F21CN: Computer Network Security: Overview

Hans-Wolfgang Loidl

http://www.macs.hw.ac.uk/~hwloidl

School of Mathematical and Computer Sciences
Heriot-Watt University, Edinburgh

1. Overview
2. Topic
3. Syllabus
4. Assessment
5. Reading List

Welcome to Computer Network Security

Hans-Wolfgang Loidl

Hamish Taylor

Welcome to Computer Network Security!

F29CN/F20CN/F21CN Computer Network Security

Welcome to Computer Network Security

Hans-Wolfgang Loidl

Hamish Taylor

Welcome to Computer Network Security!

F29CN/F20CN/F21CN Computer Network Security

Purpose of this course

The purpose of Course F21CN "Computer Network Security" is to provide a solid understanding of the main issues related to security in modern networked computer systems. This covers underlying **concepts and foundations** of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, **techniques to secure complex systems** and practical **skills in managing** a range of systems, from personal laptop to large-scale infrastructures. The course structure is designed to provide solid foundations in the first half of the course, and discuss concrete application scenarios in the second half.

Learning Objectives

- Extensive, detailed and critical understanding of the **concepts, issues, principles and theories of computer network security**
- Detailed and practical understanding of formalisms for specifying security related properties and validating them using model checking
- Critical theoretical and detailed practical knowledge of a range of **computer network security technologies** as well as network security tools and services
- Practical experience of analysing, designing, implementing and validating solutions to computer network security challenges using common **network security tools and formal methods**.

Concrete graduate skills imparted:

- **Understand** the concepts and foundations of computer security, and **identify** vulnerabilities of IT systems.
- **Use** basic security tools to enhance system security.
- **Develop** basic security enhancements in standalone applications.
- **Reflect** on tools and technologies.

Learning Objectives

- Extensive, detailed and critical understanding of the **concepts, issues, principles and theories of computer network security**
- Detailed and practical understanding of formalisms for specifying security related properties and validating them using model checking
- Critical theoretical and detailed practical knowledge of a range of **computer network security technologies** as well as network security tools and services
- Practical experience of analysing, designing, implementing and validating solutions to computer network security challenges using common **network security tools and formal methods**.

Concrete graduate skills imparted:

- **Understand** the concepts and foundations of computer security, and **identify** vulnerabilities of IT systems.
- **Use** basic security tools to enhance system security.
- **Develop** basic security enhancements in standalone applications.
- **Reflect** on tools and technologies.

Pre-requisites

Pre-requisites for this course are:

- ~~Basic knowledge of computer networking,~~
- Foundational knowledge of formal methods,
- **Basic Linux and shell usage**,
- **Solid Java programming skills**.

A general interest in

- foundations of security,
- programming,
- systems building.

Pre-requisites

Pre-requisites for this course are:

- ~~Basic knowledge of computer networking,~~
- Foundational knowledge of formal methods,
- **Basic Linux and shell usage**,
- **Solid Java programming skills**.

A general interest in

- foundations of security,
- programming,
- systems building.

Related Courses

At Heriot-Watt

- F28DA “Data Structures and Algorithms” gives a short overview of cryptographic algorithms. F28DA is a useful basis for the first half of the course, but not a pre-requisite

Compared to other (on-line) courses:

- Stronger focus on **foundations and concepts** of security
- Provides a solid basis to assess not only concrete threats today, but potential threats in the future, too
- Practicals are used to deepen the understanding
- Research topics give an outlook to further developments

Topic: Computer Network Security

- **Security** is about protecting assets.
- **Computer Security** concerns assets of computer systems: the information and services they provide.
- **Computer Network Security** focuses on the protection of assets on computers that are connected and can be accessed remotely.

This is a vast area, with techniques depending on the desired security level. In this course we focus on

- foundations and concepts of security, e.g. cryptography
- techniques to secure systems in internet-style networks, e.g. PGP for secure email
- research topics, giving an outlook of new technologies to secure systems, e.g. proof-carrying-code

Topic: Computer Network Security

- **Security** is about protecting assets.
- **Computer Security** concerns assets of computer systems: the information and services they provide.
- **Computer Network Security** focuses on the protection of assets on computers that are connected and can be accessed remotely.

This is a vast area, with techniques depending on the desired security level. In this course we focus on

- foundations and concepts of security, e.g. cryptography
- techniques to secure systems in internet-style networks, e.g. PGP for secure email
- research topics, giving an outlook of new technologies to secure systems, e.g. proof-carrying-code

Non-topics

This course will **not** cover

- Guidelines for hacking systems
- anecdots of hacking systems
- how-to guides for specific tools (but there will be practicals using tools)
- a system administrator handbook (see reading list)
- broad coverage of socio-technological aspects

Computer Security and Ethics

- Learning about potential threats should not be seen as an incentive to hack into systems
- There will be practicals, later in the course, to exercise threats in a controlled environment
- If you learn about or discover a security weakness, inform the sys admin rather than trying to exploit it
- Trying to exploit a security weakness is a gross violation of the Code of Ethics and will have consequences!

Syllabus

The first half of the course focuses on foundations for network security

- **Week 1**: Overview of the course. Network security concepts. Computer Security Landscape. (HWL)
- **Week 2**: Cryptography overview and concepts. Cryptography (symmetric, asymetric encryption). (HWL)
- **Week 3**: Cryptography (modes). (HWL) Computer networking (models, Internet network layers, etc). Network security concepts. (HT)
- **Week 4**: Computer Networks: Sockets & Services (HT)
- **Week 5**: Ciphers & Digests; Certificates & Signatures; SSL (HT)
- **Week 6**: PGP Public Keys; PGP Applications (HT)

Syllabus (cont'd)

The second half of the course focuses on practical network security and research topics

- **Week 7**: RMI I & RMI II (HT)
- **Week 8**: Web Security: Firewalls, VPNs, IDSs, malware scanners. (HT)
- **Week 9**: Operating system security (HWL)
- **Week 10**: Operating & distributed system security (HWL)
- **Week 11**: Proof-carrying-code (HWL)
- **Week 12**: Revision session (HWL,HT)

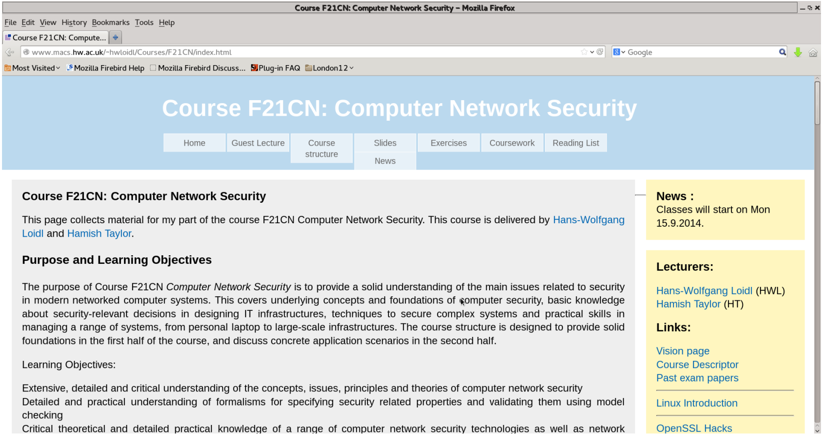
Lectures and Labs

Main web page for the course: `http://www.macs.hw.ac.uk/~hwloidl/Courses/F21CN/index.html`

Vision page for the course: `http://vision.hw.ac.uk/`

- 2 lectures per week:
  - Mon 12:15 HN LT2
  - Tue 9:15 EM 1.83
- 1 lab per week
  - Mon 17:15 EM 2.50 (Linux lab) **Week 1: EM 1.83**

Main Course Information Page



Course F21CN: Computer Network Security – Mozilla Firefox
File Edit View History Bookmarks Tools Help
Course F21CN: Compute...
www.macs.hw.ac.uk/~hwloidl/Courses/F21CN/index.html
Google
Most Visited
Mozilla Firebird Help
Mozilla Firebird Discuss...
Plug-in FAQ
London12
Home
Guest Lecture
Course structure
Slides
News
Exercises
Coursework
Reading List

Course F21CN: Computer Network Security

Course F21CN: Computer Network Security

This page collects material for my part of the course F21CN Computer Network Security. This course is delivered by Hans-Wolfgang Loidl and Hamish Taylor.

Purpose and Learning Objectives

The purpose of Course F21CN *Computer Network Security* is to provide a solid understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures. The course structure is designed to provide solid foundations in the first half of the course, and discuss concrete application scenarios in the second half.

Learning Objectives:

Extensive, detailed and critical understanding of the concepts, issues, principles and theories of computer network security
Detailed and practical understanding of formalisms for specifying security related properties and validating them using model checking
Critical theoretical and detailed practical knowledge of a range of computer network security technologies as well as network

News :
Classes will start on Mon 15.9.2014.

Lecturers:

Hans-Wolfgang Loidl (HWL)
Hamish Taylor (HT)

Links:

Vision page
Course Descriptor
Past exam papers

Linux Introduction

OpenSSL Hacks

Assessment

Assessment consist of two parts

- 60%/50% Coursework:
  - Cryptography **28.9.–10.10**
  - Certificates for network security **26.10.–14.11.**
- 40%/50% Exam:
  - 2 hours, written exam
  - topics from across the course
  - during exam period: 8–19th December
- Re-assessment is possible in summer (exam)

Main resources for the course

- Michael T. Goodrich and Roberto Tamassia *“Introduction to Computer Security”*, Addison Wesley, 2011. ISBN: 0-32-151294-4
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *“Handbook of Applied Cryptography”*, CRC Press, 2001. ISBN 0-8493-8523-7. On-line: `http://www.cacr.math.uwaterloo.ca/hac/`
- Bruce Schneier, *“Applied Cryptography”*, John Wiley & Sons, 1996. ISBN 0-471-12845-7. On-line: `http://www.cse.iitk.ac.in/users/anuag/crypto.pdf`
- William Stallings *“Network Security Essentials: Applications and Standards”*, Prentice Hall, 4th edition, 2010. ISBN 0-13-610805-9.

Reading List: General computer security

- Michael T. Goodrich and Roberto Tamassia *“Introduction to Computer Security”*,
  Addison Wesley, 2011. ISBN: 0-32-151294-4
  Good general, up-to-date introduction to the entire range of computer security, with very useful practicals from the SEED project.
- Dieter Gollmann, *“Computer Security”*,
  John Wiley & Sons, 3rd edition, John Wiley & Sons, 2010.
  Well-established textbook with general coverage of computer security.
- Matt Bishop, *“Computer Security: art and science”*,
  Addison Wesley, 2003.
  Good general coverage of computer security.

Reading List: Computer Network Security:

- William Stallings *“Network Security Essentials: Applications and Standards”*, Prentice Hall, 4th edition, 2010. ISBN 0-13-610805-9.
  Good up-to-date textbook focusing on network security.
- Joseph Migga Kizza, *“A Guide to Computer Network Security”*, Springer 2009. ISBN 978-1-84800-916-5.
  Good coverage across the field of network security, with detailed coverage of network protocols, certificates etc.

Reading List: Cryptography

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *“Handbook of Applied Cryptography”*, CRC Press, 2001. ISBN 0-8493-8523-7. On-line: `http://www.cacr.math.uwaterloo.ca/hac/`
  The bible/koran of cryptography, with detailed coverage of foundations, mathematical background, and efficient implementation of cryptographic algorithms. Fully available online.
- Bruce Schneier, *“Applied Cryptography”*, John Wiley & Sons, 1996. ISBN 0-471-12845-7. On-line: `http://www.cse.iitk.ac.in/users/anuag/crypto.pdf`
  Cryptography from a more practical, programming side, including source code etc. Fully available online
- Nigel Smart, *“Cryptography: An Introduction”*, On-line: `http://www.cs.bris.ac.uk/~nigel/Crypto_Book/`
  General introduction to security, fully available online, but a bit dated.
- William Stallings, *“Cyptography and Network Security”*,

Reading List: Security Mangement

- Edward Skoudis, Tom Liston, *"Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses"*, Prentice Hall, 2nd edition, 2006. ISBN 0131481045.

  A useful practical handbook for system administrators and a resource for securing your own systems.

- Mark Burgess,, *"Principles of Network and System Administration"*, John Wiley & Sons Ltd, 2nd Edition, 2004. ISBN 978-0-470-86807-2.

  Network security from a sysadmin point of view, with practical guidelines.

- Limoncelli, Hogan and Chalup, *"The Practice of System and Network Administration"* Addison Wesley, 2nd Edition, 2007. ISBN 978-0-321-49266-1.

  Handbook for system management from a business management point of view. Detailed coverage of good practice guidelines, not very detailed in the underlying techniques or foundations.

Reading List: Security Engineering

- Ross Anderson, *“Security Engineering”*, John Wiley & Sons Ltd, 2001.
  On-line: `http://www.cl.cam.ac.uk/~rja14/book.html`.
  Security from an engineering and system building point of view, focusing on how to build secure systems in-the-large. An old edition of this book is fully available online.
- Mark Curphey *et al*
  “A Guide to Building Secure Web Applications”,
  Open Web Application Security Project, 2002
  On-line book: `http://www.cgisecurity.com/owasp/html/`
  Security engineering specifically for web applications. Technologies are dated, but principles still valid.

On-line courses

- David Aspinall et al, University of Edinburgh. *"Computer Security"*, On-line: `http://www.inf.ed.ac.uk/teaching/courses/cs/` Excellent course material, including complete set of slides and detailed reading list. Very solid foundations of security in general, with practical applications in various areas.
- Br. David Carlson, Saint Vincent College *"Computer Security"* `http://cis.stvincent.edu/carlsond/cs225/syll225.html` Broader coverage of security, involving various socio-technological aspects.
- Wenliang Du, Syracuse University, Department of Electrical Engineering and Computer Science. *"The SEED Project: Developing Hands-on Labs for Computer SEcurity EDucation"* On-line: `http://www.cis.syr.edu/~wedu/seed/index.html` A rich set of practicals from all areas of computer security. We will use some of the practicals in this course.