Master 2 Cybersecurity
Cryptology & Security; Informatics & cyber-physical systems

UGA directors: Jean-Guillaume Dumas, Clément Pernet
Ensimag director: Marie-Laure Potet

http://cybersecurity.imag.fr
M2 CyberSecurity (CS)

1 year dedicated program at University Grenoble Alpes (UGA)

Ensimag + ufr IM²AG
cybersecurity.imag.fr

- **Goals**: formation of experts in security and coding technologies
  - **Cryptology**: mathematical protocols (RSA, AES, ECC, SHA3, PKI...)
  - **Security**: software/hardware (network, system, integration), audit
  - **Applications**: watermarking, multimedia, smartcard, ...

- **M2 P+R**: Directed to research and profession
  - Sept.-Jan.: lectures+training
  - Jan.-Sept.: project/internship
# CyberSecurity courses

<table>
<thead>
<tr>
<th>Contents</th>
<th>Credits</th>
<th>Sem.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software security, secure programming and <strong>computer forensic</strong></td>
<td>3</td>
<td>S9</td>
</tr>
<tr>
<td><em>(Laurent Mounier)</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security architectures</strong> : network, system, key managements, cybersecurity of industrial IT <em>(Jean-Guillaume Dumas)</em></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td>Cryptographic engineering, <strong>protocols and security models</strong>, data privacy, coding and applications <em>(Clément Pernet)</em></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td>Threat and risk analysis, IT security <strong>audit</strong> and norms</td>
<td>3</td>
<td>S9</td>
</tr>
<tr>
<td><em>(Florent Autreau)</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware and <strong>embedded</strong> systems <strong>security</strong> <em>(Paolo Maistri)</em></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td><strong>Optional: Advanced Cryptology</strong> <em>(Pierre Karpman)</em></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td><strong>Optional: Advanced Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internship</strong> <em>(within a Company or in a research unit)</em></td>
<td>30</td>
<td>S10</td>
</tr>
<tr>
<td>+ FLE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Research environment

• Cybersecurity: versatile domain, within different departments
  – Computer science + Mathematics
  – LIG, LJK, Institut Fourier, Verimag, TIMA, GIPSA-Lab, Inria, CEA
    (all these Grenoble research units « labs » participate in the courses)

• Complementary aspects:
  – Academia + Industry + Government
  – Many research projects (French ANR, Europe, etc.)

• An Idex project: Cyber@Alps (near 100 permanent members)
  – Federate activities in digital sciences and Humanities in Grenoble
Previously: Master SCCI

• Security, Cryptology and Coding of Information Master
  – 2002 - 2016: about 500 students

• Became CyberSecurity in 2016
Examples of Master thesis/PFE

Integration of zero-knowledge authentication on smart card [C-S]
- Secure server for SIP telecommunications [INRIA]
- Integration of strong authentication in an information system [British Telecom]
- Management of identity for printer access [Helwett-Packard, Germany]
- Reconfiguration of a secure infrastructure [France-Telecom, Grenoble]

Conception et réalisation d’un composant de sécurité [Ministère Défense, Paris]
- Analysis and deployment of a confidential data service [Solucom, Nantes]
- Integration of biometrics in crypto protocols [SAGEM, Paris]

Hidden channel attacks [SAGEM, Paris]
- Windows CardSpace components in a smart card [Gemalto, La Ciotat]
- Secure loading of jar in JavaCard3.0 [Gemalto, La Ciotat]
- Lightweight electronic signature [Dictao, Paris]
- Wireless infrastructure for emergency comm. [Wisecomm, Germany]
- Secure and anonymous communication on internet [UL, Luxembourg]
- Test of crypto-secure random generators [LTSI, Lyon]

Security analysis of a medical data protection scheme [Philips, Eindhoven]
- Supervision of the CEA computer infrastructure [CEA, Grenoble]
- Security analysis of images watermarking [GIPSA, Grenoble]
- Security audit of the SCADA platform [Atos Origin, Grenoble]

…..
Partners

- Thales
- Actoll
- Ernst & Young
- ST Micro
- Amadeus
- Sopra group
- Logica
- Solucom
- Accenture
- MinDef
- Tessi lab
- C-S
- EADS
- Technicolor
- CEA LETI
- Xerox
- Tiempo
- Orange Labs (Caen, Grenoble)
- Netheos
- Medasys infrastructure
- CGI
- Mathworks
- Consensys
- Police scientifique
- Oberthur
- Cap Gemini
- Schneider Electric
- Canal+ Technologies (Nagra)
- Netasq SA
- Aatlantide
- Gemalto
- Banque de France
- Atos
- SFR
- Onix
- Edelweb
- Prowebce
- Microstore
- Aliantiz
- Airbus
- DCNS
- Caisse d’épargne
- Motorola
- Laboratoires CNRS, INRIA, Universities
- ...
IT skills shortage

In which of the following areas do you believe your IT organization currently has a **problematic shortage** of existing skills? (Percent of respondents, N=627, multiple responses accepted)

- Cybersecurity: 46%
- Mobile application development: 37%
- Business intelligence/data analytics: 36%
- Social media/marketing technologies: 34%
- Enterprise mobility management: 31%
- Server virtualization/private cloud infrastructure: 31%
- Compliance management, monitoring and reporting: 30%
- Social enterprise/collaboration technologies: 30%
- IT architecture/planning: 30%
- Application development: 28%
- Data protection: 27%
- Database administration: 25%
- Help desk/service desk: 24%
- Storage administration: 24%
- Server administration: 22%
- Network administration: 22%
- We do not have any IT skills shortages: 12%
- Other: 1%
- Don’t know: 2%

Career growth potential

In which of the following functional areas do you believe skills development would be most beneficial to your employees (i.e., IT staff) in terms of their career path and benefit to your organization? (Percent of respondents, N=627)

- Cybersecurity (i.e., information security), 44%
- Big data analytics, 26%
- Infrastructure management, 17%
- Application development and deployment, 12%

Examples of PhD

Tancrède Lepoint
2011: M2 SCCI
2011-2014: PhD Crypto-Experts, ENS [Poincheval] & Univ. of Luxembourg [Coron]

**design and Implementation of Lattice based Cryptography**

Since then:

- 2014-2016: Junior security expert à CryptoExperts
- 2016-... : Senior research Scientist à SRI
- Director of the IACR, Co-editor of the Cyptology e-print archive

Alexandre Berzati
2007: M2 SCCI

**Analyse cryptographique des altérations d'algorithmes**

2010: Postdoc CEA Cadarache
Since 2011: Engineer expert INVIA [Semiconductor design for embedded security]

Thomas Roche
2006: M2 SCCI

**Dimensionnement et intégration d’un chiffre symétrique (...)**

2010-2011: Postdoc Paris-8
Since 2011: ANSSI (Agence nationale de la sécurité des systèmes d'information) , then APPLE

Also
Main resource: http://cybersecurity.imag.fr

- ADE: planning

- Calendar: September to January + holidays

- Regulations (in French):
  - Course ≈ 50% Exam + 50% Practice/Interrogations
  - Practice /Interrogations mandatory (ABJ 0/20, ABI DEF)
  - Average 10/20, for each semester
  - No course below 7/20
  - FLE is proposed
  - Internship: 4 to 6 months

Master 2 = Semesters 9 & 10

• Welcome week: Sept. 17 to 21, 2018
  – Foreign students welcome, administrative registration, training

• Semester 9: 14 weeks
  – Part 1: 7 weeks from Sept. 24 to Nov. 15
  – Part 2: 7 weeks from Nov. 19 to Jan. 17

• Exams: Jan 21 - 25, 2019
  – 2nd session: April 2019

• Semester 10: Internship
  – Internship defenses: September 2 – 6, 2019
September 17 – September 21

- Welcome week
  - Administrative Informations
    - Registration, Informatics accounts, ADE, information system, unix, etc.
  - Practical informations
    - student card, health insurance, bank account, residence permit
- TOURISTIC DAY + Guided VISIT OF GRENOBLE
- IntEGRE, Isso student associations
- …
<table>
<thead>
<tr>
<th>Time</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>8h15-9h45 &amp; 9h45-11h15</td>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U03 Crypto Eng.</td>
<td>GBCY9U03 Crypto Eng.</td>
</tr>
<tr>
<td>11h15-12h45</td>
<td></td>
<td></td>
<td>RATTRAPAGE</td>
<td>RATTRAPAGE</td>
<td>GBCY9U03 Crypto Eng.</td>
</tr>
<tr>
<td>14h-15h30 &amp; 15h30-17h00</td>
<td>GBCY9U04 Risk Analysis</td>
<td>Idex</td>
<td>Idex</td>
<td>Idex</td>
<td>GBCY9U05 Embedded Sec.</td>
</tr>
</tbody>
</table>
### October 1 – November 15

<table>
<thead>
<tr>
<th>3h+1.5h Matin</th>
<th>Lundi</th>
<th>Mardi</th>
<th>Mercredi</th>
<th>Jeudi</th>
<th>Vendredi</th>
</tr>
</thead>
<tbody>
<tr>
<td>8h15-9h45 &amp; 9h45-11h15</td>
<td>RATTRAPAGE</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U03 Crypto Eng.</td>
<td>GBCY9U03 Crypto Eng.</td>
</tr>
<tr>
<td>GBCY9U04 Risk Analysis</td>
<td>GBCY9U02 Security Arch.</td>
<td>RATTRAPAGE</td>
<td>GBCY9U01 Software Security</td>
<td>RATTRAPAGE</td>
<td>GBCY9U03 Crypto Eng.</td>
</tr>
<tr>
<td>11h15-12h45</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3h Après-midi</th>
<th>Lundi</th>
<th>Mardi</th>
<th>Mercredi</th>
<th>Jeudi</th>
<th>Vendredi</th>
</tr>
</thead>
<tbody>
<tr>
<td>14h-15h30 &amp; 15h30-17h00</td>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U01 Software Security</td>
<td>conférences industrielles + RATTRAPAGE</td>
<td>GBCY9U05 Embedded Sec.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anglais Ensimag</td>
<td>GBCY9U02 Security Arch.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### November 19 – January 11

<table>
<thead>
<tr>
<th>Lundi</th>
<th>Mardi</th>
<th>Mercredi</th>
<th>Jeudi</th>
<th>Vendredi</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATTRAPAGE</td>
<td>RATTRAPAGE</td>
<td>RATTRAPAGE</td>
<td>RATTRAPAGE</td>
<td>RATTRAPAGE</td>
</tr>
<tr>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U03 Crypto Eng.</td>
<td>GBCY9U02 Security Arch.</td>
<td>conférences industrielles + RATTRAPAGE</td>
<td>OPTION: Advanced Crypto. Advanced Secu.</td>
</tr>
<tr>
<td>Anglais Ensimag</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


## January 14 – January 18

<table>
<thead>
<tr>
<th>Lundi</th>
<th>Mardi</th>
<th>Mercredi</th>
<th>Jeudi</th>
<th>Vendredi</th>
</tr>
</thead>
<tbody>
<tr>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U01 Software Security</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>OPTION: -/Advanced Crypto. -/Advanced Secu.</td>
<td>Révisions</td>
</tr>
<tr>
<td>GBCY9U03 Crypto Eng.</td>
<td>RATTRAPAGE</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>RATTRAPAGE</td>
<td></td>
</tr>
<tr>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U03 Crypto Eng.</td>
<td>GBCY9U03 Crypto Eng.</td>
<td>Révisions</td>
<td>Révisions</td>
</tr>
</tbody>
</table>
Optional courses

choice before Sept 25th 2018.
  – Possible to modify until end Oct 2018

• Advanced Cryptology
  – Pierre Karpman

• Advanced Security
  – Cédric Lauradoux
Some Events

• GreHack 2018: **Friday Nov. 16\textsuperscript{th}, 2018**
  – [https://grehack.fr](https://grehack.fr)
• FEEL: **Thursday Oct. 11\textsuperscript{th}, 2018**
• 2018 Cyber Security Awareness Week in Valence
  – [www.csaw-europe.com](http://www.csaw-europe.com)
  – qualification rounds online
  – on-site competitions (**Nov. 8\textsuperscript{th} to 11\textsuperscript{th} 2018**)
• Forum int. de la Cybersécurité: **Jan 22-23\textsuperscript{th}, 2019**
  – [www.forum-fic.com](http://www.forum-fic.com)
• Forum Emploi-maths: **Dec. 12\textsuperscript{th}, 2018**
Registrations

• **Thursday September 20th, 2018**
  – Registration UGA / INP
  – Use your [@univ-grenoble-alpes.fr](mailto:@univ-grenoble-alpes.fr) and [@grenoble-inp.org](mailto:@grenoble-inp.org) addresses

• Master mention, choice of:
  – Informatique (Computer science)
  – Mathématiques & applications