A CBK for Information Security and Critical Infrastructure Protection

Marianthi Theoharidou, Eleftheria Stougiannou, Dimitris Gritzalis

Information Security and Critical Infrastructure Protection Research Group,
Dept. of Informatics, Athens University of Economics and Business,
76 Patission Ave., Athens, GR-10434, Greece
{mtheohar, estoug, dgrit}@aueb.gr

Abstract. Academic institutions educate future Information Security and Critical Infrastructure Protection (ISCIP) professionals, offering expedient and broad knowledge of the field. As industry often demands higher productivity and stronger specialization, several organizations (academic, governmental, industrial) considered the use of a Common Body of Knowledge (CBK), to serve as a tool that appropriately groups together the essential knowledge of this field. In this paper, we review the content of current ISCIP curricula, we define the necessary skills of an ISCIP Professional - as indicated and suggested by the industry - and form a multidisciplinary CBK of the ISCIP field.

Keywords: Common Body of Knowledge (CBK), Academic Curriculum, Academic Programme, Critical Infrastructure Protection.

1 Introduction

The demand for Information Security and Critical Infrastructure Protection (ISCIP) professionals is usually addressed by academia, in an expedient and broad way [10]. From its side, industry expects high productivity and strong specialization [4]; thus, it expects from academic institutions to focus mostly on "applied security", and give comparatively less emphasis to the "principles" [3]. The resulting "gap" is usually bridged by training courses and seminars [12], as well as industry-initiated and supported certifications on various security-related topics [8, 9].

The need for skilful ISCIP professionals led several organizations (academic, governmental, industrial) to consider the development of a Common Body of Knowledge (CBK) for the security domain. A CBK is "a collection of information and a framework that provides a basis for understanding terms and concepts in a particular knowledge area. It also provides a set of basic information that people who work in that knowledge area are expected to know"[1]. According to the International Information Systems Security Certifications Consortium (ISC)², a CBK is defined as "a taxonomy - a collection of topics relevant to information security professionals around the world" (www.isc2.org). In this paper, we consider a CBK as a conceptual means that define the knowledge, which is considered essential for the cognitive background and the required skills of a professional.

Several of the existing CBK efforts were initiated by the industry, mostly for certification processes of security professionals (e.g., CISSP, GIAC, CISA, etc.). One may refer to the (ISC)² CBK, which is used for certifying CISSP Professionals and receives wide recognition. It focuses on establishing a common framework of information security terms and principles, which would allow information security professionals to discuss, debate, and resolve relevant issues. It includes ten "domains" [6] and it reflects mostly the industry needs. However, its adaptation for security curricula suffers by the risk of adopting solely the practitioner's view of security.

Typical academic examples include a CBK for "Information Assurance" [3], a CBK for "Information Security in Network Technologies" [7], and a CBK for Information Security professionals [10]. These few in number efforts do not aim at providing a security CBK, but they focus on a sub-domain and serve as a guide to create a course or a curriculum [3, 7]. The CBK for "Information Security in Network Technologies" [7] provides only a schematic representation of the field, without any details about how the CBK was developed. The Information Security CBK [10] focuses on minimizing the perceived "gap" between the academia and the industry, but it is quite generic, as its main goal is to prove the concept and not give an extensive CBK. It divides the Information Security field in technical and non technical topics.

A recent governmental initiative resulted in a CBK for "Secure Software Assurance" for the U.S. Dept. of Homeland Security [1, 8]. It provides a basis for the "secure software engineering" discipline and educators can use this guide to identify both, appropriate curricular content, as well as references that detail it. The guide is designed to cover the need of the US government to procure secure software.

We consider that ISCIP is a multidisciplinary endeavor [5, 13]. For its better understanding, analysis and practice, a professional should use knowledge from fields such as management, business administration, law, ethics, sociology, political science, criminology, didactic, etc. However, none of these CBK covers ISCIP in such a way. They seem to focus on specific sub-domains of ISCIP (e.g. CBK suggested by [3, 7]), thus offering limited understanding and a narrow perception of the ISCIP as a whole.

2 Methodology for CBK Development

We aim at identifying, defining and conceptually presenting a multidisciplinary CBK for ISCIP, which may serve as a tool for developing an ISCIP curricula. We will take into account the expectations of the industry, in an effort to bridge the "gap". In order to do so, we followed a three-step approach.

Step 1: We identified the industry and academic views on this issue, by performing:

(1a). A survey on curricula and courses (Section 3). As ISCIP is dealt within different curricula, we chose and focus on those university programmes, which are related to the "information scene". As a result, we selected (undergraduate and postgraduate) programmes on computer science, business administration, information systems management, sociology, and law, that either offer an academic degree on ISCIP, or offer courses on, or related to, ISCIP.

(1b). A survey on the industry demand for ISCIP professionals, in order to identify the excepted skills of an ISCIP professional. We consulted the Career Space Consor-

tium (www.career-space.com), a coalition which includes eleven major ICT companies and the European I&CT Industry Association. It defines Generic Skills Profiles for ICT professionals. From the existing profiles we selected those related to ISCIP. With these into account, we reviewed the current demand, regarding the required knowledge and skills of a professional, and enriched the skill set.

Step 2: After the surveys were completed, we defined: (a) the structure and (b) the content of an ISCIP CBK. We first selected the disciplines that were identified to be closely related to ISCIP. Then, we identified the prerequisite knowledge by other disciplines, which an ISCIP professional must acquire.

Step 3: We developed a hierarchy of concepts and elements needed in order to develop the CBK. A top-down approach was adopted and the hierarchy was filled up with elements, according to the university curricula we had examined in the relevant survey. After the hierarchy was complete, it was checked against the skills/knowledge set, as defined by our survey. Then, we combined the elements and grouped them under a common "root", so as to create a classification of the topics. The result was a CBK with ten domains, where each domain is analyzed in a more detailed level.

3 ISCIP Programmes and Courses: A Survey

The first step was to identify the structure and the content of the current ISCIP programmes and courses. In total, we studied 135 academic institutions, which offer curricula on: Computer Science, Information Systems, Management, Engineering, Business Administration, or Law. We selected them based on a) their quality, b) their faculty and c) their geographical position. Our survey was based on an online search through university websites, as well as a study of their syllabi. It indicated that 15 institutions, at the undergraduate level, and 45, at the postgraduate level, offer degrees of some kind on ISCIP. Most of them are run under the umbrella of either a Computer Science or a Computer Engineering Department. Several offer, usually optional, ISCIP courses, without offering a degree on ISCIP. From those that offer ISCIP degrees, only few syllabi include courses from other disciplines. Examples include skills like written/oral communication, public speaking, ethics, law, and management. Table 1 refers to the content of ISCIP courses, presented in 7 categories.

Table 1. ISCIP courses content.

Category	Usual content of ISCIP Courses
Access Control and Privacy	Identification, Authentication, Access Control, Authorization, Anonymity, Privacy
Risk and Attacks	Attacks, Vulnerabilities, Risks, Intrusion Detection, Malicious Software, Tests and Audits, Safeguards, Intrusion Handling
Cryptography	Applied Cryptography, Digital Signatures/Certificates, Key Management, PKI
Networks	Security Theory, Protocols and Algorithms, Firewalls
Security Design	Design of Computer Systems Security
Business	Business Continuity Plan
Other	Ethical and Legal Issues

4 Skills of an ISCIP Professional: a review

In order to develop a CBK, one has to determine the skills that are needed when dealing with ISCIP problems. We first chose the ICT professional areas[1], as defined by the Career Space Consortium, which refer to specific security knowledge. In order to do so, we studied the content of the security courses that we identified in the previous section. Then, we listed the skills required by the chosen ICT categories professionals. Tables 2 includes the skill set of an ISCIP Professional. The order of appearance is random and all the skills are considered equally important.

Table 2. Technical and Behavioural skills of an ISCIP professional.

Category	Skills
ICT	Networks, Technology and Computer Engineering, Systems Design and Architecture, Programming, Software Development, Mathematics, Statistics, Project Management, Business Strategy and Requirements Analysis, Testing, Basic Security Skills, Technical Documentation, System Management, Quality Assurance, Evaluation and Configuration Methodologies.
Security	Information Security and Human Computer Interaction, Computer Forensics, Database Security and Data Mining, Operation Systems Security, Security Architecture, Malicious Software, Internet and Cyber-security, Incident Handling, Hacking, Cryptography, Biometric Techniques, Smart Cards, Auditing, Data and Infrastructure Protection, Risk Management.
Behavioural	Leadership, Ethics, Analytical & Conceptual Thinking, Perspicacity, Creative Thought, Knowing one's limits, Professional Attitude, Communication, Technical Orientation & Interest, Customer Orientation, Strategy & Planning, Writing & Presentation skills, Efficiency & Quality, Applying Knowledge.

5 CBK Development

This CBK aims at reconciling industry and academia, by taking into account the results of the surveys we have conducted, and, at the same time, reflects the multidisciplinary nature of ISCIP [5, 11, 13]. Practically, we cover thirteen "Dimensions of Information Security", namely Governance/Organizational, Ethical, Awareness, Policy, Certification, Measurement/Metrics, Best Practice, Legal, Technical, Strategic/Corporate Governance, Insurance, Audit, and Personnel/Human [11]. We developed the ISCIP CBK in a top-down approach. We identified several fundamental disciplines, and then the CBK was further analyzed in more specific concepts. First, we identified seven ISCIP related disciplines: Computer Science, Computer Engineering, Law, Sociology/Criminology, Ethics/Psychology, Business and Information Systems Management, and Didactic. Then, we identified and described the prerequisite knowledge that

[1] Integration and Test Engineering, Systems Specialist, Data Communication Engineering, DSP-Application Design, Technical Support, Communication Network Design, Software and Application Development, Software Architecture and Design, Research and Technology Development, ICT Management, IT Business Consultancy, ICT Project Management.

must be incorporated by other disciplines. Based on the seven CBK disciplines, we categorized the security courses identified in the first survey, as well as the skills identified in the second survey. An hierarchy was then formed. We added as elements all the topics found, following a top-down approach. The final step was to combine the related elements of the different disciplines and to group these elements under a common "root". Then, we grouped the knowledge in ten domains, presented in Table 3.

Table 3. ISCIP CBK domains.

Domain
1. Security Architecture and Models
2. Access Control Systems and Methodology
3. Cryptography
4. Networks and Telecommunications Security
5. Operating Systems Security
6. Program and Application Security
7. Database Security
8. Business and Management of Information Systems Security
9. Physical Security and Critical Infrastructure Protection
10. Social, Ethical and Legal Aspects of Security

Each general domain is then analyzed into sub-domains. A selection of seven domains are schematically presented in the Appendix (Fig. 1-7)[2]. Each element of them can be further analyzed in more detailed sub-elements. Here, we present the elements up to their second level of analysis. One should note that some elements are included in more than one domains and that, in each domain, the disciplines each topic mainly derives from are graphically presented.

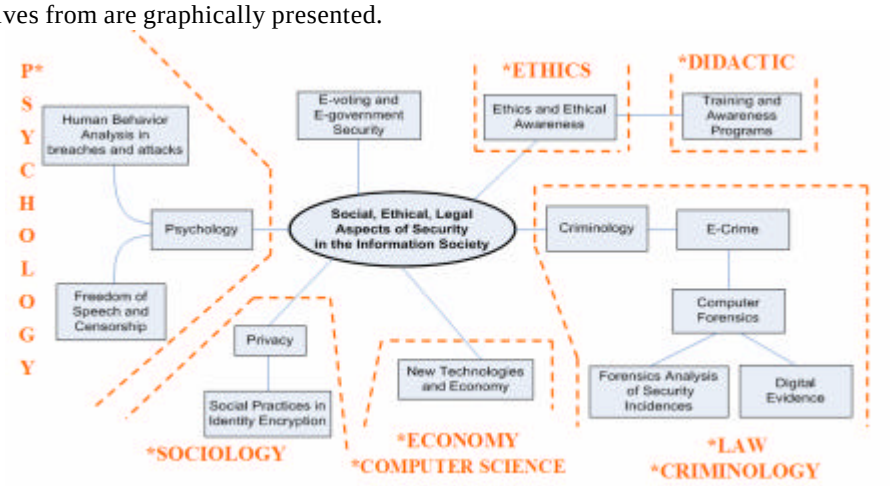

Fig. 1. Social, Ethical, and Legal Aspects of Security (Domain 10)

[2] An earlier version of this paper appears in the IEEE Security & Privacy, Vol. 4, No. 2, pp. 64-67, March/April 2007.

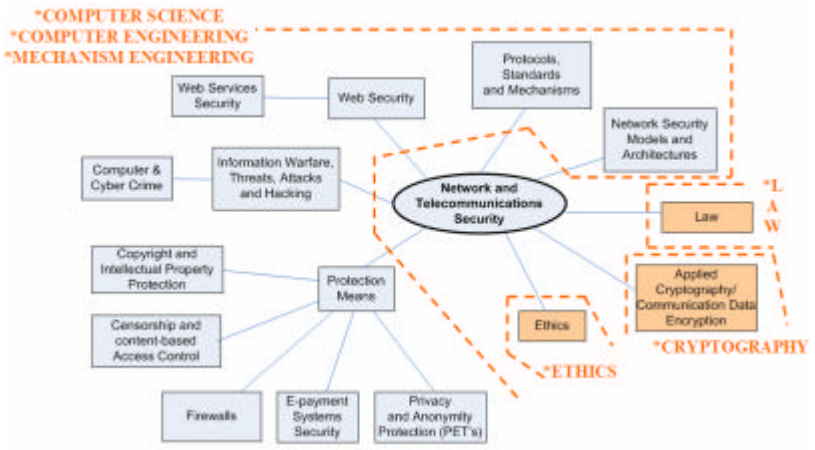

Fig. 2. Network and Telecommunications Security (Domain 4)

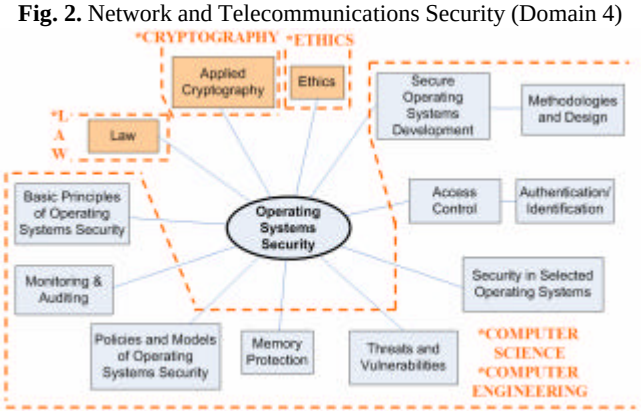

Fig. 3. Operating Systems Security (Domain 5)

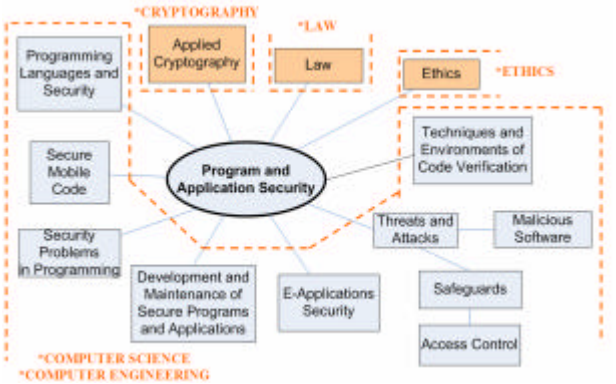

Fig. 4. Program and Application Security (Domain 6)

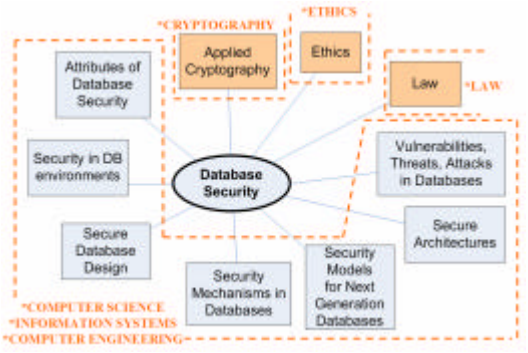

Fig. 5. Database Security (Domain 7)

Fig. 6. Security Architecture and Models (Domain 1)

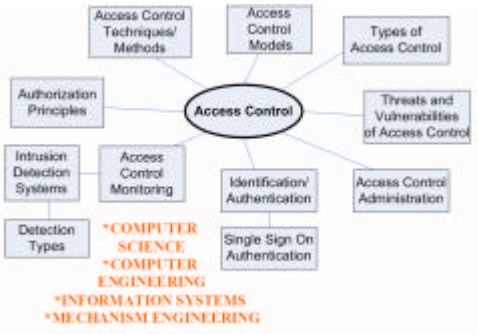

Fig. 7. Access Control Systems and Methodology (Domain 2)

6 Conclusions

We reviewed the content of current ISCIP curricula and courses, formed a skill set of the ISCIP Professional and, based on these, we formed a broad ISCIP CBK that encompasses seven disciplines. We designed the CBK to serve as a tool when designing a curricula or course in ISCIP. It is presented in two levels of analysis and categorizes the knowledge of the field. Nevertheless, this CBK has not been applied thoroughly, so evaluation results are not yet available. We will improve and evaluate it, when we

observe and document its use in the design of academic courses or curricula, which is one of our future goals. One idea is to restructure a course in ISCIP, based on this CBK, either an introductory course or a more specific one based on one or two domains. Furthermore, an ISCIP CBK needs to be constantly refined in order to fit into the emerging context and content of the field, so this is an ongoing process. The ten domains most likely will remain the same for some time, however, we expect their elements to transform regularly. Its application may also introduce refinements, additions or different groupings. We have to point out that this CBK was initially formed to assist on curricula design. Therefore, it is intended to be abstract and generic, as it attempts to group and categorize all the ISCIP knowledge, and not a specific ISCIP topic of interest (e.g. Information Assurance). This is the reason why it does not include the content and the teaching material of the knowledge elements and only their structure. We believe that this CBK can help the teacher structure the contents of his course or curricula and then he can enrich its course material from commonly accepted sources.

References

1. Bishop M., Engle S.: The Software Assurance CBK and University Curricula. 10th Colloquium for Information Systems Security Education. University of Maryland, USA (2006). Available online at: http://nob.cs.ucdavis.edu/bishop/talks/2006-cisse-1/swacbk.pdf.
2. Cabay M.: Information security education resources for professional development, ver. 11 (2004). Available online at: www2.norwich.edu/mkabay/overviews/infosec_ed.pdf.
3. Crowley E.: Information system security curricula development. In: Brewer J., Mendonca J. (Eds.): Proc. of the 4th Conf. on ITechnology Curriculum. ACM Press, USA (2003).
4. Egan L.: Closing the "Gap" between the university and industry in computer science. ACM SIGCSE Bulletin, Vol. 8, No. 4. ACM Press (1976) 19-25.
5. Gritzalis D., Theocharidou M., Kalimeri E.: Towards an interdisciplinary information security education model. In: Miloslavskaya N., et al. (Eds.): Proc. of the 4th World Conf. on InfoSec Education (WISE-4). Moscow (2005) 22-35.
6. Krause M., Tipton F. 2006. Handbook of Information Security Management, CRC Press.
7. Morneau K.: Designing an Information Security Program as a core competency of Network Technologists. In: Proc. of the 5th Conf. on IT Education. ACM Press, USA (2004) 29-32.
8. Redwine S. (Ed.): Secure Software Assurance: A guide to the Common Body of Knowledge to produce, acquire and sustain secure software, US Dept. of Homeland Security (2006).
9. Slay J., Lock P.: Developing an Undergraduate IT Security Stream: Industry Certification and the Development of Graduate Qualities. In: Miloslavskaya N., et al. (Eds.): Proc. of the 4th World Conf. on Information Security Education (WISE-4). Moscow (2005) 57-66.
10. Smith E., Kritzinger E., Oostuizen H., Von Solms S.: Information Security education: Bridging the gap between academic institutions and industry. In: Miloslavskaya N., et al. (Eds.): Proc. of the 4th World Conf. on InfoSec Education (WISE-4). Moscow (2005) 45-55.
11. von Solms S.: Information Security - A Multidimensional Discipline. Computer & Security Vol. 20, No. 20. Elsevier (2001) 504-508.
12. Wilson M., Hash J.: Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50. USA (2003).
13. Cresson-Wood C.: Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud & Security, Elsevier (2004) 16-17.