Appendix: 19. Justification for course ICS 455

1 Rationale for the course

With the advent of networks and expansion of cyber space, security and trust have become a central concern in computation and in information systems. This course will provide an overview of the crucial concepts and techniques of information assurance in networks and cyber space, indispensable for many career paths leading from the ICS degree. It is the second component of our program update, initiated in response to the new workforce needs, and to the new requirements of the industry, and of the local and national governments in education and in research.

2 Expected course enrollment

25-30

3 Learning objectives

3.1 Program learning objectives

(a) Students can apply the computational and mathematical models relevant for information assurance in cyber space.

(b) Students can analyze the problems of information assurance, and identify and define the computing requirements and cryptographic techniques appropriate to its solution.

(c) Students can design, implement, and evaluate a computer-based system, process, component, or program to meet security requirements of noninterference, confidentiality, or authenticity and integrity.

(d) Students can function effectively on teams to accomplish a common goal.

(e) Students have an understanding of social issues of information assurance.

(f) Students can communicate effectively with a range of audiences concerned with the problems of information assurance in cyber space.

(g) Students can analyze the local and global impact of information technologies and their security repercussions on individuals, organizations, and society.

(h) Students can recognize the need for and an ability to engage in continuing professional and career development in the area of cyber security.

(i) Students can use current techniques, skills, and tools necessary solving the basic problems confidentiality and privacy, or authenticity and integrity.

3.2 Institutional learning objectives

(a) Know: Breadth and Depth of Knowledge. Students will develop their understanding of the world with emphasis on Hawaii, by gaining insight into the critical processes of security and trust, and of their growing importance for networked society, both globally and locally. Together with the prerequisite course ICS 355, and its continuation in ICS 655, this course will make our students more responsive to the current strategic needs of the State of Hawaii, and to the US Government initiatives in cyber security.

(b) Do: Intellectual and Practical Skills. Students will improve their ability to think critically and creatively through analyzing the adversarial processes and designing security structures and trust mechanisms. They will develop their explorative capabilities and literature research skills through individual and group projects. They will increase their literacy and their communication skills by preparing and delivering class presentations, and their numeracy by learning about the quantitative aspects of security models.

(c) Value: Personal and Social Responsibility. Students will demonstrate excellence, integrity, and social engagement through collaborative projects that will facilitate reconciling their cultural, social and individual differences. With the problems of security and trust directly emerging from the conflicts of social and individual interests, this course will directly increase students' awareness and stewardship of their social and natural environment, their sense of ethics, and their intellectual, professional and personal growth within the diverse cultural and natural environment of Hawaii.

4 Syllabus

4.1 Synopsis

Channel security. Trojans and noninterference. Basic concepts of cryptology. Cryptographic primitives. Protocols for authentication and key establishment.

4.2 Student objectives and professional enabling

Security engineer, analyst or designer.

4.3 Background and reading materials

1. Lecture Notes
2. Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security (Prentice Hall 2002, 2nd ed.)
3. Colin Boyd and Anish Mathuria, Protocols for Authentication and Key Establishment (Springer 2003)

4.4 Prerequisites and credits

Prerequisites: 355

Credits: 3

4.5 Lecture topics

1. Introduction: Private communication in a public world
2. Refresher of resource and channel security

3. Overview of cryptographic primitives and cryptanalysis
4. Key establishment
5. Authentication
6. Challenge-Response and Matching Conversation
7. Protocol Derivations
8. Man-in-the-Middle and Impersonation
9. Pervasive security and multi-channel authentication
10. Review

4.6 Examination and coursework

There will be 4 take-home assignments, worth 40% of the grade. The remaining 60% of the grade will be assigned to final examination.

4.7 Related courses

The related courses were given at:

2008-10: Department of Computer Science, University of Oxford

5 Relation of the proposal with the curriculum plans

This course is a part of the ICS curriculum update, intended to enhance our academic excellence in cyber security.

6 Availability of instructors and impact on faculty work load

The newly hired faculty specializing in security (Depeng Li and Dusko Pavlovic) are available to teach the new courses in security. The work load is 3 credit hours.

7 Additional resources required to teach the course

None

8 Possible overlaps

The currently offered security courses at UHM are

- ICS 425 *Computer Security and Ethics* and ICS 426 *Computer System Security*

- EE 406 and EE 609 *Computer and Network Security I and II*.

The proposed course differs from the existing courses in that it approaches security as a strategic concern in *cyber space*, where it is resolved through the processes of *trust*; whereas the existing courses present the traditional problems of *computer* security, and of *network* security. The distinctions between these various aspects are clarified in the introductory lectures.

The three areas of security: *computer* security, *network* security, and *cyber* security with *trust*, are complementary. They open up different career paths, and address different workforce needs. They are all suitable as components of a modern curriculum in Computer Science, and necessary for excellence in cyber security.

9 Academic units for which the course will be a major or degree requirement

ICS: Bachelor of Arts (BA) in Information and Computer Sciences with Focus on Science of Security

10 Consultation with other academic units

There are no prerequisites taught at other academic units. Courses EE 406 and EE 609, taught at Electrical Engineering, present some complementary materials in computer and network security. This was confirmed with Yingfei Dong, who designed and still teaches these courses.