K792 PhD Course
Security, Privacy, and Trust in e-Business
Winter 2020 Course Outline

Information Systems Area
DeGroote School of Business
McMaster University

COURSE OBJECTIVE

This advanced PhD course is designed to discuss security, privacy, and trust issues in e-business. Security, privacy, and trust are critical for the success and survival of electronic commerce. Today new technologies and new applications will not be widely adopted until it can be demonstrated that the security of the underlying ICT infrastructure and the privacy of information being processed are both protected. Only then will users trust and therefore use these innovations and then, and only then, will the developers and society as a whole reap the benefits of the innovation. In this course students will learn the technical, legal, and managerial aspects of security assurance, privacy protection, and trust building through paper reading, seminar presentation and class discussion. Students will also learn how to do research by writing a research paper. MBA students may attend this course with specific permission from the instructor.

INSTRUCTOR AND CONTACT INFORMATION

Dr. Yufei Yuan
Instructor
yuanyuf@mcmaster.ca
Office: DSB A204
Office Hours:
By appointment.
Tel: (905) 525-9140 x23982

Class Location: DSB 227
Mondays 1:30 - 4:30 pm

Course Website: http://avenue.mcmaster.ca

COURSE ELEMENTS

Credit Value:	3	Team skills:	Yes	IT skills:	Yes	Global:	Yes
Avenue:	Yes	Verbal skills:	Yes	Numeracy:	No	Political:	No
Participation:	Yes	Written skills:	Yes	Innovation:	Yes	Social:	No

COURSE DESCRIPTION

This advanced PhD course is designed to discuss issues on security, privacy and trust. Students will learn the technical, legal, and managerial aspects of security, privacy, and trust through paper reading, seminar presentation, and class discussion. Each student will be required to make two seminar presentations and write a research paper on a selected topic. MBA students may attend this course with specific permission from the instructor.

LEARNING OUTCOMES

Upon completion of this course, students will be able to learn the following topics:

- The issues on security, privacy, and trust;
- Risk analysis and security management;
- Security protection technologies;
- Privacy concerns and privacy protection;
- Trust and approaches to improve consumer trust in e-commerce.

REQUIRED COURSE MATERIALS AND READINGS

Lecture notes posted on the course web site

OPTIONAL COURSE MATERIALS AND READINGS

Reference Papers

Security

[S1] Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management,* 51(1), 138-151.

[S2] Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security,* 30(8), 719-731.

[S3] Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly, 43*(2).

[S4] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation,* 2(6-10), 71.

[S5] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security

countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.
[S6] Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203-236.
[S7] Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly*, 71-90.
[S8] Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Res*earch, 20(1), 121-139.
[S9] Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database*, *38*(1), 60-80.
[S10] Soomro, Z.A., Shah, M.H. and Ahmed, J., (2016), Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), pp.215-225.
[S11] Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.
[S12] Venter, H. S., & Eloff, J. H. (2003). A taxonomy for information security technologies. *Computers & Security*, 22(4), 299-307.
[S13] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.
[S14] Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft. *IEEE security & privacy*, 4(2), 30-38.

Privacy

[P1] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
[P2] Head, M. and Yuan, Y. (2001), "Privacy Protection in Electronic Commerce – A Theoretical Framework," *Human Systems Management*, Vol. 20, 2001, pp. 149-160.
[P3] Dinev, T. (2014), "Why would we care about Privacy?" *European Journal of Information systems*, (2014) 23, 97-102.
[P4] Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, 26(4), 639-655.
[P5] Pavlou, P. A. (2011), "State Of The Information Privacy Literature: Where Are We Now And Where Should We Go?" *MIS Quarterly*, December 2011, pp. 977-988.
[P6] Pollach, I. (2007), What's Wrong With Online Privacy Policies? *Communications of the ACM*, September 2007, Vol. 50, No. 9, pp. 103- 108.
[P7] Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4), 989-1016.
[P8] Tang, Z., Hu, Y., & Smith, M. D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems*, 24(4), 153-173.

Trust

[T1] Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 71, 62-77.

[T2] Benbasat, I., Gefen, D., & Pavlou, P. A. (2010). Introduction to the special issue on novel perspectives on trust in information systems. *MIS Quarterly*, 34(2), 367-371.

[T3] Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly*, 373-396.

[T4] Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies*, 58(6), 783-812. [T]Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, 44(2), 544-564.

[T5] Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic commerce research and applications*, *29*, 50-63.

[T6] Li, F., Pieńkowski, D., van Moorsel, A., & Smith, C. (2012). A holistic framework for trust in online transactions. *International Journal of Management Reviews*, 14(1), 85-103.

[T7] McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, 13(3), 334-359.

[T8] Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, 105-136.

[T9] Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys* (CSUR), 45(4), 47.

[T10] Xiao, B., & Benbasat, I. (2011). Product-related deception in e-commerce: a theoretical perspective. *MIS Quarterly*, 35(1), 169-196.

EVALUATION

Learning in this course results primarily from lecturing, reading, in-class discussion, specific topic presentation, and research paper. All work will be evaluated on an individual basis. Your final grade will be calculated as follows:

Components and Weights

Class participation	Class discussion, search and share information	10%
Specific Topic Presentation	Each student will make two one-hour presentation on selected topics	30%
Research paper	Require quality of journal or conference submission	60%
Total		100%

Grade Conversion

At the end of the course your overall percentage grade will be converted to your letter grade in accordance with the following conversion scheme.

LETTER GRADE	PERCENT
A+	90-100
A	85-89
A-	80-84
B+	75-79
B	70-74
B-	65-69
F	0-64

COMMUNICATION AND FEEDBACK

Students that are uncomfortable in directly approaching an instructor regarding a course concern may choose to send a confidential and anonymous email to the respective Area Chair at:

http://www.degroote.mcmaster.ca/curr/emailchairs.aspx

Students who wish to correspond with instructors directly via email must send messages that originate from their official McMaster University email account. This protects the confidentiality and sensitivity of information as well as confirms the identity of the student.

Instructors should conduct an informal course review with students by Week #4 to allow time for modifications in curriculum delivery. Instructors should provide evaluation feedback for at least 10% of the final grade to students prior to Week #8 in the term.

ACADEMIC DISHONESTY

It is the student's responsibility to understand what constitutes academic dishonesty. Please refer to the University Senate Academic Integrity Policy at the following URL:

http://www.mcmaster.ca/univsec/policy/AcademicIntegrity.pdf

This policy describes the responsibilities, procedures, and guidelines for students and faculty should a case of academic dishonesty arise. Academic dishonesty is defined as to knowingly act or fail to act in a way that results or could result in unearned academic credit or advantage. Please refer to the policy for a list of examples. The policy also provides faculty with procedures to follow in cases of academic dishonesty as well as general guidelines for penalties. For further information related to the policy, please refer to the Office of Academic Integrity at:

http://www.mcmaster.ca/academicintegrity

COPYRIGHT

McMaster University has signed a license with the Canadian Copyright Licensing Agency (Access Copyright) which allows professors, students, and staff to make copies allowed under *fair dealing*. Fair dealing with a work does not require the permission of the copyright owner or the payment of royalties as long as the purpose for the material is private study, and that the total amount copied equals **NO MORE THAN 10 percent** of a work or an entire chapter which is less than 20 percent of a work. In other words, it is illegal to: i) copy an entire book, or ii) repeatedly copy smaller sections of a publication that cumulatively cover over 10 percent of the total work's content. Please refer to the following copyright guide for further information:

http://library.mcmaster.ca/about/copying.pdf

MISSED TESTS AND ASSIGNMENTS

The Faculty of Business has approved the following policy:

> When students miss a regularly scheduled mid-term exam for legitimate reasons, as adjudicated by the Academic Programs Office (APO), the weight for that exam will be redistributed across other evaluative components of the course as deemed most appropriate by the instructor.
>
> There is one exception to this "no make-up" rule.
>
> If a student has a documented stress-related or retention-related disability (assessed through the Centre for Student Development) that is in conflict with

mark redistribution, then a make-up exam may be given. In such cases, the test/exam will be administered through the CSD.

When a student cannot write a final exam for documented, legitimate reasons, the student will be granted a deferred exam privilege.

Instructors cannot themselves allow students to unofficially write make-up exams/tests for finals. Adjudication of the request must be handled by the APO.

For any other issues pertaining to missed exams, tests or assignments, please contact the APO.

STUDENTS WITH A DISABILITY

Students with disabilities are required to inform the Centre for Student Development (CSD) of accommodation needs for examinations on or before the last date for withdrawal from a course without failure (please refer to official university sessional dates). Students must forward a copy of such CSD accommodation to the instructor immediately upon receipt. If a disabled student chooses NOT to take advantage of a CSD accommodation and chooses to sit for a regular exam, a petition for relief may not be filed after the examination is complete. The CSD website is:

http://csd.mcmaster.ca

RESEARCH USING HUMAN SUBJECTS

Research involving human participants is premised on a fundamental moral commitment to advancing human welfare, knowledge and understanding. As a research intensive institution, McMaster University shares this commitment in its promotion of responsible research. The fundamental imperative of research involving human participation is respect for human dignity and well-being. To this end, the University endorses the ethical principles cited in the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans:

http://www.pre.ethics.gc.ca/english/policystatement/policystatement.cfm

McMaster University has mandated its Research Ethics Boards to ensure that all research investigations involving human participants are in compliance with the Tri-Council Policy Statement. The University is committed, through its Research Ethics Boards, to assisting the research community in identifying and addressing ethical issues inherent in research, recognizing that all members of the University share a commitment to maintaining the highest possible standards in research involving humans.

If you are conducting original research, it is vital that you behave in an ethical manner. For example, everyone you speak to must be made aware of your reasons for eliciting their responses and consent to providing information. Furthermore, you must ensure everyone understands that

participation is entirely voluntary. Please refer to the following website for more information about McMaster University's research ethics guidelines:

http://www.mcmaster.ca/ors/ethics

Organizations that you are working with are likely to prefer that some information be treated as confidential. Ensure that you clarify the status of all information that you receive from your client. You **MUST** respect this request and cannot present this information in class or communicate it in any form, nor can you discuss it outside your group. Furthermore, you must continue to respect this confidentiality even after the course is over.

CLASS SCHEDULE (SUBJECT TO POSSIBLE MODIFICATION)

Week	Date	Topic	Readings/Assignments
1	Jan. 6	Introduction to security, privacy, and trust issues	Choo (2011), Acquisti et al. (2015), Von Solms & Van Niekerk (2013).
2	Jan. 13	Risk analysis and security management	Siponen & Oinas-Kukkonen (2007), Straub & Welke (1998), Baskerville, et al. (2014).
3	Jan. 20	Information security technologies Blockchain and biometrics	Venter & Eloff (2003), Crosby, et al. (2016)
4	Jan. 27	Security behaviour studies	D'Arcy et al. (2009), Guo et al. (2011), Liang & Xue (2009).
5	Feb. 3	Specific topics on security	Student presentation
6	Feb. 10	Privacy basics	Head & Yuan (2001), Smith, et al. (2011), Dinev (2014)
7	Feb 17-21	Spring break	No class
8	Feb. 24	Privacy research	Pavlou (2011), Tang, et al. (2008), Dinev, et al. (2015).
9	Mar. 2	Specific topics on privacy	Student presentation
10	Mar. 9	Trust basics	McKnight, et al. (2002), Grabner-Kräuter & Kaluscha (2003), Dimoka (2010).
11	Mar. 16	Trust research	Pavlou, et al. (2007),

			Xiao & Benbasat (2011), Bansal & Zahedi (2015)
12	Mar. 23	Specific topics on trust	Student presentation
13	Mar. 30	Research paper presentation	Research paper due

Specific Topic Presentation Guidelines

Objective: To make a seminar presentation that addresses a current issue on security, privacy and trust in electronic business. The presentations are mainly based on literature review. Each student will be required to make two presentations (one hour each) on two different fields.

Topic Selection: Following are the schedule of student presentation. Each topic will be presented by up to three students. Each student can select two topics from the list. You may select a subtopic based on the recommendation or your own interests. Please make sure your subtopics are not overlap with each other.

Presentation Schedule

Week		**Topic**	**Sub Topics**
5	Feb. 3	Specific topics on security	• Cyber security • Intrusion and fraud detection • Identity issues with AI technology • Effectiveness of security measures • Security breach • Blockchain
9	Mar. 2	Specific topics on privacy protection	• Privacy protection in healthcare • Privacy protection in social media • Privacy issues with AI technology • Privacy issues in big data and cloud computing • Privacy paradox
12	Mar. 23	Specific topics on trust	• Trust building in e-business • Trust repair • Trust in social media • Trust towards AI enabled service • The relationship between security, privacy and trust

Presentation and paper sharing: For each subtopic, please prepare a PowerPoint presentation and provide a copy of most valuable papers (three to four) and a list of references for students to share.

Research Paper Guidelines

Objective:

To write a research paper that addresses a current issue on security, privacy and trust in electronic business. The topic of your research paper can overlap with your seminar presentation but should be more in depth study. Students are expected to work more closely with the instructor for possible conference or journal publication.

Topic Selection:

The topic of your research paper may be on any contemporary issue relating to security, privacy, and identity theft in electronic business. A one page proposal of your research topic must be handed in by the third week. You may build a theoretical framework or evaluate existing technologies. Your topic should not cover too broad a field, since your report will not be long enough to do justice to the material and will result in a poor mark. For example, "Network Security" is too broad as a topic, while "Hackers on Internet" is considerably narrower, and "Intrusion detection techniques" has an even sharper focus.

Guidelines:

1. Since many students will not have much experience within their selected topic, most of the material for the research paper will be gathered from literature surveys. The University library has many books and journals which may be of use, and your instructor may also help you in your search if you are short of material. Your best sources of information will likely be the World Wide Web and the electronic libraries available in the Innis Room. **Do not** consult your instructor until you have looked at topics from this source. Books are good sources of material, but to obtain up-to-date material, journals should also be consulted.

2. Since the purpose of this research paper is to show that you have studied a particular topic area well, do not simply repeat information you find in your literature review. In particular, beware of the unbridled enthusiasm on many topics often appearing in the popular press. This may be a mask to cover a lack of facts. You should not consider yourself as a reporter, but as an analyst. Present your own views on the material gathered, since this develops your ability to think logically and creatively. Remember, marks are given for originality.

3. Your report must be typed. It should be a minimum of 20 (maximum of 35) double spaced 8 x 11 typewritten pages, (not including references, figures, and appendices). However, you will not be penalized if you can put forward a good presentation in less than 20 pages.

4. Your report should be written in a concise, crisp, business-like style such as would be used in writing a report for high level management. Try to use diagrams and tables to get your point of view across and to "dress up" your report's appearance.

5. Your report should include the following sections:

    - A cover page which includes the title, the course name and number, the date, and the author’s' name.

    - Abstract: The abstract should cover the most important points presented in your paper as well as any conclusions that should be derived from the report.

- Introduction: This section includes background material to bring the reader "up to speed" before launching into the main thrust of your report. It should also briefly discuss a general outline of the report which follows.

- Report body: The body of the report should be broken into reasonably sized sections on various aspects of the topic under consideration. Each section should be numbered and given an appropriate heading.

- Major findings and conclusions: This section should reflect the important results that the reader should have learned from the paper.

- References: You must show several references from more advanced literature (you may also reference the popular press, but it may tend towards uncritical enthusiasm). Guidelines for reference format are provided below.

- Appendices: If appropriate, appendices should be included after your reference section.

6. Jargon should not be used unless the words are carefully defined when they are first used in your report. In general, make sure you carefully define your topic, assuming that potential readers may have little or no background knowledge within the area.

7. References to gender should not appear in the paper, unless referring to an actual person. A minimal use of "he or she" is permitted instead of "he" or "she", but it is normally possible to eliminate such references entirely. For example, consider the following sentence: "The manager will normally rely on his secretary to perform her work as rapidly as possible, regardless of whether or not she has access to a word processor". A statement like this one will cost you marks in your paper, so consider the following statement as a replacement: "Managers will normally rely on their secretaries to work as rapidly as possible, regardless of whether they have access to word processors". There are other ways to achieve this effect, but this should demonstrate what is desired.

8. Sources for your material must be referenced. If you develop original material in your report, be sure to substantiate the grounds upon which you build your arguments, through references to other published material or personal communications. All of your reference material should be referred to by numbers in square brackets, corresponding to numbers used in your reference list at the end of your paper. In your reference section, references should be listed in alphabetic order of the first author's last name. An example of proper reference format is shown below:

   Cofta, P. (2007), *Trust, Complexity and Control: Confidence in a Convergent World*, Wiley &Sons, 2007.

   Pollach, I. (2007), What's Wrong with Online Privacy Policies? *Communications of the ACM*, September 2007, Vol. 50, No. 9, pp. 103- 108.

9. Short footnotes may be used, provided that they are referenced on the same page with a special symbol such as a dagger or an asterisk. Longer footnotes should be included as appendices, to avoid breaking the continuity of the presentation.

10. Figures or tables should be numbered and should appear as soon as possible after they are referenced in the paper. However, if a large number of tables or figures are referenced in one place, it is best to move all the tables and/or figures to the end of the report.

11. Appendices should have titles and be numbered using Roman numerals.

12. All pages of the report, except the title page, should be numbered.

13. Equations should be numbered if they are referred to elsewhere in the report.

14. Grammar, spelling, sentence and paragraph structure are important. A good general reference which may be useful is the Harbrace College Handbook published by Longman Canada Limited. Other references which contain helpful sections on business report writing style are:

    - Ewing, E.W. (1979), Writing For Results, New York: Wiley, 1979.
    - Himstreet, W.C., and W.M. Baty (1977) Business Communications, Belmont, California : Wadsworth, 1977.
    - Smith, R.S. (1976), Written Communications For Data Processing, New York: Van Nostrand, 1976.
    - Weiss, A. (1977), Write What You Mean, New York: Amacom, 1977.

15. PowerPoint presentation. You should prepare and submit (email me) your PowerPoint presentation document one day before the scheduled presentation time. You will have 25 minutes presentation followed by 10 minutes discussion.