LETTER OF OFFER – CYBERSECURITY PROGRAMME 2019/2020

Issued by:

Masaryk University, Faculty of Informatics
Address: Botanická 554/68a, 602 00 Brno, Czech Republic
ID No.: 00216224
Bank account Nr.: 85636621/0100

Represented by: Prof. RNDr. Jiří Zlatuška, CSc., Dean

Contact person: XXXXXXXXXX

(hereinafter referred to as “FI MU”)

and addressed to:

GSO-1(A), Foreign Training (MT-16)
Directorate General of Military Training (MT-16)
General Staff Branch
Intergrated HQ of MoD (Army)
Room No 712, A wing
Sena Bhawan, Raja Ji Marg
New Delhi-110011
India

Represented by: Lt Col Sreenath Reddy

Contact person: XXXXXXXXXX

(hereinafter referred to as “MT-16”)

hereinafter jointly referred to as the “**parties**” and individually also as a “**party**”

I.
Subject of the Offer

1. The subject of this Offer is the participation of MT-16 nominated candidates in the “Special Long Term Programme in Cybersecurity”, which is at the FI MU side fully recognized and accredited as the Master of Science (Magistr) programme in Computer Systems, Communication and Security, with the specialization in information security. Hereinafter, the programme shall be referred to as Full Programme.
2. FI MU agrees to provide high quality training specified in the Article II of this Offer.

II.
Programme Courses

1. Content of the Full Programme

– *PV079 Applied Cryptography:* This course explores the issues of cryptography deployment issues, standards and applications. The course enhances students' working experience with up-to-date cryptosystems, and enables them to deploy cryptography effectively.

- *IV054 Coding, Cryptography and Cryptographic Protocols:* Lecture deals with the basic methods to solve three key problems of the transmission of information. All three problems are of large practical importance and their solutions are based on elegant theoretical results. On successful completion of the course students should be able to: understand problems of the theory of error-correcting codes; understand basic principles and results of the theory of secure communication; know principles and problems of basic cryptosystems for encryption (both secret and public key), digital signing and authentication; know methods to create core cryptographic protocols primitives; analyze and practically use simple cryptosystems; be experienced in methods of quantum cryptography and steganography.
- *PV181 Laboratory of security and applied cryptography:* The aim of this lab course is to understand implementation details of cryptographic algorithms and protocols and be able to apply the gained knowledge in practice. At the end of the course students should be able to design and implement cryptographic applications independently, and possibly also with support of smartcards.
- *PA168 Postgraduate seminar on IT security and cryptography:* The seminar participants will discuss a broad range of topics in IT security and cryptography in a greater depth. PhD and Master's students undertaking research in these and closely related areas are expected to report on their work.
- *PA192 Secure hardware-based system design:* The course is focused on architectures of secure digital systems, to ensure reliability, dependability and security of digital systems, assess and learn how to design safe and reliable digital systems. An important part of the course is to familiarize students with the principles and techniques of secure programming in language C and design of secure embedded systems. Course will present common problems and design of secure digital systems on real-world examples.
- *PA193 Secure coding principles and practices:* Language level vulnerabilities, secure programming techniques and approaches, input processing, code checking, security testing, integrity of modules, concurrent issues, random number generation and usage, security primitives, security code review.
- *PV204 Security Technologies:* The aim of this subject is to understand details of smart cards security, secure authentication and authorization, security of hardware modules, trusted boot, analysis of malware and rootkits (both black-box and gray-box), reverse engineering of binary applications, multilevel security and file/disk encryption. Student should be able to apply the gained knowledge in a practice based on experience gained from laboratory a project work.
- *IA169 System Verification and Assurance:* This course will provide the necessary theoretic background as well as hands-on experience with relevant tools for bug finding and formal verification techniques. An introductory insight into security standards like Common Criteria for Information Technology Security Evaluation and FIPS 140 shall be provided first, together with a discussion of security threat models. Following this, the core topics of this course will include testing, simulations, advance testing and symbolic execution, abstract interpretation, static analysis, theorem proving, automated formal verification as well as an introduction to model-based verification. With the help of a tutor students will get acquainted with a number of concrete software verification tools for analysis of concurrent systems, real-time systems, hybrid systems, cryptographic systems and systems with probabilities.

- *PA197 Secure Network Design:* Basic design requirements and principles (basic network architecture and functions, general requirements on the security and reliability). Network specific faults, threats, and attacks. Security architectures (Secure and resilient routing, secure DNS, secure channels, trusted network access, resilient architectures). Operational security management – how to design and manage reliable networks. Network monitoring and defence mechanisms (firewalls, IDS, netflow). Penetration testing. WiFi networks and security. (Wireless) personal area networks. Wireless Sensor Networks (WSN). Cryptographic aspects of WSN.
- *PA018 Advanced Topics in Information Technology Security:* This advanced-level course reviews selected topics in IT security in a greater depth. Students are expected to work on several assignments and a term project.
- **Elective Courses:**
    - *PV222 Security Architectures*
    - *PV210 Cyber security in an organization*
    - *IA066 Introduction to Quantum Computing*
    - *IA077 Advanced Quantum Information Processing*
- **Other courses,** in order to fulfill requirements of the Master programme Computer Systems, Communication and Security, with the specialization in information security as listed for the current academic year at the webpages of FI MU.
- **Project**
    - Master thesis (every thesis will have a supervisor from one country and advisor from other country). They would return to India in June and work on their Master thesis, submitting early in December with other students in the Master programmes and defending the thesis with the state exam in January or February.

III.
Letter of Offer and Acceptance Letter

1. The Letter of Offer from FI MU is based on a discussion of the Liaison Coordinators (see Section V below), with the following details:
    a. 3 offered positions for students from MT-16 in the Full Programme.
    b. Cost per participant for the Full Programme shall be 300’000 (three-hundred-thousands) Czech korunas. The total cost is therefore 900’000 Czech korunas.
    c. Starting date 9/9/2019 and final month of June 2020.
2. The Acceptance Letter must be received within two months of the issue date of a given Letter of Offer in order to take effect.
3. Letter of Offer and the corresponding Acceptance Letter based on the appendix A of this Letter of Offer received within three months of the date of a given Letter of Offer then form a mutual written agreement.

IV.
Price of Work and Payment Conditions

1. The Contracting Parties have agreed that the total price for each run of a designated programme specified in Article II and performed under conditions agreed in this Agreement amounts will be specified in Czech korunas in the amendments set in Article III.
2. The MT-16 agrees to pay this price upon invoices issued by FI MU. The date of issue of the invoice is also the date of the taxable transaction.
3. The Parties have agreed that an invoice shall be due within 45 days after the date of issue at FI MU, where FI MU guarantees the invoice delivery to the MT-16 contact address (email and postal addresses) within 15 business days of the invoice issue.
4. The MT-16 agrees to pay the first payment of one half of the total amount. The first payment will be invoiced within a month after the commencement of the programme run.
5. The full price agreed in the Article III will be invoiced within one month from the particular programme run completion (typically with the State final exams and thesis defence in February for the Full Programme and January or June for the Short Programme).
6. If MT-16 shall be in default with the payment of the Price agreed in the Article IV.1, the FI MU shall be entitled to require from MT-16 the penalty equal to 0,05 % from the due amount for each such day of default.
7. The provision regarding the penalty shall in no way affect the right of the Contracting Parties in respect to indemnity.

V.
Liaison Coordinators

1. Each Party nominates a Liaison coordinator who shall act as a contact person for all matters concerning this Agreement.
2. The Liaison coordinator on behalf of FI MU is XXXXXXXXXX, the Liason coordinator on behalf of MT-16 is XXXXXXXXXX.

VI.
Admission to the courses

1. Candidates will meet the following selection criteria for the Special Long Term programme of FI MU:

   1/ Completed Bachelor or Master degree in Computer Science / Computer Engineering / Computer Communications / Mathematics.
   2/ Extensive knowledge of Computer Science & Engineering
   3/ Basic knowledge of Cryptography and Computer Security
   4/ Academic track record, performance and English proficiency.
2. The participating students will be selected and admitted by FI MU on the recommendation of MT-16.
3. The deadline for sending in the completed applications for eligible candidates shall be no

later than April 30, 2019.

4. FI MU shall inform MT-16 of its final admission decisions within a month of the application of the candidates being made available to FI MU.
5. Students shall be subject to the rules, regulations and discipline of the FI MU. While registered in the courses within the programmes concerned, they will be registered as students of FI MU.

VII.

Dispute Resolution and Governing Law

1. Any dispute arising out of this Agreement shall be referred for resolution in the first instance to the liaison coordinators referred to in clause V.
2. If the dispute has not been settled sixty days after referral to them or within such other period as the parties may agree in writing, all disputes that may arise in connection with this present Agreement or the breach thereof shall be adjudicated exclusively by the Czech courts.
3. The contracting parties are aware of the requirements under the Czech Act no. 340/2015 Coll., on Special Conditions for Effectiveness of Some Contracts, Disclosure of These Contracts and on Registry of Contracts (Registry of Contracts Act), and if it is necessary according to this Act to publish this agreement, the contracting parties agree with its publication in the registry of contracts, as well as with the publication of any agreements (amendments), which supplement, change, replace or cancel this agreement. The contracting parties agree that the publication of the agreement in accordance with the above-mentioned Act is ensured by FI MU.

VIII.
Final provisions

1. The Parties declare that the laws of the Czech Republic are applicable to this Letter of Offer and the resulting agreement and to the legal relationship between the Parties resulting from it.

Masaryk University,
Faculty of Informatics

In Brno on March 4, 2019

____

Prof. RNDr. Jiří Zlatuška, CSc.,
Dean

Appendix A: ACCEPTANCE LETTER– CYBERSECURITY PROGRAMME 2019/2020

On behalf of MT-16 and with respect to the “LETTER OF OFFER – CYBERSECURITY PROGRAMME 2019/2020”, from Masaryk University, Faculty of Informatics, dated March 4, 2019, I hereby confirm acceptance of the proposal from the Letter of Offer regarding the training in the „Special Long Term Programme in Cybersecurity” and confirm that the conditions as stated in that Letter of Offer are accepted on our side without any modifications.

GSO-1(A), Foreign Training (MT-16)
Directorate General of Military Training (MT-16)
General Staff Branch
Intergrated HQ of MoD (Army)
Room No 712, A wing
Sena Bhawan, Raja Ji Marg
New Delhi-110011
India

In New Delhi on 9.9.2019

____
Lt Col Sreenath Reddy