Minor in

INFORMATION SECURITY

esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

at ESIEA Laval, France

Program Strengths

Provides a thorough overview of information and network security, from secure programming to risk management within a company.

Program developed by Prof. Dr. Eric Filiol, an internationally recognised expert in the field of computer security and the lead teacher in the minor.

Taught within ESIEA's research laboratory CVO°, headed by Prof. Dr. Filiol and dedicated to operational cryptology and virology.

Case studies of real-life situations the laboratory has had to manage (in companies, in the criminal justice system…)

Do you have what it takes?

- You have a strong interest in information security issues.
- You're a good programmer and you have solid working knowledge of C.
- You are highly motivated and not afraid of hard work.
- You would like to discover France, its language, its culture and its people.
- If you've answered YES to all four questions, then→

YOU ARE THE PERFECT CANDIDATE FOR THIS PROGRAM!

Program Organization

- Orientation week beginning of September
- Courses run from the 2nd week of September to Christmas, starting September 2014
- Each module is organised over one week (18 hours of contact + individual assignments)
- 2 hours of French classes every week
- Opportunity to meet and interview with companies at our « Forum Entreprises » in November
- Possibility of staying for a major project over the second semester (January-May)

Program Content—Overview

Course title	Contact hours	ECTS
Information Theory	18	2
Maths for Information Security	18	2
Code Theory	18	2
Networks : Local Security	18	2
Networks : Security Architecture	18	2
Secure Programming	18	2
Smart Cards	18	2
Cryptology	18	2
Networks : Controls and Audits	18	2
Security and Risk Management	18	2
Social Engineering	18	2
French Language and Culture	24	3
Individual Project in Security	As needed	5

Module descriptions (1)
Information Theory

- **Objectives**: To gain clear and deep knowledge of what information and communication is. To be able to formalize most of the concepts and to manipulate at the mathematical level for later engineering applications.

- **Program**:
  - Entropy and uncertainty : entropy and its properties, conditional entropy, information
  - Communication channel and Shannon theory : noiseless coding theorem for memoryless sources
  - Communication through noisy channels
  - Perfect secrecy
  - Applications

Module descriptions (2)
Maths for Information Security

- **Objectives**: To discover thorough mathematical concepts and tools to be able to formalize most issues arising in the security field (systems and information). From that formalization, students must be able to identify which algorithmic approach must then be used to solve those issues in an operational ways or to prove that the relevant problems have no practical solution.

- **Program**:
  - Complexity and computability theories
  - Basics in combinatorics (graph theory)
  - Formal grammars and automata
  - Boolean functions and applications
  - Game theory

Module descriptions (3)
Code Theory

- **Objectives**: To gain clear and deep knowledge of the different issues arising during a noisy communication and to discover concepts, tools and techniques that enables to prevent noise during communication and maximize mutual information. A large number of engineering applications are used to illustrate the full scope of ECC (error-correcting code) theory.
- **Program**:
  - Error-correcting codes : coding problem and general sources (Markov, ergodic)
  - Structure of natural languages (redundancy, Zipf law)
  - Linear codes and syndrome decoding
  - Cyclic codes
  - Applications : The Mariner Code, Reed-Muller codes

Module descriptions (4)
Networks: Local Security

- **Objectives**: The aim of this course is to explain the vulnerabilities found on Local Area Networks (LAN) especially with OSI level 2 equipment (switch – A.P.) and protocols (Ethernet – WIFI – Bt).
- **Program**:
  - Network reminders

    - Lab : “system and network configuration”
  - Internet access imputability

    - Lab : “captive portal”
  - securing the access to media

    - Lab : network frame analysis
    - Lab : security of Ethernet, WIFI and Bt
    - Lab : access authentication (option)

Module descriptions (5)
Networks: Security Architecture

- **Objectives**: The aim of this course is to present the network security architectures deployed to protect companies' network service.

- **Program**:
  - Firewall and DMZ

    - Lab : "filtering, address translation and DMZ"

    - Lab : "services firewalls (proxy)"
  - Virtual Private Network

    - Lab : "VPN"
  - Intrusion detection

    - Lab : "Intrusion Detection System"

Module descriptions (6)
Secure Programming

- **Objectives**: To explain the different security problems arising when unsecure programming primitives are used and how attackers can exploit them. In a second part, the students will learn how to use secure programming primitives and to perform static/dynamic analysis on source codes.

- **Program**:
  - Security of applications and vulnerabilities (buffer overflow, heap overflow, integer and string format attacks…)
  - Secure programming in C and secure primitives
  - Static analysis of source code (flawfinder, coverity)
  - Dynamic code analysis (valgrind, Seeker)

Module descriptions (7)
Smart Cards

- **Objectives**: Be able to design and program a complete smart card application, both on-card and off-card parts, to solve a given problem.

- **Program**: JavaCard, PCSC, OCF, both on-card and off-card applications development

Module descriptions (8)
Cryptology

- **Objectives**: To explain the different concepts around information security and system security both at the COMSEC and TRANSEC levels. The students must learn how to protect information (confidentiality) and system (availability and integrity, authentication) with the most recent mathematical tools provided by cryptology.

- **Program**:
  - Introduction to cryptology (cryptography and cryptanalysis, steganography)
  - Symmetric cryptography (confidentiality)
  - Asymmetric cryptography (integrity, authentication)
  - Applications : encrypted filesystems, email protection, secure data transfer

Module descriptions (9)
Networks: Controls and Audits

- **Objectives**: To learn to prepare a technical security audit. Managing and mastering the security tools. Understanding the ethics when performing an audit on an operational system.

- **Program**:
  - Organization
  - Port scanning
    - Lab : “nmap”
  - Network services knowledge
    - Lab : “network services analysis”
  - Vulnerability detection
    - Lab : “OpenVAS, NSE”
  - WIFI /Bt
    - Lab : “WIFI cartography”

Module descriptions (10)
Security and Risk Management

- **Objectives**: To bring a detailed approach and a methodology for the management of security and risks in the corporate environment. Students will learn to manage risk, to analyze a situation and to propose appropriate measures in order to limit or eradicate the risks for an enterprise / administration.

- **Program**:
  - Risks and their actors
  - Risk analysis
  - Business Continuity
  - Crisis & Incident management
  - Case study of real situations

Module descriptions (11)
Social Engineering

- **Objectives**: to understand our environment via media and geopolitics, to discover computer science monitoring and learn about social engineering and human psychology (how to manipulate a target)

- **Program**:
  - Analysis and understanding of the environment
  - Methods of medias analysis
  - Geopolitics and social psychology of organizations
  - Computer science monitoring and tools
  - Social Engineering and human psychology

Module descriptions (12)
French Language and Culture

- **Objectives**: To give the students the language skills necessary to manage shopping, going to restaurants, taking public transport, etc. To introduce students to French culture (gastronomy, architecture, film, etc.)

- **Program**:
  - Emphasis on communication: listening and speaking
  - Small-group lessons provide students with many opportunities to speak.
  - Visits of cultural and historical sites in and around Laval

Module descriptions (13)
Individual Project in Security

- **Objectives**: To give the students the opportunity to work on an aspect of information security that interests them.

- **Program**:
  - Students work with tutors to determine their field of interest
  - Students and tutors work together to negotiate deliverables (nature and number of deliverables, milestones)
  - Possibility of continuing onto second semester for a larger project
  - **The best students can be kept on in second semester on an internship basis (modest monthly salary)**

Interested???

Contact your International Office for more information!

A bientôt!!!