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

UGA director: Jean-Guillaume DUMAS
Ensimag director: Marie-Laure POTET

http://cybersecurity.imag.fr

September 23, 2019
M2 CyberSecurity (CS)

1 year dedicated program at Université Grenoble Alpes (UGA)

Ensimag + ufr IM²AG

cybersecurity.imag.fr ⇒ application from Jan. (FSA)

- **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
  - Feb.-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><strong>Security architectures</strong>: network, system, key managements, blockchains, cybersecurity of industrial IT</td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td>Cryptographic engineering, <strong>protocols and security models</strong>, 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><strong>Optional</strong>: <strong>Advanced Cryptology</strong></td>
<td>6</td>
<td>S9</td>
</tr>
<tr>
<td><strong>Optional</strong>: <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></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, MinDef, Europe, etc.)

- An Idex project « Grenoble Alpes Cybersecurity Institute »
  - Federate Security activities in Grenoble
  + humanities
Following SCCI

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

• Becomes Cybersecurity
  – From 2016

• Total more than 500 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]
- Reconfiguraton 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

- Sébastien Varrette
  2003: M2 SCCI
  2003-2007: PhD Grenoble (LIG-Inria [Roch]) & Univ. Luxembourg [Leprévost]
  **Security in Large Scale Distributed Systems: Authentication and Result Checking**
  Since 2007: Research fellow Université Luxembourg [Distributed Platforms Security and HPC systems]

- 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),
  J-B Orfila (LJK 2018), M. Puys (Vérimag 2017), N. Bordes (LJK, ongoing) …
• 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 is proposed
  – Internship: 5 to 6 months

Master 2 = Semesters 9 & 10

• Welcome week: Sept. 16 to 20, 2019
  – Foreign students welcome, administrative registration, training

• Semester 9: 14 weeks
  – Part 1: 7 weeks from Sept. 23 to Nov. 14 (first week refresh)
  – Part 2: 7 weeks from Nov. 18 to Jan. 17 (option start)

• Exams: Jan 20 – 24, 2020
  – 2nd session: April 2020

• Semester 10: Internship
  – Internship defenses: September 1 – 4, 2020
September 16 – September 20

- http://ensimag.grenoble-inp.fr/orientation-day-ensimag-im2ag-master-2/

- 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
# Semester 9: 14 weeks

## 6 semaines : du 30 septembre au 15 Novembre

<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>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U03 Crypto Eng.</td>
<td>GBCY9U03 Crypto Eng.</td>
</tr>
<tr>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U02 Security Arch.</td>
<td>Anglais Ensimag</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U05 Embedded Sec.</td>
</tr>
<tr>
<td>8h15-9h45 &amp; 9h45-11h15</td>
<td>11h15-12h45</td>
<td>14h-15h30 &amp; 15h30-17h00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 6 semaines : du 30 septembre au 15 Novembre
- moins vacances toussaint ; moins Jeudi 10 octobre, FEEL ; moins lundi 11 novembre ; moins vendredi 15 novembre GreHack

## 6 semaines : du 18 Novembre au 10 Janvier ;

<table>
<thead>
<tr>
<th>Lundi</th>
<th>Mardi</th>
<th>Mercredi</th>
<th>Jeudi</th>
<th>Vendredi</th>
</tr>
</thead>
<tbody>
<tr>
<td>GBCY9U04 Risk Analysis</td>
<td>GBCY9U01 Software Security</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>OPTION: -/Advanced Crypto. -/Advanced Secu.</td>
<td></td>
</tr>
<tr>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U05 Embedded Sec.</td>
<td>GBCY9U03 Crypto Eng.</td>
<td></td>
</tr>
</tbody>
</table>

## Semaine du 23 Septembre

<table>
<thead>
<tr>
<th>Lundi</th>
<th>Mardi</th>
<th>Mercredi</th>
<th>Jeudi</th>
<th>Vendredi</th>
</tr>
</thead>
<tbody>
<tr>
<td>9am KICK-OFF</td>
<td>GBCY9U03 Crypto Refresh</td>
<td>GBCY9U03 Crypto Refresh</td>
<td>GBCY9U03 Crypto Refresh</td>
<td>OPTION: -/Advanced Crypto. -/Advanced Secu.</td>
</tr>
<tr>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U02 Security Arch.</td>
<td>Anglais Ensimag</td>
<td>Révisions</td>
<td>Révisions</td>
</tr>
<tr>
<td>8h15-9h45</td>
<td>9h45-11h15</td>
<td>11h15-12h45</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Semaine du 13 janvier

<table>
<thead>
<tr>
<th>Lundi</th>
<th>Mardi</th>
<th>Mercredi</th>
<th>Jeudi</th>
<th>Vendredi</th>
</tr>
</thead>
<tbody>
<tr>
<td>GBCY9U04 Risk Analysis</td>
<td>GBCY9U01 Software Security</td>
<td>OPTION: -/Advanced Crypto. -/Advanced Secu.</td>
<td>Révisions</td>
<td>Révisions</td>
</tr>
<tr>
<td>GBCY9U02 Security Arch.</td>
<td>GBCY9U02 Security Arch.</td>
<td>Anglais Ensimag</td>
<td>Révisions</td>
<td>Révisions</td>
</tr>
<tr>
<td>14h-15h30 &amp; 15h30-17h00</td>
<td>Idex Orientation days</td>
<td>Idex Orientation days</td>
<td>Idex Orientation days</td>
<td>8h15-9h45</td>
</tr>
</tbody>
</table>
Advanced Cryptology/Security

• Course with choice
• Starts November 21\textsuperscript{st} 2019

Pierre Karpman / Cédric Lauradoux

Some common courses ...
... then choice of group & subject
Some Events

- **GreHack 2019**: Friday Nov. 15th, 2019
  - [https://grehack.fr](https://grehack.fr)

- **FEEL**: Thursday Oct. 10th, 2019

- **Forum Emploi-maths (Paris)**: Oct. 15th, 2019

- **Journée du doctorat (PhD) UGA**: Oct. 17th, 2019

- **CSAW europe (Valence)**: Nov. 6-8th, 2019

- **Forum int. de la Cybersécurité**: Jan 28-30th, 2020
  - [www.forum-fic.com](http://www.forum-fic.com) (Lille)
Registrations

• From **Tuesday September 17th, 2019**
  – Registration UGA / INP
  – Use your @univ-grenoble-alpes.fr and @grenoble-inp.org addresses

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