

# Computer Systems and Network Security

PhD Program, DI-FCT-UNL

Henrique João L. Domingos

# Course Overview

- Initial information
- Course topics / Objectives
- Background / Requirements
- Bibliography
- Assessment
- Classes / Course Planning

# Initial information

- Contacts:
  - Henrique João L. Domingos
  - Office: room P2/6, DI/FCT/UNL – CITI building
  - Students (direct contact): Friday, 14h-15h
  - Int. Phone Ext. 10727, Email: [hj@di.fct.unl.pt](mailto:hj@di.fct.unl.pt)
- Web information
  - <http://asc.di.fct.unl.pt/~hj/cscs-phd>
  - Public info + Access-Restricted (pwd) area for registered students
- Calendar:
  - Course-Overview/Presentation: 16/Oct/09
  - Classes + mid-term assessment:
    - From 23/Oct/09 to 5/Fev/10 (14 weeks)
  - Exams / Final assessment: until 28/Feb

# Course Topics and Background

(Ref. in DI-FCT-UNL)

BSC Level (1<sup>st</sup> Cycle – Bologna): 3 anos

Profile: Ciências de Engenharia



MSC Level (2<sup>nd</sup> Cycle – Bologna): 2 anos

Specialization Profile: Sistemas e Redes de Computadores



PHD Level (3<sup>rd</sup> Cycle – Bologna): 2 anos

PhD Thesis Topic:

**Distributed Systems Security / Computer Systems and Communications Security**

- ISRC – Introd. Aos Sistemas e Redes de Computadores
- RC Redes de Computadores
- SD Sistemas Distribuidos
- AC Arquitectura de Computadores
- FSO Fund. Sist. Operativos
- Programming principles and practice (IP – AED – LAP)

- Sistemas Distribuídos
- Redes de Comp. TCP/IP
- Seg. Em Sistemas e Redes de Comp.
- Sist. Comput. Móvel e Ubíqua
- Sist. e Tecnol. de Middleware

- Computer Systems and Com. Security
- Thesis Preparation

# Course Topics

- Concepts, Terminology, Framework OSI x.800 vs. RFC 2828 / Classic Adversary Models
- Rev. Computational Crypto / Math foundations
- Rev. Security Services and Protocols (TCP/IP Framework)
  - Security models and frameworks
  - Attack models, Security (specific and pervasive) Mechanisms and Security Services
  - TCP/IP Stack and Security Services
- New Adversary models / selfish environments and dependability issues
  - Dolev-Yao based model vs. Intrusion-Based models
  - Case of AdHoc Nets, Manets, WSNs: Attack models and security services
  - Byzantine adversary models
  - Intrusion Tolerance in Selfish Environments in a Dependable Systems Vision
  - Byzantine + Probabilistic Adversary Models
- Wireless Ad-Hoc and Sensor Networks Security
  - MAC-Layer protection / Sec. Communication Primitives
  - Network Level: Secure Routing / Data-Dissemination
  - Key-Establishment
  - Secure Network Processing and Data-Aggregation
  - Pro-active resilience based on randomized solutions

# Background / Requirements

- **M)** Good background on Computer Networks (TCP/IP stack) and Distributed Systems (architectural concepts, design principles and paradigms)
  - Ex., J. Kurose, Computer Networking: a top down approach featuring the Internet, Addison
  - Ex., A. Tanenbaum, Computer Networks, Prentice Hall
  - Ex., G. Coulouris et. al., Distributed Systems: concepts and Design, Addison Wesley
  - Ex., A. Tanenbaum, Marteen Van Steen, Distributed Systems: Principles and Paradigms, Prentice Hall
- **M)** Previous background on Computer Networks and Distributed Systems Security
  - Ex., W. Stallings, Cryptography and Network Security, Person/Prentice Hall
  - Ex., Ross Anderson, A Guide to Building Dependable Distributed Systems
- **M)** Programming practice / autonomy: JAVA-J2EE, IDE (ex., Eclipse, etc), Java-Network Programming (TCP/IP, Sockets, RMI, WS...)
  - Ex. Elliotte Rusty Harold, Java Network Programming, O'Reilly
- **M)** Programming practice / autonomy: JCA/JCE, Java Security
  - Ex., Scott Oaks, Java Security, O'Reilly
  - Ex., David Hook, Cryptography with Java, Wrox Ed.
- **F)** Knowledge on Mobile Computing issues (802.11, WI-Fi, ...) and programming practice (MIDPs, JAVA JME,...)
- **F++)** Use of Net Simulators or WSN simulators (ex., NS2, ... TOSSIM/TinyOS, Jprowler, ... )

# WSN Simulation Environments & Tools

- TOSSIM/TinyOS
  - <http://www.tinyos.net/>
- Jproowler:
  - <http://www.escherinstitute.org/Plone/frameworks/nes/tools/prowler>
  - <http://www.isis.vanderbilt.edu/projects/nest/jprowler/index.html>
- Others... (research)

# Bibliography (books)

- W. Stallings, Computer Security, Principles and Practice, Prentice Hall, 2008
- W. Stallings, Cryptography and Network Security, Prentice Hall, 2006
  - W. Stallings, Network Security Essentials: Applications and Standards, 3/E, 2007
- F. Adelstein, S. Gupta, G. Richard III and L. Schwiebert, Fundamentals of Mobile and Pervasive Computing, McGraw Hill, 2005
- Security in Sensor Networks, Ed. By Yang Xiao, Auerbach Publications, 2007
- Wireless Sensor Network Security, IOS Press, Ed. By J. Lopez and J. Zhou, 2008

*More about bibliography : see the course web page*

# Bibliography (compl.)

- Suggested readings / selected papers on topics of Security for *AdHoc* and *WSNs*
  - Introduced / mapped in lectures (course plan)
  - Base bibliography
    - Topics presentation by students

# Assessment

- 2 mid-term freq. tests (2 parts: closed-book and open-book)
  - on pre-suggested readings
  - 25 % of final assessment
- 2 mid-term work-assignments (group work, 2 students)
  - On selected topics / bibliog. Readings + lab work
  - 25 % of final assessment
- Final Exam + Final individual project/work assignment
  - 50 % of the final assessment (25% each)

# Course orientation vs. assessment (1)

- IP: Instructor lectures and slides introducing the topics, with suggested readings (mainly book-chapters)
- SP: students prepare a summary-survey on selected papers and bibliog. research and present specific topics (from suggested topics)
- WAP: presentations by students – work-assignments, papers/tech. reports and lab/demos
  - Typically organized in two workshops to be planned (extra-classes)

# Calendar (init. Approach) (1)

- **W1:** 16/Oct/09
- **W2:** 19-23 Oct
- **W3:** 26-30 Oct
- **W4:** 2-6 Nov
- **Week 9-13 Nov**
- **W5:** 16-20 Nov
- **W6:** 23-27 Nov
- **W7:** 30/Nov – 4/Dec
- **W8:** 7/Dec – 11/Dec

SPs

No classes.  
1<sup>st</sup> Work Assignments

1<sup>st</sup> Work assignment deliverables  
(specific pres/demo/dic.  
workshop plan **WAP**)

1st mid-term freq. test

SPs

# Calendar (init. Approach) (2)

- **W9:** 14/Dec-18/Dec
- **Week 21/Dec - 01/Jan** → No classes  
2<sup>nd</sup> Work Assignments
- **W10:** 4/Jan – 8/Jan
- **W11:** 11/Jan – 15/Jan SP
- **W12:** 18/Jan – 22/Jan SP
- **W13:** 25/Jan – 29/Jan: → 2<sup>nd</sup> Mid Term Freq. Test  
2<sup>nd</sup> Work-Assignment deliverables  
(specific pres/demo/disc.Plan **WAP**)
- **W14:** 1-5/Fev: Final Freq. Assessment and  
Conclusion. Final Proj. Assignments

# Starting / Revision / Readings

- Revise the background/requirements and related bibliography
- First week (preparation):
  - W. Stallings, Cryptography and Network Security, Prentice Hall, 2006, Chap. 1  
or
  - W. Stallings, Network Security Essentials: Applications and Standards, 3/E, 2007, Chap. 1  
or
  - W. Stallings, Computer Security, Principles and Practice, Prentice Hall, 2008, Chap. 1