# Intensive Programme on Information and Communication Security

Christian Schläger, Ludwig Fuchs, and Günther Pernul
*Department for Information Systems, University of Regensburg, Germany*
*(christian.schlaeger | ludwig.fuchs | guenther.pernul) @ wiwi.uni-regensburg.de*

## Abstract

*IT Security is a problem that can only be addressed and taught holistically. Just as broad as the field of ICT itself, IT Security is an integral part of all network and software applications. Security must be guaranteed throughout services. Too often, a single university or department cannot offer the complete range of IT Security subjects to their students or provide the up-to-date information and knowledge needed. Consequently, the demand of keeping up with hackers, threats, and risks is hardly met. Our proposal is a combination of the know-how of multiple institutions, aligned in an Intensive Programme for Master- and PhD Students of Computer Science, Information Systems, and Business Informatics. The proposed Intensive Programme on Information and Communication Security (IPICS) uses e-learning and traditional learning methods to form a blended learning course. Using the synergies of 19 contracted European Universities and their IT Security experts, IPICS will deliver momentum for IT Security education and training to those who take part and furthermore through their networks.*

## 1. Introduction

Systems, Business Informatics, and Computer Science have become a viable part of Europe's universities' curricula. IT professionals are needed by companies, research institutes, and software manufacturers alike. Society and economy are requesting well educated, flexible professionals, able to govern and manage the complex subject of ICT. Due to its complexity, one of the major challenges of ICT is security. Although recognised as being very important, today, IT Security only plays a minor part in most curricula. Too often consequences of system failures, successful attacks by hackers, terrorists, competitors, or business espionage are put aside in favour of other ICT subjects. As IT Security should be part of every IT process, hard- and software, as well as business policies it is just as complex as the systems it secures. In addition, shorter software life cycles and the competition between attackers and software developers put increasing pressure on IT Security experts. In this race most universities are not able to provide needed resources and staff for a thorough and comprehensive IT Security education.

In the last decade some universities have specialised in IT Security providing bachelor, master, and PhD courses as well as master degrees in IT Security. Within Europe's constructive heterogeneity and diversity different IT Security clusters have specialised differently summing up to a holistic, exhaustive, and innovative knowledge base in Europe. Since 1998 the IPICS network is trying to exploit this knowledge base to the best for their students and institutions. Former IPICS schools took place in Austria, Greece, Belgium, Spain, Sweden, and the UK.

There is still significant need for co-operation and collaboration of Universities in the field of Information and Communication Security, with a view towards

- increasing European cohesion in developing a common IT Security culture;
- monitoring the needs of society and industry in information and communication systems security education;
- developing, maintaining and disseminating European-wide curricula and intensive programmes in the field.

In 2008 the IPICS is going to be held in Regensburg, Germany. The programme has been contracted as an Erasmus Intensive Programme by the European Union receiving funds via the National Agency DAAD – the German Academic Exchange Service.

The upcoming IPICS will introduce two new elements to the curriculum:

- Web-based trainings and
- Web-based dissemination.

In the past, demands on the IPICS have grown. Motivated by industry requirements as well as new specialisations among the partner universities, the content to be taught during the two IPICS weeks has enlarged. Simultaneously, the complexity has reached a level where web-based training is needed to establish

a common knowledge of IT Security among the participants. Web-based dissemination is used to make the outcome and results of IPICS accessible to partner universities, IPICS students, and the public. IT Security knowledge is a subject so important for today's processes and networks, access to it must not be restricted. In addition the results of past IPICS meetings will also be published as a work-book on IT Security with Artech House.

## 2. IPICS History

The IPICS organiser can look back to a successful history of previous events. So far, IPICS meetings and schools were held in ten different locations throughout Europe. Starting with the first IPICS in 1998 in Vienna, Austria each summer an IPICS school was organised and conducted. Table 1 gives an overview of all past IPICS schools.

TABLE 1. IPICS HISTORY

| Year | City | Country |
|---|---|---|
| 1998 | Vienna | Austria |
| 1999 | Chios | Greece |
| 2000 | Stockholm | Sweden |
| 2001 | Samos | Greece |
| 2002 | Samos | Greece |
| 2003 | Málaga | Spain |
| 2004 | Graz | Austria |
| 2005 | Chios | Greece |
| 2006 | Leuven | Belgium |
| 2007 | Glamorgan | United Kingdom |
| 2008 | Regensburg | Germany (scheduled) |

Aim and organisation of the first IPICS was described by Katsikas in 1999 [1] and further developed by the same author in 2000 [2].

## 3. Erasmus Intensive Programme

For 2008, the IPICS is funded in the EC's Lifelong Learning Programme[1] (formerly known as SOKRATES) as an Erasmus Intensive Programme (IP). An IP is a short programme of study for subject related work between 2-6 weeks. Students and teachers from higher education institutions can participate. Eligible for funding are only EU countries. The consortium must incorporate at least three different countries. Aims of the IP comprise[2]:

- Encourage efficient and multinational teaching of specialist topics which might otherwise not be taught at all, or only in a very restricted number of universities;
- Enable students and teachers to work together in multinational groups and so benefit from special learning and teaching conditions not available in a single institution, and to gain new perspectives on the topic being studied;
- Allow members of the teaching staff to exchange views on teaching content and new curricula approaches and to test teaching methods in an international classroom environment.

[1] http://ec.europa.eu/education/programmes/llp

[2] http://ec.europa.eu/education/programmes/llp/guide/fiches/erasmus6_e

## 4. Concept and Curriculum

### 4.1 Organisational Structure

Following the successful organisation of the past IPICS an organisational form was defined consisting of four main entities and stakeholders.

1) **IPICS Standing Committee (SC)**: To ensure continuity and quality an IPICS standing committee was formed. It is responsible for the general curriculum, selection of IPICS partner organisations, evaluation of efforts, students, and lecturers, quality control, scientific dissemination. Members of the SC as of today are: Prof. Dr. Sokratis Katsikas (GR), Prof. Dr. Gerald Quirchmayr (AT), Prof. Dr. Bart Preneel (BE), Prof. Dr. Javier Lopez (ES), and Prof. Dr. Günther Pernul (DE).
2) **IPICS Local Coordinator (LO)**: The Local Coordinator is responsible for the organisation and infrastructure on-site. It will be organising student and lecturer mobility, lectures, resources including e-Learning infrastructure elements, finances, and other local organisational tasks. The local coordinator reports to the NA and the SC on status, participant feed-back, and quality guidelines set by the SC. For 2008, IPICS LO will be the University of Regensburg.
3) **IPICS Universities (IU)**: So **far** 19 European universities have merged as IPICS Universities each sending at least one **IPICS Lecturer (IL)** to the course.
4) **IPICS Students (IS)**: Master- **and** early PhD students inscribed at an IU can apply for the programme. Additionally the programme is open for students from non-IU universities and for High Professional IT Security experts.

The single building blocks and their connections are depicted in Fig. 1.

### 4.2 Curriculum

Each day will be dedicated to two specific IT Security topics. As a basis the IT Security curriculum by the German GI will be taken as a guideline [3]. For each topic one expert from an IPICS partner university will be responsible. The subject will be taught by lectures, lab experiments, using team work, and case studies. The IPICS SC is responsible for selecting only topics fitting into a common scenario. For 2008 this scenario will be "Security for European Enterprises".

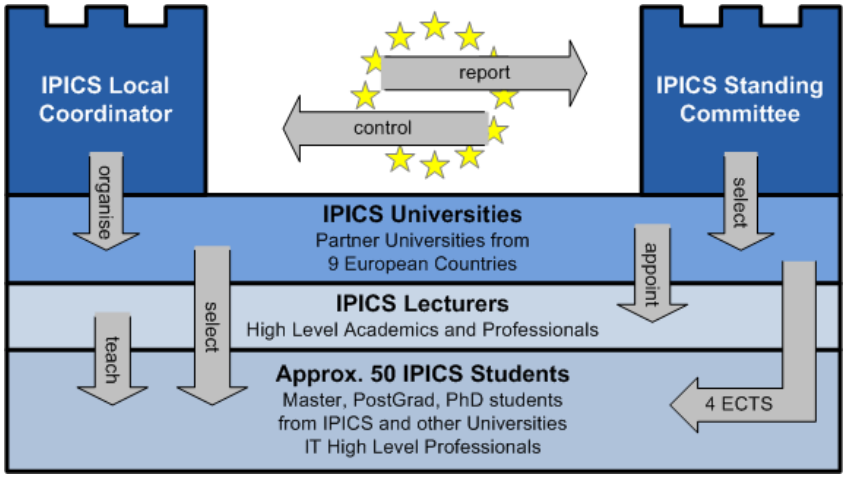


**Fig. 1. IPICS organisation and building blocks**

This case is superimposed to all lectures. This enables the integration of the partners' innovations and research into a broader context, making knowledge usable and understandable for all IPICS students in this multidisciplinary field.

The IPICS adds value to every IPICS member's curriculum, raising IT Security awareness in all institutions and forming new knowledge and research connections throughout Europe. IPICS students will return to their home institution passing along knowledge, references, and contacts from the IPICS to all participating countries helping in forming an EU wide culture of IT Security. Additionally, IPICS students will not only be educated to become professionals in their chosen field but as well become security experts on a global scale.

The IPICS formally establishes and extends existing co-operation between the participating institutions. Even though a number of national and international associations are active in the field (e.g. GI FB Sicherheit, IEEE Security & Privacy, ACM SIGSAC), only one international working group (IFIP WG 11.8[3]) is busy with issues related to security education. Many of the members of IFIP WG11.8 are also participating in the IPICS. Moreover, even though the number of formal education programmes in the field of Information and Communication Systems is growing, IT Security education still remains unacceptably low, compared to the stated needs of industry and society. Indeed, there is very high demand in industry for professionals trained in Information and Communication Systems Security. Moreover, it is clear today that all Computer Science, Informatics and related subjects students should at least be exposed to one or two courses in IT Security; however, there is a clear lack of expertise on the part of European Universities for meeting these minimum requirements. This is partly due to the fact that Information and Communication Systems Security is an interdisciplinary field, comprising aspects of cryptology, networking, operating systems, databases, hardware, human factors, law, management, economics, etc. All of these subjects are included in the IPICS curriculum.

The IPICS adds value to the curricula of the participating universities by extending and complementing local courses and lectures. The IPICS curriculum offers basic IT Security lectures to assure a common basis and understanding. On top of these basic seminars, each IPICS university adds its own specialisation to the curriculum. Under the superimposed case, defined by the IPICS SC, all special topics are integrated. It is obvious, that no single European university can offer such an

[3] http://www.118.ifip.info/

exhaustive approach to IT Security. Only by using synergies and joined resources the complete field of Information and Communication Security can be addressed.

The innovation of IPICS lies in this joined European effort as well as in the integration of specialisations made tangible via a global IPICS case study.

Nineteen topics have been identified representing needed knowledge and subjects for the partner universities on the one hand and subjects that the consortium has special expertise in on the other hand. The curriculum comprises classical IT Security subjects such as Cryptography as well as relatively new topics such as Authentication and Authorisation Infrastructures. With lessons in IT Security methodology young PhD students are addressed. Theoretical knowledge is made tangible by case studies and training on actual applications. The actual learning method will vary. Lessons are given for example as lab-work or group work.

The complete list of IT Security topics taught at IPICS is given in Table 2.

TABLE 2: IPICS CURRICULUM - TOPICS

| No. | Topic |
|---|---|
| 1) | Security Concepts, Services and Threats |
| 2) | Case Study "IT Security in European Enterprises" |
| 3) | Information Security Management |
| 4) | Authentication Technologies |
| 5) | Authorization and Access Control |
| 6) | Security for Data Centric Applications |
| 7) | Modern Cryptology |
| 8) | Network Security |
| 9) | Mobile Security |
| 10) | Smart Cards and Tokens |
| 11) | Authentication and Authorization Infrastructures |
| 12) | Privacy and Privacy-Enhancing Technologies (PETs) |
| 13) | Content Control Technologies |
| 14) | Cybercrime Investigation |
| 15) | Computer Forensics |
| 16) | Systemic Holistic Approach to IT Security |
| 17) | Legal Issues and Security Standards |
| 18) | Research Methodologies for Young Researchers in IT Security |
| 19) | Applications of Security |

IPICs will start on Sunday with the participants and lecturers arriving at site. On Monday lectures start. Each day is divided in two blocks (as depicted in Fig. 2). Time and resources are assigned to topics according to their significance for IPICS, IT Security, and other topics. The topic of, e.g., Modern Cryptology, comprises two complete blocks as it is necessary and fundamental for many other IT Security related subjects and understanding of the subject is vital for all students IPICS.

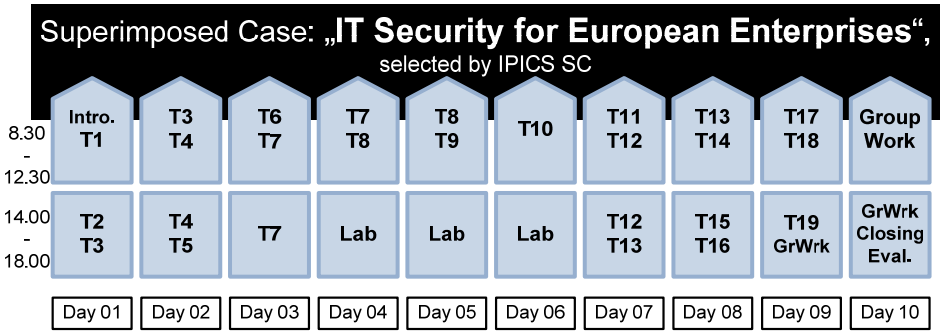


**Fig. 2: IPICS Curriculum - daily schedule**

Overall, IPICS will have 10 lecture days and a social programme designed to let students and lecturers network and discuss. For days 4-6 lab work is scheduled where students are going to try hacking and securing systems. Additionally, these lab works sessions can be used for simulations [4].

IPICS will close with a series of group works and an evaluation session.

## 5. E-Learning Elements

The IPICS will make use of ICT not only to demonstrate the effects of IT Security but also as a methodological element for teaching. During the course students will use the Internet for their research, conduct group and practical work in a computer laboratory, and work with computer-based simulations.

These actions alone can already be considered electronic learning or, as they are used in combination with traditional lessons, blended learning. This work, however, will focus on web-based activities happening post and prior to the actual course.

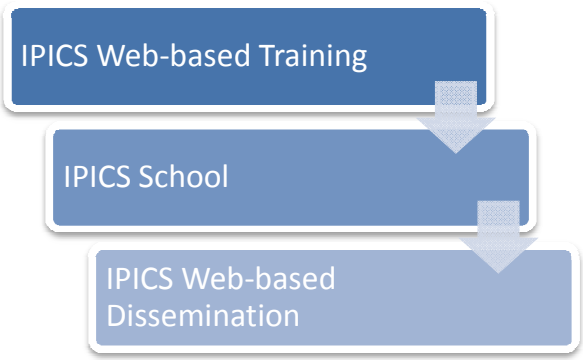


**Fig. 3: IPICS learning phases**

IPICS consists of three subsequent phases (see Fig. 3), namely the web-based training of participants, the IPICS School itself, and the consecutive Web-based dissemination of knowledge. The first phase will be used for establishing common knowledge about IT Security among all participants. This phase is called "IPICS Web-based Training". Emphasis is put on collaboration and individual needs. To support knowledge and information sharing, an electronic document management system (EDMS) will be installed (e.g. BSCW). This system is going to form the central point of electronic information exchange in the first learning phase as participants are going to be able to use it for web-based training prior to the IPICS lessons. Students will find lectures preparing them for the course in Regensburg, further information in the form of web links, or links to the partner universities' e-learning tools.

Additionally, students can contact the IPICS teachers and lecturers as well as their fellow students with questions concerning preparation, content or exercises. This way the electronic system will facilitate ad-hoc information exchange and problem solving among participants.

It is our firm believe that IT Security cannot be taught online alone but needs discussion and exchange in an environment like a summer school. The IPICS has been designed and organised to not only to transfer knowledge via lectures but especially to enable the exchange of experiences, research ideas, and effective collaboration. Consequently, IPICS uses e-Learning only as a supportive tool.

However, effective collaboration can only be enabled if participants share a common knowledge background as far as IT Security basics are concerned. During the "IPICS School" participants will continue using the EDMS for knowledge exchange and solving organisational issues. As mentioned beforehand lab experiments, team work, case study efforts, and other practical work are going to be supported by the usage of collaborative software and computer-based simulations.

After the actual IPICS school, the third phase begins: "IPICS Web-based Dissemination". Aiming at the creation of a European culture in IT Security the IPICS organisers will set up a Wiki as a website that allows participants straightforward access to add, edit, and remove content on IPICS subjects. The IPICS Wiki will be used as a knowledge management tool. Students will provide the Wiki with their knowledge, experiences, research activities, and essays on IPICS subjects and topics. This way the IPICS Wiki will become a research and information tool for IPICS members and – extending the impact of IPICS – to all IPICS university students and the public. Furthermore it can be used as a common knowledge basis and discussion platform for future IPICS programmes. It is the organisers' goal that the Wiki develops to a durable and vivid base for IT Security knowledge exchange in the future. In this fashion its contribution and improvement is to essentially connecting the previously independent and isolated yearly IPICS programmes representing a common base of IT-Security topics and knowledge.

In addition, the IPICS will use a portfolio of ICT tools to support collaborative project working. A mailing list will be set up to encourage communication and exchange of ideas among the participants at large. An IPICS web site (with the project description and its current achievements) will be set up and regularly updated. The development of local, partner specific WWW pages will be also encouraged. The project web site will be used also for dissemination purposes.

## 6. Conclusion

IPICS brings together students and researchers throughout the European Union interested in IT Security. A curriculum has been designed extending the IPIICS partner universities' specialisations. Thus, IPICS enhances IT Security training. To address the inherent complexity of IT Security and enable an environment of knowledge exchange, IPICS has settled on using blended learning methods. Students can learn necessary basics online and start cooperating beforehand. After the IPICS summer school, the process of acquiring and dissemination knowledge is not stopped but further fostered with the help of

knowledge management tools like a Wiki, mailing lists, and new groups. This way the independent yearly IPICS programmes are connected and building up on a common knowledge base. Doing this seamless information exchange and the development of a vivid IPICS community are ensured.

## References


[1] S. K. Katsikas, "Academic curricula and curricula developments in Europe-The ERASMUS/SOCRATES Approach", Proc. of the Ifip Tc 11 WG 11.8 1st Conference on Information Security Education (WISE 1), Kista, Sweden, 1999.

[2] S. K. Katsikas, "A Postgraduate Programme on Information and Communication Systems Security", Proc. of the 16th Annual Working Conference on Information Security (Ifip TC 11) "Information Security for Global Information Infrastructures" (SEC 2000), Beijing, China, 2000.

[3] GI AK Sicherheit, "IT-Sicherheit in der Ausbildung". Bonn: Gesellschaft für Informatik e.V. (GI), 2006, pp. 12.

[4] G. Goluch, A. Ekelhart, S. Fenz, S. Jakoubi, B. Riedl, and S. Tjoa, "CASSIS - A Computer-based Academy for Security and Safety in Information Systems", Proc. of the 2nd International Conference on Availability, Reliability and Security (ARES 2007), Vienna, Austria, 2007.


## Acknowledgement


This work owes thank to all participating lecturers and institutions. Input came from all involved lecturers, the IPICS Standing Committee, and the IPICS Institutions.


## Appendix

TABLE 3: IPICS UNIVERSITIES AND SPECIALISATIONS (AS OF 1.12.2007)

| University | | Specialisation |
|---|---|---|
| Graz University of Technology | AT | Security for Embedded Systems, RFID, Network Security, Trusted Computing, Cryptography, E-Government |
| Vienna Technical University | AT | Organizational IT Security, Security In E-Learning, Penetration Testing, Internet Security, Software Security |
| Vienna University | AT | IT Security Management, Legal Aspects, Security Compliance, Crisis Management |
| Katholieke Universiteit Leuven | BE | Cryptology, Mobile Security, E-Payment |
| University of Regensburg | DE | Information Security, Security Management, Authentication, Cryptography, Penetration Testing, Authorisation, Access Control, Identity Management, Privacy |
| University of Castilla-La Mancha | ES | Database and Data Warehouses Security, Security in Web Services, Security Metrics, Security in Business Processes, Information Security Management Systems, Security Architectures, Security Requirements |
| University of Málaga | ES | Information Security, Network Security, Applied Cryptography, Authentication & Authorization Infrastructures |
| University of Lapland | FIN | Applied Information Technology, Law, Management and Business |
| Aristotle University of Thessaloniki | GR | Information Systems Design and Implementation, Information Security, Health Care Informatics (E-Health), Database Systems Design Implementation and Security |
| University of Piraeus | GR | Network Security, Intrusion Detection, Risk Analysis, Security Management |
| University of the Aegean | GR | Risk Analysis, Smart Cards, PKI, Security Patterns, Privacy |
| University of Milan | IT | Privacy, Access Control Policy Models and Systems, Data Security, Information Protection |
| Karlstad University | SE | Privacy Enhancing Technologies, Identity Management, Social Aspects, Legal Aspects |
| University of Lund | SE | Security Strategy, Holistic Security Approach, Contingency Plans |
| Kingston University London | UK | IT Computer Communication Systems, Digital Forensics, Military Command and Control Systems, Image Recognition Systems |
| Royal Holloway University of London | UK | Cryptography, Network Security, Smartcards, Trusted Computing, Mobile Security, Security Frameworks |
| University of Glamorgan | UK | Computer Forensics, Computer Systems Security, Mobile Computing, Computer Crime, Wireless Security |
| University of Kent | UK | Public Key Infrastructures, Privilege Management Infrastructures, X.509, Grid Security, Campus Security, Single Sign On, Firewalls |
| University of Plymouth | UK | Information Security Management, User Authentication, Computer Crime, Network Security, Human Aspects and Usability, Intrusion Detection and Response, Malicious Code |