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

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

http://cybersecurity.imag.fr

September 20, 2021
M2 CyberSecurity

1 year dedicated program at Université Grenoble Alpes (UGA)

Ensimag + UFR IM²AG

cybersecurity.imag.fr  application from Feb.

- **Goals**: formation 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**: watermarking, multimedia, smartcard, …

- **M2 P+R**: Directed to Research and Industry
  - Sept.-Jan.: lectures + training
  - Feb.-Sept.: project / internship
# 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, blockchains, cybersecurity of industrial IT</td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td><strong>Cryptographic engineering</strong>, protocols and security models, data privacy, coding and applications</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>Hardware and <strong>embedded</strong> systems <strong>security</strong></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td>Group: <strong>Advanced Cryptology</strong></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td>Group: <strong>Advanced Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internship</strong> (within a Company or in a research unit)</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 » are involved in the courses)

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

• An Idex project « Grenoble Alpes Cybersecurity Institute »
  – Federate Security activities in Grenoble between science and humanities
An already long history

• Security, Cryptology and Coding of Information Master – 2002 - 2016: about 400 students

• Becomes Cybersecurity in 2016

• Total over 550 graduates ...
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
- ...
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

- **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.imag.fr

• ADE: planning

• Calendar: Sept. - Jan. + 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 (Français langue étrangère) is proposed
  – Internship: 5 to 6 months

Master 2 = Semesters 9 & 10

• Welcome week: Sept. 15 to 17, 2021
  – Foreign students welcome, administrative registration, training

• Semester 9: 14 weeks
  – Part 0: 1 week from Sept. 20 to Sept 25 (refresh week)
  – Part 1: 5 weeks from Sept. 27 to Oct. 29
  – Part 2: 8 weeks from Nov. 8 to Jan. 14 (group option start, last week = catch-up slots)

• Exams: Jan 17 – 21, 2022
  – 2nd session: April 2022

• Semester 10: Internship
  – Internship defenses: September 1 – Sept. 6, 2022
  ➢ Start now to look for one
Advanced Cryptology/Security

• Elective courses
• Starts November 8, 2021

Pierre Karpman / Cédric Lauradoux

- Shared Plenary courses (CM)
- Elective lab (TP) and practical sessions (TD)
Some Events

• FEEL: Thursday Oct. 7, 2021

• GreHack 2020: Friday Nov. 19, 2021


• Forum int. de la Cybersécurité: June 7-9, 2022
  – www.forum-fic.com
Registrations

• From **Wednesday September 15\textsuperscript{th}, 2021**
  – Registration UGA / INP
  – Use your @univ-grenoble-alpes.fr and @grenoble-inp.org addresses

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