Master in Computer science

Cybersecurity 2nd year

Presentation

The global economic impact of losses due to cybercrime amounts to hundreds of billions of euros per year ($445 billion according to the McAfee/CSIS study of 2014) with a strong increase in attacks, especially for identity theft and digital data theft, as well as malicious attacks. Protection against these vulnerabilities includes:

- Robustness to cyber attacks of sensitive infrastructure (e.g. stuxnet)
- Robustness of security components against software vulnerabilities and data leaks (e.g. heartbleed)
- Protection of privacy and security of cloud infrastructures
- Robust design and evaluation of safety components
- Fault detection in protocols or software and hardware components

The topics covered in the training cover the complementary areas of Cybersecurity, including cryptology, forensics, and privacy, in particular for embedded systems and distributed architectures.

Train cybersecurity experts (including data privacy aspects) with a bac + 5 degree, able to evolve immediately in an industrial environment and who can also pursue a thesis.

Registration and scholarships

The second year master’s is accessible to candidates according to their transcripts (and/or interview):- having validated the first year of a compatible course- or by validating studies or acquired experience according to the conditions determined by the university or the training.

Public continuing education : You are in charge of continuing education :

- if you resume your studies after 2 years of interruption of studies
- or if you followed a formation under the regime formation continues one of the 2 preceding years
- or if you are an employee, job seeker, self-employed

If you do not have the diploma required to integrate the training, you can undertake a validation of personal and professional achievements (VAPP).

Do you want to apply and register? Note that the procedure differs depending on the degree considered, the degree obtained, or the place of residence for foreign students.

Find out which procedure applies to me and apply

Further studies

Depending on the nature of their practicum, students may wish to pursue research in a doctoral thesis.

Practical informations :

- Component : Grenoble INP, Institut d'ingénierie et de management, UFR IM2AG (informatique, mathématiques et mathématiques appliquées)
- Duration : 1 year
Course type: Initial and Continuing Education
Location(s):

Contacts

Program director
Potet Marie-Laure
Marie-Laure.Potet@grenoble-inp.fr

Pernet Clement
Clement.Pernet@univ-grenoble-alpes.fr

Program administration
Beaujolais Carine
carine.beaujolais@univ-grenoble-alpes.fr
Phone 04.76.63.57.22

Program

Master 2nd year

Semester 9

<table>
<thead>
<tr>
<th>UE Software security, secure programming and computer forensics</th>
<th>3 ECTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Security architecture: network, system, key management, cybersecurity of industrial IT</td>
<td>6 ECTS</td>
</tr>
<tr>
<td>UE Cryptographic engineering, protocols and security models, data privacy, coding and applications</td>
<td>6 ECTS</td>
</tr>
<tr>
<td>UE Threat and risk analysis, IT security audit and norms</td>
<td>3 ECTS</td>
</tr>
<tr>
<td>UE Physical Security: Embedded, Smart Card, Quantum &amp; Biometrics</td>
<td>6 ECTS</td>
</tr>
</tbody>
</table>

1 option(s) to choose from 2

<table>
<thead>
<tr>
<th>UE Advanced cryptology/Advanced Security</th>
<th>6 ECTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Advanced security</td>
<td>6 ECTS</td>
</tr>
</tbody>
</table>

Semester 10

<table>
<thead>
<tr>
<th>UE Research practicum (in company or laboratory)</th>
<th>30 ECTS</th>
</tr>
</thead>
</table>

The information contained in this document is for information purposes and is non-contractual. - Updated on 20 April 2021