Co-funded by the
Erasmus+ Programme
of the European Union

lmpi
licence master professionnel
en protection informatique

# LMPI – SPAIN_P6_ University of Vigo

# INTERIM TECHNICAL REPORT

# Index

Higher education ..... 3
New/updated courses ..... 4
Teaching/training activities ..... 7

# Higher education

Within the Vietnamese higher education institutions (henceforth, HEIs), the LMPI project activities under development have led to the definition of two new or updated training programmes directly related to the protection of information, systems and networks, thus inscribed into the broad field of cybersecurity:

- A two-year master-level programme in cybersecurity offering advanced courses on a wide range of applied topics with the common thrust of managing and protecting logical and physical information systems and resources. This Master in Cybersecurity will be implemented by the three Vietnamese universities participating in the project (Hanoi University of Science and Technology, Ho Chi Minh University of Technology, and Vietnam National University of Agriculture) as a set of common courses embodying the core contents, plus a variable set of elective/optional courses depending on the staff and interest from each partner. Thus, the curriculum is instantiated as two programmes with a duration of two years and a workload of 120 ECTS, and a third programme also for two years but amounting 94 ECTS in total.
- A four-year bachelor programme including specialisation/minor tracks in cybersecurity or data & network security. The courses leading to this specialisation are new but will be part of existing bachelor curricula in computer or systems engineering in the hosting institutions. The creation of new specialised tracks will attract new students to this area of expertise, in compliance to the goals of the LMPI project. The new training paths will be offered by HCMUT and VNUA in the following academic years according to the interest of the 2nd year students.

The curriculum for the master programme has been developed by respecting as close as possible the general principles of the Bologna process. Specifically,

- The proposed curriculum specifies in full detail the skills and competences that the students will be able to demonstrate after pursuing the degree. In addition, the competences are aligned with the ones set out by international steering groups (e.g., ACM, IEEE), accreditation agencies, and HEIs from Europe and USA.
- The curriculum encompasses a set of courses, mandatory and elective, whose workload has been measured along the lines of the ECTS (European Credit Transfer System). Special effort has been put into measuring all the possible student activities when accounting for the workload of each course, thus trying to shape the curriculum so that mobility with partner institutions in Europe is as seamless as possible.
- The entry requirements to the master clearly establish the cyclic structure of the training program: a 180+ bachelor level in a similar discipline is required. Similarly, it is clearly stated that the master degree entitles the graduates to pursue a Ph.D. in science/engineering, after satisfying the particular requirements of the institution.

Currently, the accreditation file is about to be finished: the courses and their outcomes (competences) have been defined, and the general structure of the training program and the teaching goals have been identified. Further work is still required in adding more refinement to the assessment methods of the students, basically, and in a fine-grain description of the learning modules that will compose each course. We expect to finish this part of the work by May, 2018, in accordance to the new chronogram of the LMPI project.

# New/updated courses

As part of the curriculum definition, the following courses have been identified as essential for all the three master programmes. The courses entail 6 ECTS each and are built from a reduced set of learning units which are also listed in the following tables. The plan is that all the three involved universities (HUST, HCMUT, VNUA) offer these courses as part of their new diplomas in cybersecurity, having the official names:

- HUST: M.Eng. Data & system security, security management.
- HCMUT: M.Eng. Computer engineering, cybersecurity.
- VNUA: M.Eng. Information Technology with a track on System & Data Security. B.Sc on Programing, Track on Data & Application security,

The courses, together with the master's thesis, **amount at least 72 ECTS**, that is, at least 60% of the total volume for being granted the diploma. Next, we list the fundamental courses which are common to all the offer in Vietnam:

| **Course name** | **Contents** |
|---|---|
| Cryptography | 1. Encryption<br>2. Stream cyphers<br>3. Block cyphers<br>4. Message integrity<br>5. Hashing<br>6. Public key encryption<br>7. Digital Signatures<br>8. Identification protocols<br>9. Secure computation |

| **Course name** | **Contents** |
|---|---|
| Network security | 1. Networking review<br>2. Physical layer security<br>3. MAC & network layer security: spoofing, poisoning, hijacking<br>4. Transport layer security. TLS/SSL, QUIC, buffer overflow, throttling, mobility<br>5. Distributed denial of service. Principles, countermeasures.<br>6. Web security: server side, client side, code injection, impersonation.<br>7. Anonymization & obfuscation<br>8. Differential privacy |

| **Course name** | **Contents** |
|---|---|
| Mobile & wireless security | 1. Wireless channels & physical layer security<br>2. Wireless LAN security: Wi-Fi, Bluetooh, PAN<br>3. Security protocols & techniques in mobile networks: 4G/5G<br>4. Security in wireless sensor networks & IoT<br>DDoS in wireless networks & systems |

| Course name | Contents |
|---|---|
| Database systems | 1. Database & information systems: architecture<br>2. Code injection & query forgering<br>3. Security in structured information systems<br>4. Security in non-structured information systems<br>5. Differential privacy & anonymization in information systems<br>6. Secure queries, secure computations & homomorphic encryption<br>7. Secure transactions |

| Course name | Contents |
|---|---|
| Security management | 1. Security of infrastructure: logical & physical<br>2. Vulnerabilities, risks, threats. Metrics<br>3. Data & information protection<br>4. Equipment & systems security<br>5. Monitoring & surveillance, intrusion detection systems<br>6. Situation management<br>7. Security plan, strategies & policies<br>8. Standards |

| Course name | Contents |
|---|---|
| Audit & forensics | 1. Log monitoring, processing & auditing<br>2. Reverse engineering<br>3. Byzantine robustness in distributed systems, isolation<br>4. Digital forensic techniques for systems, networks & programs<br>5. Forensic techniques for data & information<br>6. Multimedia forensics |

| Course name | Contents |
|---|---|
| Secure software development | 1. Static analysis techniques<br>2. Dynamic analysis techniques<br>3. Software vulnerabilities<br>4. Memory corruption, resource overflow, access control<br>5. Operating systems security<br>6. Secure software development for mobile devices<br>7. Testing software security |

| Course name | Contents |
|---|---|
| Cybercrime & law | 1. Foundations of law<br>2. Faults, crimes & attacks to digital assets<br>3. Laws & regulations on data privacy<br>4. National laws on cybercrime<br>5. International laws on cybercrime<br>6. Digital rights management & intellectual property rights<br>7. Cyberdefense<br>8. Strategy & policy against cybercrime |

The range for the number of ECTS in the essential courses are summarised in the following table. The specific decision about the mandatory/optional character and the amount of ECTS will depend on the orientation of the programme, the professional profile and the academic

human resources. Finally, the master thesis will be a mandatory autonomous work from the student with a total number of ECTS no less than 15.

| Course name | ECTS range | |
|---|---|---|
| Cryptography | **6** | **Mandatory** |
| Network security | **12** | **Mandatory** |
| Mobile & wireless security | **6-12** | **Optional/Mandatory** |
| Database systems | **3-6** | **Optional/Mandatory** |
| Security management | **12** | **Mandatory** |
| Audit & forensics | **6-12** | **Mandatory** |
| Secure software development | **6-12** | **Optional/Mandatory** |
| Cybercrime & law | **3-6** | **Mandatory** |

At the time of writing, the percentage of development for each of these courses is approximately 60%: contents/modules have been agreed on, and the learning materials will be developed in the following weeks or are currently under development. Since the new programmes will be launched in September, 2018, none of the courses have been implemented yet. Regarding the (local) accreditation and recognition procedures, the requests for this goal have already been initiated in the three universities. The percentages of the level of achievements are in the following table:

| HEI | % (development/update) | % (recognition/accrediton) | % (implementation/delivery) |
|---|---|---|---|
| HUST | **85** | **25** | **0** |
| HCMUT | **85** | **25** | **0** |
| VNUA | **85** | **25** | **0** |

## Teaching/training activities

Vietnamese HIEs selected their participants according to their CV and ranking them according to the proved experience in the following related topics: applications, networking, databases, OS, programming, distributed architectures, etc. (both training and research)

As planned, two training visits have been carried out in Vigo (Spain) oriented to the preparation of Vietnamese staff within the scope of the new degrees. The training activities have been mostly centred around state-of-the-art technology training, presentation of research directions, and discussions on research management and research support to cybersecurity in the European entity, rather than in specific courses or narrow-focused talks. A summary of the main activities, their type, aims and achievements, follow:

1. Activity 1: Study Visit to the SOC of R, regional Telco - 1 day.
2. Activity 2: Risk Management at the regional HPC Centre (CESGA) – 1 day
3. Activity 3: Training on cryptographic research (GRADIANT) – 1 day
4. Activity 4: Designing e-learning contents for cybersecurity programmes (FAITIC-UVIGO) – 1 day.
5. Activity 5: Security in Network Infrastructure (IT department–UVIGO) – 1 day.
6. Activity 6: Case studies of the Tuning methodology over cybersecurity Programmes (EET-UVIGO) – 3 days.

Finally, as a result of the training activities, the staff in HCMUT, HUST and VNUA who participated in them have been in charge in their native institution of transferring his knowledge to the local faculty in order to finish the design of the accreditation files.