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

UGA director: Clément PERNET
Ensimag director: Marie-Laure POTET

http://cybersecurity.imag.fr

September 19, 2022
1 year dedicated program at Université Grenoble Alpes (UGA)

*Ensimag + UFR IM²AG*

[cybersecurity.imag.fr](http://cybersecurity.imag.fr) application from January.

A well established program: since 2002 (Crypto., SCCI, Cybersecurity)

→ Over 600 graduated students

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

- Directed to both **Research** and **Industry** careers
  - Sept.-Jan.: lectures + training + industrial conferences
  - Feb.-Sept.: project / internship
Research and Economical environment in Grenoble

• 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 » are involved in the courses)

• Complementary aspects:
  – Academia + Industry + Government
  – Many research projects (Cifre, French ANR, MinDef, Europe, etc.)
  – PEPR PIA4 : privacy, secure component, tools for security evaluation

• The Grenoble Alpes Cybersecurity Institute
  – Federate Security activities in Grenoble between science
    and humanities
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, Arcueil, Rennes, Paris, Grenoble)
- Netheos
- Medasys infrastructure
- CGI
- Sogeti High Tech
- Mathworks
- Consensys
- Deloitte
- 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
- ...

5
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)

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

Examples of PhD

- **Nicolas Bordes**
  
  2017: M2 CyberSecurity
  2018-20...: PhD Grenoble LJK [Karpman, Dumas]

  *Symmetric primitives of low multiplicative complexity, side channel attacks and masking*

- **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**
  
  J. Javelle (LIG), M.-A. Cornelie (IF), A. Kumar (Inria/LIG/Verimag), M. Duclos (Verimag, 2016), K. Layat (IF, 2015),
  Z. Sultan (LIG/LJK, 2016), G. Dejulis (IF, 2014), R. Jamet (Verimag, 2015), J-B Orfila (LJK 2018), M. Puys (Vérimag 2017),
## CyberSecurity courses

<table>
<thead>
<tr>
<th>Contents</th>
<th>Credits</th>
<th>Sem.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software security</strong>, secure programming and computer forensic</td>
<td>3</td>
<td>S9</td>
</tr>
<tr>
<td><strong>Security architectures</strong>: network, system, key managements,</td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td>blockchains, cybersecurity of industrial IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cryptographic engineering</strong>, protocols and security models, data</td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td>privacy, coding and applications</td>
<td></td>
<td></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><strong>Hardware and embedded systems security</strong></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td><strong>Group</strong>: <strong>Advanced Cryptology</strong></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td><strong>Group</strong>: <strong>Advanced Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internship</strong> (within a Company or in a research unit) + FLE</td>
<td>30</td>
<td>S10</td>
</tr>
</tbody>
</table>
Organisation

Main site for the program: cybersecurity.imag.fr

- weekly planning: ADE
- Calendar: September to January + holidays
- Regulations (in French):
  - Course ≈ 50% final exam (ET)+ 50% Lab work / midterm exams (CC)
  - Lab work / midterm exams Interrogations are mandatory
    justified absence (ABJ)=0/20, Nonjustified Absence(ABI)=FAILED (DEF)
  - Passing grade: 10/20, for each semester
  - Threshold: no course below 7/20
  - FLE (Français langue étrangère) is proposed
  - Internship: 5 to 6 months (5 months required)
    - Defenses on Sept. 4-5-6-7 2023
    - Early denses in June possible for candidates to phd scholarships
Master 2 = Semesters 9 & 10

• Welcome week: Sept. 14 to 16, 2022
  – Foreign students welcome, administrative registration, training

• Semester 9: 14 weeks
  – Part 0: 1 week from Sept. 19 to Sept. 23 (refresh week)
  – Part 1: 6 weeks from Sept. 26 to Nov 11
  – Part 2: 7 weeks from Nov. 14 to Jan. 11 (elective course, last week = catch-up slots)

    Warning: Classes on Monday Dec. 20, but not on Tuesday Dec. 21.

• Exams: Jan 16 – 20, 2022
  2nd session: April 10 – 14, 2022

• Semester 10: Internship
  – Internship defenses: September 1 – Sept. 6, 2022

⇒ Start now to look for one
Semester 9: 14 weeks

5 semaines : du 3 Octobre au 11 Novembre
moins jeudi 13 octobre, FERI, moins vendredi 11 novembre

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45 & 9h45-11h15  RATTRAPAGE  GBCY9U05 Embedded Sec.
          GBCY9U05 Embedded Sec.
13h15-12h45  GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          GBCY9U01 Crypto Eng.
          GBCY9U03 Crypto Eng.

14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U03 Crypto Eng.
GBCY9U02 Security Arch.
GBCY9U03 Crypto Eng.

Semaine du 19 Septembre 2022

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  Semaine  GBCY9U02 Security Arch.
          GBCY9U03 Crypto Refresh
9h45-11h15  de  cours  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
13h15-12h45
14h-15h30 & 15h30-17h00
GBCY9U03 Crypto Refresh
GBCY9U03 Crypto Refresh

Semaine du 9 janvier 2023

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  OPTION: GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          -Advanced Crypto. -Advanced Secu.
9h45-11h15  -Advanced Crypto. -Advanced Secu.
          -Advanced Crypto. -Advanced Secu.
13h15-12h45  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U04 Risk Analysis
GBCY9U02 Security Arch.
GBCY9U01 Crypto Eng.
GBCY9U03 Crypto Eng.
GBCY9U05 Embedded Sec.

Semaine du 26 septembre 2022

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  OPTION: GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          -Advanced Crypto. -Advanced Secu.
9h45-11h15  -Advanced Crypto. -Advanced Secu.
          -Advanced Crypto. -Advanced Secu.
13h15-12h45  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U04 Risk Analysis
GBCY9U02 Security Arch.
GBCY9U01 Crypto Eng.
GBCY9U03 Crypto Eng.
GBCY9U05 Embedded Sec.

Semaine du 16 janvier 2023

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  OPTION: GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          -Advanced Crypto. -Advanced Secu.
9h45-11h15  -Advanced Crypto. -Advanced Secu.
          -Advanced Crypto. -Advanced Secu.
13h15-12h45  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U04 Risk Analysis
GBCY9U02 Security Arch.
GBCY9U01 Crypto Eng.
GBCY9U03 Crypto Eng.
GBCY9U05 Embedded Sec.

Semaine du 23 janvier 2023

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  OPTION: GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          -Advanced Crypto. -Advanced Secu.
9h45-11h15  -Advanced Crypto. -Advanced Secu.
          -Advanced Crypto. -Advanced Secu.
13h15-12h45  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U04 Risk Analysis
GBCY9U02 Security Arch.
GBCY9U01 Crypto Eng.
GBCY9U03 Crypto Eng.
GBCY9U05 Embedded Sec.

Semaine du 30 janvier 2023

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  OPTION: GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          -Advanced Crypto. -Advanced Secu.
9h45-11h15  -Advanced Crypto. -Advanced Secu.
          -Advanced Crypto. -Advanced Secu.
13h15-12h45  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U04 Risk Analysis
GBCY9U02 Security Arch.
GBCY9U01 Crypto Eng.
GBCY9U03 Crypto Eng.
GBCY9U05 Embedded Sec.

Semaine du 6 février 2023

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  OPTION: GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          -Advanced Crypto. -Advanced Secu.
9h45-11h15  -Advanced Crypto. -Advanced Secu.
          -Advanced Crypto. -Advanced Secu.
13h15-12h45  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U04 Risk Analysis
GBCY9U02 Security Arch.
GBCY9U01 Crypto Eng.
GBCY9U03 Crypto Eng.
GBCY9U05 Embedded Sec.

Semaine du 13 février 2023

Lundi  Mardi  Mercredi  Jeudi  Vendredi
8h15-9h45  OPTION: GBCY9U04 Risk Analysis  GBCY9U02 Security Arch.
          -Advanced Crypto. -Advanced Secu.
9h45-11h15  -Advanced Crypto. -Advanced Secu.
          -Advanced Crypto. -Advanced Secu.
13h15-12h45  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE  RATTRAPAGE
14h-15h30 & 15h30-17h00
GBCY9U02 Security Arch.
GBCY9U04 Risk Analysis
GBCY9U02 Security Arch.
GBCY9U01 Crypto Eng.
GBCY9U03 Crypto Eng.
GBCY9U05 Embedded Sec.
Elective courses:
Advanced Cryptology/Security

• Starts November 14, 2022

Advanced Cryptography: Pierre Karpman
Advanced Security: Cédric Lauradoux

→ Make up your choice by October 28th
https://international.univ-grenoble-alpes.fr

> Section « Votre séjour à l’UGA »  > « Getting Organized » section
- Logement, titres de séjour, assurances, dispositifs d’aide et de soutien, espaces d’accueil, etc.
- Guides et fiches pratiques pdf téléchargeables
- Accommodation, residence permits, insurances, support services, services centers, etc.
- Welcome guides and info sheets available

Accueil :
Welcome:

<table>
<thead>
<tr>
<th>Grenoble</th>
<th>Valence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bâtiment iCampus – Welcome Center</td>
<td>Site Briffaut</td>
</tr>
<tr>
<td>1025 Avenue Centrale</td>
<td>DSDA, Bâtiment 2</td>
</tr>
<tr>
<td>Campus Saint-Martin-d’Hères</td>
<td>Site Latour-Maubourg</td>
</tr>
<tr>
<td>Tram B &amp; C « Bibliothèques Universitaires »</td>
<td>Maison de l’Etudiant</td>
</tr>
</tbody>
</table>

Temps d’infos rentrée : vos démarches à l’arrivée  Info sessions: first steps upon arrival
- Assurances, compte en banque, assurance maladie, etc.
- Chaque semaine en septembre (programme sur le portail international de l’UGA)
- Insurances, bank account, healthcare system, etc.
- Each week in September (program on UGA international website)
Rule of conduct

**Fraud and plagiarism** are strictly forbidden

- Team work is not copy/paste
- Applies to all documents subject to an evaluation (Lab reports, exams and internship reports)
- When detected, triggers a **disciplinary commission**
- Sanctions from simple warning to permanent expulsion from any public higher education institution

**Fight against Gender based Violence and discrimination:**

Gender-Based violence and harassment, disability, racism, anti-Semitism, homophobia, transphobia, religious discrimination...

- During class and lectures
- In your student life
- In your internship
- During student events

→ **Zero tolerance**

Some Events

- **FEEL**: Thursday Oct. 13, 2022
- GreHack 2022: Friday Nov. 18, 2022
  - 2022.forum-emploi-maths.com
- Forum int. de la Cybersécurité: June 7-9, 2022
  - www.forum-fic.com
Registrations

• From **Wednesday September 14\textsuperscript{th}, 2022**
  – Registration: either UGA (UFR-IM2AG) or INP (Ensimag)
  – Use your \texttt{@univ-grenoble-alpes.fr} and \texttt{@grenoble-inp.org} addresses

• Master mention, choice of:
  – Informatique (Computer science)
  – Mathématiques & applications
Semester 10 : internships

Instructions are available on cybersecurity.imag.fr

• **Warning**: procedure depends on your affiliation (INP or UGA)
• We will propose a chamillo page with some subjects
• A « confortable » planning :
  – Prospection during October and November
  – Application before end of December
  – Internship starting in February
  – But there is some slack : 5 months before end of August
  – Defenses on Sept. 1, 4-5-6. (book your agenda)

Further informations :
  - [https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/](https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/)
  - [https://www.ssi.gouv.fr/guide/les-profils-de-la-cybersecurite/](https://www.ssi.gouv.fr/guide/les-profils-de-la-cybersecurite/)
Contact

• For any general questions, address your mail to both program directors:
  - Marie-laure.potet@grenoble-inp.fr
  - Clement.pernet@grenoble-inp.fr

• For questions regarding your registration:
  - Carine.beaujolais@univ-grenoble-alpes.fr (UFR-IM2AG)
  - Emmanuel.villemont@grenoble-inp.fr (Ensimag)