1EL6000 – Networks and Security

Instructors: Pierre Wilke
Department: CAMPUS DE RENNES
Language of instruction: FRANCAIS, ANGLAIS
Campus: CAMPUS DE PARIS - SACLAY
Workload (HEE): 60
On-site hours (HPE): 35,00

Description

This course aims to provide CentraleSupélec students with basic knowledge in computer networking, as well as a reasonable awareness of information security issues.
Regarding networking, the mechanisms allowing users like us to browse and use Internet services will be highlighted. Thus, the various network layers, from the physical to the applicative level, will be introduced, as well as additional network services such as DNS (Domain Name System). Hands-on and tutorial sessions will allow students to face the actual implementation of the various concepts covered, in realistic situations and systems.
Regarding information security, lectures will introduce fundamental concepts and will succintly present a few security mechanisms. They will be complemented by lab sessions illustrating various security risks and the associated countermeasures.

Quarter number
SG1 and SG3

Prerequisites (in terms of CS courses)

- Information systems and programming
- Basic Python programming

Syllabus
Part 1 : Networking – lower layers

- Physical layer / data link layer (Ethernet and 802.11)
- Address Resolution Protocol (ARP), Media Access Control (MAC) addresses

Part 2 : Networking – intermediate layers

1. IP protocol and addresses
2. IP routing and routing protocols

3. Transport protocols (TCP and UDP)
4. Tutorial 1 : Network traffic analysis (Wireshark)
5. Tutorial 2 : Specification of a communication protocol
6. Lab 1 : Networking equipment handling (routers / switches)
7. Personal work: Border Gateway Protocol (BGP), peering, IPv4-IPv6 migration, congestion control, flow control, QoS...

Part 3 : Networking – Applicative layers and services

- Domain name resolution (DNS)
- HTTP protocol, web technologies
- Tutorial 3 : Implementation of the protocol specified in tutorial 2, in Python (socket programming)
- Personal work: e-mail protocols (IMAP, POP, SMTP), directories (LDAP)...

Part 4 : Information security

- Introduction to information security, fundamentals
- Legal and social aspects
- Introduction to cryptography and cryptographic protocols
- Introduction to malware
- Lab 2 : Virtual Private Networks (VPN)
- Lab 3 : Web application security
- Personal work: IPSec, DNSSec, TLS, secure instant messaging...

Class components (lecture, labs, etc.)
Networking – lower layers: lecture (3h)
Networking – intermediate layers: lecture (3h), tutorial (6h), lab (3h), personal work (9h)
Networking – Applicative layers and services : lecture (3h), tutorial (3h), personal work (9h)
Information security : lecture (6h), lab (6h), personal work (10h)
Written exam (2h)

Occurrences 1.2 and 1.4 are taught in French
Occurrence 1.3 is taught in English

Grading
The evaluation will be the average of a written examination at the end of the session (CF) lasting 2h and the evaluation of the labs 1 and 2 (mandatory evaluation)
- 50% final exam (written, multiple choice questions, no documents)
- 25% lab 1
- 25% lab 2

Lab grades always participate in the final grade, whether they improve it or not.

Course support, bibliography

Lecture slides provided in electronic format
Books :

- J.F. Kurose and K.W. Ross, *Computer Networking : A Top-Down Approach*, 7th ed. Eyrolles. Pearson. ISBN : 978-0133594140
- Ross J. Anderson, *Security Engineering : A Guide to Building Dependable Distributed Systems*, 2nd Edition. Wiley. ISBN : 978-0470068526 (available online on https://www.cl.cam.ac.uk/~rja14/book.html)

MOOC :

- Stanford Online : *Introduction to Computer Networking* (https://lagunita.stanford.edu/courses/Engineering/Networking-SP/SelfPaced/about)
- Coursera / Université du Maryland : *spécialisation Cybersécurité* (https://www.coursera.org/specializations/cyber-security)
- Cisco Networking Academy: CCNA1 and CCNA2 modules (https://netacad.centralesupelec.fr/)

Resources

- Teaching staff : Rennes/CIDRE team members, as well as Paris-Saclay teachers (computing and telecommunications departments);
- Most tutorials and lab sessions require a personal laptop ;
- Software used: Wireshark, Python, VirtualBox, OpenVPN (all free/open source);
- Some tutorials and lab sessions involve specific networking equipment ;
- Some lectures may be presented remotely from Rennes.

Learning outcomes covered on the course

After completion of this course, students will be able to:

- Know TCP/IP computer networking concepts, protocols and mechanisms;
- Analyse the network activity generated by web applications ;
- Know the main types of cryptographic schemes;
- Know techniques used by malware ;
- Set up and manage switched and routed computer networks ;
- Design and implement an applicative communication protocol;

- Set up and configure a Virtual Private Network (VPN) ;
- Detect and analyse some web application vulnerabilities.

Description of the skills acquired at the end of the course

- C1.1 - Examine a problem in full breadth and depth, within and beyond its immediate parameters, thus understanding it as a whole. This whole weaves the scientific, economic and social dimensions of the problem.Examine a problem in full breadth and depth, within and beyond its immediate parameters, thus understanding it as a whole. This whole weaves the scientific, economic and social dimensions of the problem
- C1.4 - Design, detail and corroborate a whole or part of a complex system
- C2.1 - Thoroughly master a domain or discipline based on the fundamental sciences or the engineering sciences.