INSE 6630: Recent Developments in Information Systems Security

1 General Information

- Course name: INSE 6630 Recent Developments in Information Systems Security (4 credits)
- Lecture time & location: Mondays, 17:45–20:15, FG-B040
- Instructor: Mohammad Mannan, Concordia Institute for Information Systems Engineering, ENCS.
- Office: EV6.221 (EV building, 6th floor)
- Email: m.mannan@concordia.ca
- Office hours: Tuesdays from 11:00–12:30
- Course materials: accessible only on Moodle (via MyConcordia.ca)
- Communication: Last minute changes, announcements and useful hyperlinks will be made available on Moodle or via email (must access the email registered at MyConcordia.ca)

2 Course Description

- New types of security and privacy incidents occur in every day. This course discusses recent developments in the area of information systems security. Emphasis is placed on the analysis of recent security and privacy breach incidents from managerial, technical, and ethical perspectives. The goal of this course is to relate the techniques and methodologies learned in previous security courses to real-life security incidents. The course will be given in a seminar style. The instructor will provide some introductory information and a reading list related to some information security topics. Students are expected to read the assigned articles and prepare for in-class discussion. With a focus on the recent developments in information systems security, this course will complement the existing core information systems security courses, namely INSE6110, INSE6120, INSE6130, and INSE6140.
- The following topics will be covered (if time allowed): Security and privacy legislations. New security threats and solution on personal computers, enterprise computers, personal information, confidential information, identity fraud, financial fraud, and social networking. Recent developments in trusted computing for critical cyber infrastructure, privacy-aware information sharing, cybercrime, and cyber forensics techniques. Cyber espionage, cyber terrorism, and cyber war.
- Prerequisites: Any two of INSE 6110, INSE 6120, INSE 6130, INSE 6140.

3 Schedule

The following topics and papers will be covered in class. I may update the topics and their order as we discuss them. Additional related work and security incidents may also be included. You are expected to read the papers ahead of each class, and actively participate in the class discussion.

1. Deception for defense
   “Planning and Integrating Deception into Computer Security Defenses.”
   Almeshekah and Spafford. NSPW 2014.
   “Explicit Authentication Response Considered Harmful.”
   Zhao and Mannan. NSPW 2013.

2. Google Glass
   “PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces.”
   Templeman et al. NDSS 2014.
3. Internet-scale scanning
   “ZMap: Fast Internet-wide Scanning and Its Security Applications.”
4. SSL: Heartbleed
   “The Matter of Heartbleed.”
   Durumeric et al. IMC 2014.
5. Censorship and protocol mimicry attacks
   “The Parrot is Dead: Observing Unobservable Network Communications.”
6. Evil-maid attacks and defenses
   “STARK tamperproof authentication to resist keylogging.”
   Müller et al. FC 2013.
7. Trusted computing for data security
   “Unicorn: Two-Factor Attestation for Data Security.”
   Mannan et al. CCS 2011.
8. Defense against coercion
   “Gracewipe: Secure and Verifiable Deletion under Coercion.”
   Zhao and Mannan. NDSS 2015.
9. Smartphone security
   “Upgrading Your Android, Elevating My Malware: Privilege Escalation through Mobile OS Updating.”
10. Targeted and state-level attacks
    “Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware.”
    Hardy et al. USENIX Security 2014.
    “When Governments Hack Opponents: A Look at Actors and Technology.”
11. Open-source software security
    de Carnavalet and Mannan. ACSAC 2014.

Notes:

- The aforementioned schedule, content and order may be subject to modification by the instructor when judged academically appropriate without prior notice.
- Exact time for the exams, and the project presentations/report submission will be announced in class and via the course Moodle site.

4 Course Materials

All topics will be covered from recent papers. The papers will be posted on the Moodle site.

5 Marks Distribution

1. 40%: Assignments/Projects (may include programming, report writing, presentations, and class participation)
2. 20%: Exam 1
3. 40%: Exam 2
Late Assignments: All assignments/projects will be due in class (unless otherwise specified). Late assignments suffer a penalty rate of 20% per day, up to 5 days (weekends count).

Exam 1 Makeup: There will be NO makeup for Exam 1. In the case of a serious illness or emergency, the weight of Exam 1 will be moved towards the final exam. Be prepared to provide written documentation (e.g., a medical excuse from your doctor) to verify the emergency and its seriousness.

6 Academic Code of Conduct

Any form of cheating, plagiarism, impersonation, falsification of a document as well as any other form of dishonest behaviour by a student is an academic offence under the Academic Code of Conduct and may lead to severe academic penalties up to and including suspension and expulsion. As examples only, you are not permitted to:

- Copy from anywhere without indicating where it came from
- Let another student copy your work and then submit it as his/her own
- Hand in the same assignment in more than one class
- Have unauthorized material or devices in an exam. Note that you do not have to be caught using them just having them is an offence
- Copy from someone else's exam
- Communicate with another student during an exam
- Add or remove pages from an examination booklet or take the booklet out of an exam room
- Acquire exam or assignment answers or questions
- Write an exam for someone else or have someone write an exam for you
- Submit false documents such as medical notes or student records
- Falsify data or research results

For details of the Academic Code of Conduct, see: provost.concordia.ca/academicintegrity/

7 Students’ Responsibilities

1. Students are expected to attend every class. Some material may only be covered in class and not made available on the course website. Students are expected to read the assigned material and to actively participate in class discussions.
2. Students are expected to be respectful of other peoples opinions and to express their own views in a calm and reasonable way. Disruptive behaviour will not be tolerated. Students are expected to be familiar with the Code of Rights and Responsibilities: http://rights.concordia.ca
3. If you cannot attend class for any reason, unforeseen or not, you are to come and talk or write to me as soon as possible.

8 Student Services

1. Concordia Counselling and Development offers career services, psychological services, student learning services, etc. http://cdev.concordia.ca
2. The Concordia Library Citation and Cycle Guides: http://library.concordia.ca/help/howto/citations.html
3. Advocacy and Support Services: http://supportservices.concordia.ca
4. Student Transition Centre: http://stc.concordia.ca
5. New Student Program: http://newstudent.concordia.ca
7. The Academic Integrity Website: http://provost.concordia.ca/academicintegrity/
9 Disclaimer

In the event of extraordinary circumstances beyond the University’s control, the content and/or evaluation scheme in this course is subject to change.