IPSI The Identity, Privacy and Security Initiative

UNIVERSITY OF TORONTO • 40 ST. GEORGE STREET, TORONTO, ON M5S 2E4

UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCES AND ENGINEERING
FACULTY OF INFORMATION

ECE1518 & JIE1001
Seminar in Identity, Privacy and Security

2017 Tentative Course Outline
(Up-dated December 14, 2016)

2017 Theme: 'Establishing Trust in a Cyber Physical Social Systems World'

Instructor: Konstantinos N. (Kostas) Plataniotis
T: 416-946-5605, E: kostas@ece.utoronto.ca, L: Bahen Centre, Rm 4140
W: www.comm.utoronto.ca/~kostas

Teaching Assistant: TBA

Format: Public lecture: 1-1.5 hours, Seminar: 1.5-2 hours, weekly

Lectures:

Thursdays: 12:00 noon – 13:15 pm RS211 (public seminar)
Thursdays: 13:30 pm – 15:00 pm RS211 (regular lecture)

Statement: Cyber-Physical-Social systems (CPSS) tightly link physical, cyber, and social worlds based on real time interactions amongst these worlds. CPSS will change the way we interact with the physical world similarly to the way that the internet has changed the way we interact with each other. CPSS rely on sensing, communication, processing, and actuation/control infrastructures. Their successful deployment and operation requires managing a plethora of physical sensors, utilizing a multitude of processing and communication solutions, and adapting to constantly changing application environments. This area is a new research and development field which necessitates careful examination, research, evaluation, and development of privacy and security methodologies.

The successful development of such meaningful and viable identity, privacy and security measures touches upon a number of diverse disciplines ranging from information and communication technologies, to data science, computing, law and information studies. Moreover, the widespread implementation of identity and security technologies and systems will depend upon a new breed of professionals who are able to design, develop and implement effective but also fair and transparent products, practices, services and policies for the emerging CPSSS paradigm. This course aims to provide an interdisciplinary foundation for the education of such professionals.

Calendar Description: This interdisciplinary course examines issues of identity, privacy and security from a range of technological, policy and scientific perspectives, highlighting the relationships, overlaps, tensions, tradeoffs and synergies between them. Based on a combination of public lectures, in-depth seminar discussions and group project work, it will study contemporary identity, privacy and security systems, practices and controversies, with such focal topics as biometric identification schemes, public key encryption infrastructure, privacy enhancing technologies, identity theft risks and protections, on-line fraud detection and prevention, and computer crime, varying between offerings.

Prerequisites: Students should come with a basic appreciation for the recurring technical, scientific or policy issues in the fields of identity, privacy and security. While students should already have some basic background in one of these areas, it is not expected that they will come with substantial knowledge in them, only the interest to learn. Because this course is jointly offered by Electrical and Computer Engineering (ECE) and the Faculty of Information (FI), students should expect to be exposed to technical and policy approaches to identity, privacy and security topics they will not immediately be familiar with. However, given the deliberate inter-disciplinarity of the course, presentations and materials will be tailored to suit a broad range of backgrounds. There is no formal pre-requisite for this course. If you have concerns about whether you have the necessary preparation for the course, contact an instructor as soon as possible to discuss this.

Teaching approach: The course will be conducted as a combination of public lectures, followed by seminar discussions among registered students, instructors, and guest speakers when present – with student review and commentary on the lectures, assigned readings and recent media news reports. There will be a strong emphasis on exploring issues from a variety of perspectives with others who have varied disciplinary backgrounds. This will require attention to clear expression of experiences, concepts and opinions in conjunction with respectful listening and willingness to engage with alternative viewpoints. Active participation in these discussions, based on prior reading and/or experience is expected. There will be occasions during the course when students will make presentations to classmates and wider audiences, for which they will receive feedback and be graded on. Students will also be expected to submit assignments, submit and defend a project report, and participate in discussions reflecting on the readings and class discussions.

On-line Facilities: The course will make use of the University of Toronto's 'blackboard" web portal. The course will make use of Blackboard (http://portal.utoronto.ca) for important course announcements. *All students must register on Blackboard and check it regularly.* Course notices, handouts and general information will be administered using the course websites (Note: there are two web sites one for ECE1518 and one for JIE1001).

Required Readings: There will be required readings each week. Information will be provided via the blackboard portal.

Evaluation: Grades will be assigned by the instructor for a combination of supervised (S) and unsupervised (U) work conducted individually (I) and collectively within project groups (G) for the following assignments:

ECE1518 & JIE1001: Composition of the Final Mark

• Assignment 1, 15%: Assigned Thursday January 19, 2017; will have two weeks to complete (I).
• Assignment 2, 15%: Assigned February 2, 2017; will have two weeks to complete (I).
• Participation in discussions during public lectures & project presentations: 10% (I).
• Proposal for the end of term project: 5% (should include one page summary overview and description of the data sets to be used): Due on Thursday, February 9, 2017 (G).
• Assignment 3, 15%: Assigned March 2, 2017; will have two weeks to complete (I).
• Project: 40% marked on the basis of a submitted report, simulation results and/or code submitted, and in-class presentation. In class project presentations Thursday, March 30, 2017, Final reports are due on Thursday, April 6, 2017 (G).

Assignments

Assignment	**Deadline**	**Topic**
Assignment 1	February 16, 2017, 17:00 pm	Canadian National Security Green Paper
Assignment 2	March 2, 2017, 17:00 pm	Hand Geometry based Person Identification
Assignment 3	March 16, 2017, 17:00 pm	Surveillance Drones: Privacy Implications

Final Project

A project will be assigned or chosen by Thursday, February 9, 2017. End of term projects could be relevant to the students' graduate work. Students are encouraged to select a topic that will advance their research or their work interests. An end of term report, with no more than 20 pages, in IEEE draft style format, plus code if applicable, is due on Thursday, April 6, 2017, 5:00 pm. Quality should be suitable for a conference presentation. Students are expected to make a presentation on their approach and methodology in addressing the project tasks, during the class meeting on Thursday, March 30, 2017. Interactive discussion and feedback from the class is expected.

Note:

- Students with diverse learning styles and needs are welcome in this course. In particular, if you have a disability/health consideration that may require accommodations, please feel free to approach the instructor and/or Accessibility Services at (416) 978 8060; Web support: (http://accessibility.utoronto.ca).
- Questions regarding marking must be formally written on a piece of paper and submitted along with the associated test/assignment to myself or the cognizant TA. There is a 48-hour limit from the time the test/assignment is first returned in which you may request a recheck.
- Please note that late assignments and projects will be deducted 10% per business day.
- Academic integrity is of utmost important. Any issues of plagiarism and inappropriate collaboration will be taken seriously and reported to the appropriate higher authority.
- The instructor welcomes your comments on the course at any time. Please use the "course tools" section of the web page to provide feedback. Feel free to send comments -- in the past, the instructor has obtained helpful remarks that allow him to make improvements mid-course. IPSI, the ECE Department and the iSchool want to maximize the value of this course for everyone and welcome your input, positive or negative. A formal evaluation of the course will be performed in April (end of term).

Confirmed Guest Speakers for winter 2017:

- Dr. Ann Cavoukian (Ryerson University)
- Prof. Arash Mohammadi (Concordia University)
- Prof. Petros Spachos (University of Guelph)
- Prof. Avi Goldfarb (Rotman School of Management, University of Toronto)
- Prof. Mourad Debbabi (Concordia University)

(Other invitees pending)

Tentative Syllabus of In-Depth Lectures:

- Introduction to Cyber Physical Social Systems (CPSS)
- Cyber Physical Systems (CPS) security and privacy
- CPS and smart grid
- Differential privacy
- Biometrics
- Biometrics and privacy
- CPSS, Internet of Things (IoT), security and privacy
- Federal Initiatives and Regulatory Compliance

Tentative Course plan

January 12: Lecture 1

Introduction to the course

Subject Matter: Cyber physical social systems (CPSS), ICT, Data Science

Seminar Topic: Cyber Physical Social Systems – A tutorial introduction, K.N. Plataniotis, University of Toronto.

January 19: Lecture 2

Subject Matter: Privacy, Policy, Law

Seminar Topic: TBA, Dr. Ann Cavoukian, Privacy and Big Data Institute, RYERSON University.

January 26: Lecture 3

Subject Matter: Biometrics, Privacy, Security

Seminar Topic: Biometrics for Privacy and Security - A tutorial introduction, K.N. Plataniotis, University of Toronto.

February 2: Lecture 4

Subject Matter: Cyber physical systems (CSS), smart grid

Seminar Topic: TBA, Prof. Arash Mohammadi,, Concordia Institute of Information Systems Engineering (CIISE), Concordia University.

February 9: Lecture 5

Subject Matter: Biometrics

Seminar Topic: In depth coverage of biometrics-based recognition, K.N. Plataniotis, University of Toronto.

February 16: Lecture 6

Seminar Topic: TBA

February 23: Lecture 7

Seminar Topic : TBA

March 2: Lecture 8

Seminar Topic : TBA

March 9: Lecture 9

Subject Matter: IoT security, UAV privacy, quality of experience in CPSS

Seminar Topic : TBA, Prof. Petros Spachos, University of Guelph.

March 16: Lecture 10

Subject Matter: Privacy, Economics, Innovation

Seminar Topic: TBA, Prof. Avi Goldfarb, Rotman School of Management, University of Toronto

---

March 23: Lecture 11

Subject Matter: CPSS privacy and security

Seminar Topic: Differential Privacy – A tutorial introduction, K.N. Plataniotis, University of Toronto

---

March 30: Lecture 12

In class project presentations.

April 6: Lecture 13,

Subject Matter: Cyber physical systems security

Seminar: TBA, Prof. Mourad Debbabi, Concordia Institute of Information Systems Engineering (CIISE), Concordia University.

Required Format for Submitting Assignment Reports

Assignment reports be kept short, and be organized in a uniform manner to simplify grading. The following format achieves these objectives.

Page 1. Cover Page. Typed:

- Homework title
- Course number
- Student's name
- Student ID
- Date due
- Date handed in

Page 2. Pertinent discussion. One to three pages (max). This section should include the techniques used and the principal equations (if any) implemented.

Page 3 (or 5). Discussion of results. Two to five pages (max). A discussion of results should include major findings in terms of the project objectives, and make clear reference to any result generated.

Layout. The entire report must be in standard sheet size format (8.5 x 11 inches in the U.S.) The report should be submitted as PDF email attachment, or uploaded through the web portal. The PDF file name should strictly follow the naming convention listed below:

ECE1518_AssignmentNumber-by-STUDENTNAME
Or
JIE1001_AssignmentNumber-by-STUDENTNAME