considered illegal? What are the legal measures against computer crime? Another important legal aspect of information security is the protection of personal data (of customers or employees). This module also discusses the obligations of a company to achieve an acceptable level of information security. Besides protection against attacks, we also deal with the legal framework for electronic signatures and e-commerce.

Teacher: Paul De Hert

Date: Theory lesson on 21 June 2012

Teachers

SCIENTIFIC COORDINATION:



Prof. dr. ir. Eric Laermans
Department of Information
Technology, Ghent University,
IBBT



Prof. dr. ir. Ingrid Moerman
Department of Information
Technology, Ghent University,
IBBT



ir. Andy Van Maele
Department of Information
Technology, Ghent University,
IBBT

TEACHERS:

- > **Paul De Hert**, Law Science Technology & Society, Vrije Universiteit Brussel
- > **Francky Deleu**, Jan Yperman Hospital
- > **Piet Demeester**, Department of Information Technology, Ghent University, IBBT
- > **Chris Develder**, Department of Information Technology, Ghent University, IBBT
- > **Eric Laermans**, Department of Information Technology, Ghent University, IBBT
- > **Ingrid Moerman**, Department of Information Technology, Ghent University, IBBT
- > **Dimitri Roman**, VASCO Data Security International
- > **Tim Stevens**, National Bank of Belgium
- > **Marc Vael**, Smals
- > **Gunter Van de Velde**, Cisco
- > **Andy Van Maele**, Department of Information Technology, Ghent University, IBBT

Subscription form

Preferably via www.ipvv.ugent.be/networking OR by using this form:

- > **by mail:** Ghent University- Institute for Continuing Education (IVPV) – attention of Els Van Lierde, Technologiepark 913, 9052 Zwijnaarde, Belgium
- > **by fax:** IVPV +32 9 264 56 05

	Fee Generalist track	Fee Specialist track
Part I: Communication networks		
Module 1: Fixed networks	<input type="checkbox"/> € 1.050	<input type="checkbox"/> € 1.050
Module 2: IPv6	<input type="checkbox"/> € 300*	<input type="checkbox"/> € 450
Module 3: Wireless networks	<input type="checkbox"/> € 450*	<input type="checkbox"/> € 600
Module 4: Multimedia networks	<input type="checkbox"/> € 300*	<input type="checkbox"/> € 600
Complete package	<input type="checkbox"/> € 1.680	<input type="checkbox"/> € 2.160
Part II: Security		
Module 1: Security basics	<input type="checkbox"/> € 300	<input type="checkbox"/> € 300
Module 2: Security applications	<input type="checkbox"/> € 900	<input type="checkbox"/> € 900
Module 3: Advanced security configuration		<input type="checkbox"/> € 750
Module 4: Organizational aspects	<input type="checkbox"/> € 300	<input type="checkbox"/> € 300
Module 5: Legal aspects	<input type="checkbox"/> € 150	<input type="checkbox"/> € 150
Complete package	<input type="checkbox"/> € 1.320	<input type="checkbox"/> € 1.920
All modules Part I & II		<input type="checkbox"/> € 3.570

* Remark: the Generalist track does not include the hands-on labs of Modules 2 to 4 of part I.

- I want to follow the theoretical sessions via streaming video.

Reference Books

- 'Computer networking – a top-down approach featuring the internet', 5th edition' by J.F. Kurose and K.W. Ross (€ 56,71 incl VAT) (reference book for Part I, modules 1 and 4)
- 'Mobile communications', 2nd edition by J. Schiller (€ 63,00 incl VAT) (reference book for Part I, module 3)
- 'Cryptography and Network Security, Principles and Practices', 5th edition by W. Stallings (€ 63,00 incl VAT) (reference book for Part II, modules 1 and 2)

Return completed and signed form (use capitals):

Name: _____

First name: _____ M F

Private-address: _____

Street: _____ N°: _____

Zip: _____ City: _____ Country: _____

Telephone: _____

Company: _____

Function: _____

Company address: _____

Street: _____ N°: _____

Zip: _____ City: _____ Country: _____

Telephone: _____ Fax: _____

E-mail: _____

VAT n°: _____

Invoice: Company Private

Date: _____ Signature: _____

Your address data are incorporated by the IVPV in a database in order to be able to keep you informed of our activities and programmes. In accordance with the law from 8/12/1992 safeguarding personal privacy with respect to the processing of personal data, you are entitled to examine, correct or cancel this information kept by the IVPV.

Practical info

PRACTICAL INFORMATION

The programme consists of different modules. Each module can be followed separately. The theoretical lessons are organized as follows:

- > 18h00 – 19h30: session 1
- > 19h30 – 20h00: sandwich break
- > 20h00 – 21h30: session 2

A detailed timetable for the lab sessions will be announced later. Extra lab sessions will be organized if necessary.

LOCATION

- > Theoretical lessons: Ghent University, Institute for Continuing Education, Campus Engineering Faculty, Building Magnel, IVPV classroom A, Technologiepark 904, 9052 Zwijnaarde, Belgium
- > Lab sessions: Ghent University, IBBT, Zuiderpoort Office Park, Gaston Crommenlaan 8, 9050 Gent-Ledeberg, Belgium

STREAMING VIDEO

The theoretical lessons can be attended via streaming video. For more information, please contact us. A demo of this method can be found on <http://www.ivpv.ugent.be/networking>

PARTICIPATION FEE

The participation fee includes the tuition fee, course notes, soft drinks, coffee and sandwiches. Payment occurs after reception of the invoice. All invoices are due in thirty days. All fees are exempt from VAT. Travelling expenses and accommodation are at the expense of the participant.

	Fee Generalist track	Fee Specialist track
Part I: Communication networks		
Module 1: Fixed networks	€ 1.050	€ 1.050
Module 2: IPv6	€ 300*	€ 450
Module 3: Wireless networks	€ 450*	€ 600
Module 4: Multimedia networks	€ 300*	€ 600
Complete package	€ 1.680	€ 2.160
Part II: Security		
Module 1: Security basics	€ 300	€ 300
Module 2: Security applications	€ 900	€ 900
Module 3: Advanced security configuration		€ 750
Module 4: Organizational aspects	€ 300	€ 300
Module 5: Legal aspects	€ 150	€ 150
Complete package	€ 1.320	€ 1.920
All modules Part I & II		€ 3.570

* Remark: the Generalist track does not include the hands-on labs of Modules 2 to 4 of part I.

When a participant of a company subscribes for the complete course, a reduction of 20% is given to all additional subscriptions from the same company, even on single modules. Invoicing is then done by one company invoice. For larger numbers of subscriptions, additional reductions can be envisaged.

REFERENCE BOOKS

- > 'Computer networking – a top-down approach featuring the internet', 5th edition by J.F. Kurose and K.W. Ross (€ 56,71 incl VAT) (reference book for Part I, modules 1 and 4)
- > 'Mobile communications', 2nd edition by J. Schiller (€ 63,00 incl VAT) (reference book for Part I, module 3)
- > 'Cryptography and Network Security, Principles and Practices' by W. Stallings (€ 63,00 incl VAT) (reference book for Part II, modules 1 and 2)

Reference books are billed directly by the bookshop.

LANGUAGE

English is used in all presentations, lab exercises and documentation, so a good knowledge of this language is required.

CANCELLATION POLICY

When cancelling up to 10 days before the start of the course or module, 25% of the participation fee will be charged. When cancelling less than 10 days before the start of the module, the full fee is due.

TRAINING CHEQUES

Ghent University has been recognized as an official training supplier within the framework of the training cheques of the Flemish Community.

Thereby you can save on the participation fee of this training (<http://www.vdab.be/opleidingscheques>).

For employers we refer to the KMO-portefeuille (www.kmo-portefeuille.be; use authorization ID: DV.0103 194).

INFORMATION & DOCUMENTATION

All the information of this course can be found on: <http://www.ivpv.ugent.be/networking>

Institute for Continuing Education
Instituut voor Permanente Vorming (IVPV)
Secretariat: Els Van Lierde
Technologiepark 913, 9052 Zwijnaarde, Belgium
Tel: +32 9 264 55 82, Fax: +32 9 264 56 05
E-mail: ivpv@UGent.be

Dates may change due to unforeseen reasons.