	Course	CS 7301.012 **- Cyber-Physical Systems Security and Privacy**
	Professor	Alvaro A. Cardenas
	Term	Fall 2014
	Meetings	F, 2:30-5:15pm

Professor's Contact Information

Office Phone	972-883-4537
Office Location	ECSS 3.705
Email Address	alvaro.cardenas@utdallas.edu
Office Hours	M 1:30-3:30pm (or by appointment)

General Course Information

Pre-requisites, Co-requisites, & other restrictions	No pre-requisites
Course Description	The Stuxnet attack was a wake-up call to improve the security of our critical infrastructures, which include the smart grid, transportation networks, water distribution, and other cyber-physical systems, where computation, communications, and control are tightly integrated. This class covers the security of cyber-physical systems from a multi-disciplinary point of view, from computer science security research (network security and software security), to public-policy (e.g., the Executive Order 13636), risk-assessment, business drivers, and control-theoretic methods to reduce the cyber-risk to cyber-physical critical infrastructures.
Course Project	There will be a class project (teams of two students) to encourage independent research in any topic of interest related to security for critical infrastructures. Ties with student's current research interests are encouraged. Suggestions on project topics, research ideas and relevant literature will be provided after the first few weeks of the semester.
Learning Outcomes	The students will learn the most pressing challenges for protecting critical infrastructures and will present solutions to an identified problem. At the end of the class the students should be familiar with the best practices for securing the smart grid, SCADA systems and other control systems.
Grading (credit) Criteria	60% Course Project 30% Student Presentations 10% Class Participation
Exams	No Exams

Tentative Schedule

- **Basic Introduction to Information Security and Privacy**
  - Integrity, Authentication, Access Control
  - Cryptography
  - Network Security
  - Software Security
  - Privacy
  - Secure Architectures (Separation of Duty, Fault Tolerance)

- **Introduction to Cyber-Physical Systems (CPS)**
  - Embedded Devices and Internet of Things
  - Communication Technologies in CPS
    - Wireless Sensor Network Communication Standards
  - Control Theory
  - Examples of CPS:
    - Smart Grids
    - Intelligent Transportation Systems
    - Industrial Control Systems
    - Embedded Medical Devices

- **Security for Cyber-Physical Systems**
  - Attacks
    - Physical Terrorist Attacks
    - Cyber-Attacks Against CPS
  - Risk Assessment
    - APT
    - Shodan
  - Defenses
    - Investing in Security and Policy Issues
    - Security Mechanisms
      - Device Security
        - Attestation
      - Network Security
        - Anomaly Detection
      - Situational Awareness
    - Resilient Control Architectures and Algorithms
    - Specific Security Issues in Different CPS Domains

  - Privacy

Required Reading

Introduction to Information Security
Cyber Security: Basic Defenses and Attack Trends Alvaro A. Cárdenas, Tanya Roosta, Gelareh Taban, Shankar Sastry. Homeland Security Technology Challenges. July, 2008.

Introduction to Cyber-Physical Systems
Cyber-Physical Systems: A Perspective at the Centennial. Kyoung-Dae Kim and P.R. Kumar. Proceedings of the IEEE, May 2012.

Problems for Securing Control Systems
Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs. Pietre-Cambacedes, Trischler, Ericsson. IEEE Transactions on Power Delivery, Vol 26, No. 1, January 2011.

Incentives for Protecting Critical Infrastructures
Security economics and critical national infrastructure. Anderson, R., & Fuloria, S. In Economics of Information Security and Privacy (pp. 55-66). Springer US. 2010.

Stuxnet
Stuxnet: Dissecting a Cyberwarfare Weapon. R. Langner. IEEE Security & Privacy. 2011.

Cyber Conflict
Cyberwar Thresholds and Effects. James A. Lewis. IEEE Security and Privacy Magazine, 2011.

Critical Infrastructures and APT
Securing Critical Infrastructures from Targeted Attacks. Marc Dacier, Frank Kargl, Alfonso Valdes. Report from Dagstuhl Seminar 12505. 2012

Smart Grid Security
Security and Privacy in the Smart Grid Alvaro A. Cárdenas, Reihaneh Safavi-Naini
In Sajal K. Das, Krishna Kant, and Nan Zhang Eds. Handbook on Securing Cyber-Physical Infrastructures: Foundations and Challenges. Morgan Kaufmann, 2012.

Privacy
SoK: Privacy Technologies for Smart Grids- A Survey of Options. Marek Jawurek, Florian Kerschbaum and George Danezis. White Paper, 2013.

Resilient Control
Attacks against process control systems: risk assessment, detection, and response. AA Cárdenas, S Amin, ZS Lin, YL Huang, CY Huang, S Sastry. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (AsiaCCS) 2011.

Experimental Tools and Resources

Shodan
http://www.shodanhq.com

Quantitatively Assessing and Visualizing Industrial System Attack Surfaces Eireann P. Leverett. Master Thesis, University of Cambridge 2011.

Industrial Risk Assessment Map http://www.scadacs.org/projects.html

Power Grid Simulation
GridLAB-D http://www.gridlabd.org

Electricity Consumption Traces
Green Button Data http://www.greenbuttondata.org/greendevelop.aspx

Computer Networks and Intelligent Transportation Co-Simulation
Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. C. Sommer, R. German and F. Dressler. IEEE Transactions on Mobile Computing, vol. 10 (1), pp 3-15, January 2011

OMNeT++ and SUMO http://veins.car2x.org
Ns-2 and SUMO http://lca.epfl.ch/projects/trans/

Car Testbed
OCTANE (Open Car Testbed and Network Experiments): Bringing Cyber-Physical Security Research to Researchers and Students.

https://www.usenix.org/conference/cset13/octane-open-car-testbed-and-network-experiments-bringing-cyber-physical-security

AMICI
I haven't figured out what this tool is yet, but it may be worth checking out. http://sourceforge.net/projects/amici/?source=navbar

Survey of Models and Software Tools
Methodologies and Applications for Critical Infrastructure Protection: State of the Art. J. Yusta, G. Correa, R. Lacal-Arántegui. Energy Policy 39. 2011.

Critical infrastructure interdependency modeling: a survey of US and international research. Pederson, Peter, et al. Idaho National Laboratory (2006): 1-20.

Further (Suggested) Reading

Internet of Things and Networks for Embedded Devices (Modernizing Critical Infrastructures)

The Role of the RPL Routing Protocol for Smart Grid Communications. Emilio Ancillotti, Raffaele Bruno, and Marco Conti. IEEE Communications Magazine, January 2013

End-to-End Security for Sleepy Smart Object Networks. Mohit Sethi, Jari Arkko, Ari Keranen. IEEE International Workshop on Practical Issues in Building Sensor Network Applications 2012.

CoAP: An Application Protocol for Billions of Tiny Internet Nodes C. Bormann, Castellani, Shelby. IEEE Internet Computing Volue 16, Issue 2, March-April 2012.

Stuxnet (and Maroochy and Aurora)

Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier. February 2011.

The Cousins of Stuxnet: Duqu, Flame and Gauss. Boldizsar Bencsath, Gabor Pek, Levente Buttyan, and Mark Felegyhazi. Future Internet 2012.

Basic Attack Strategy of Stuxnet 0.5. Report by the Instintute for Science and International Security (ISIS). Februrary, 2013.

Lessons learned from the Maroochy water breach. Slay, Jill, and Michael Miller. CIP Conference. Springer US, 2007.

Myth or Reality--Does the Aurora Vulnerability Pose a Risk to my Generator? M. Zeller. IEEE 64th Annual Conference for Protective Relay Engineers, 2011.

Cybersecurity and Critical Infrastructures

CYBERSECURITY Continued Attention Needed to Protect Our Nation's Critical Infrastructure. Government Accountability Office, July 26, 2011.

Offensive Cyber Weapons: Construction, Development, and Employment. Dale Peterson. The Journal of Strategic Studies, 2013.

Smart Grid Security

Towards modeling the impact of cyber attacks on a smart grid. Kundur, Deepa, et al. International Journal of Security and Networks 6.1 (2011): 2-13.

Cyber-Physical Security of a Smart Grid Infrastructure. Mo, Kim, Brancik, Dickinson, Lee, Perrig, Sinopoli. Proceedings of the IEEE, Special Issue on Cyber-Physical Systems. 2012.

Impact of Integrity Attacks on Real-Time Pricing in Smart Grids. R. Tan, V.B. Krishna, D. Yau, Z. Kallbarczyk. In Proceedings of the 2013 ACM Conference on Computer and Communications Security (CCS) 2013.

Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems. I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller and M. Gruteser. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS) 2012.

Electricity for Free? The Dirty Underbelly of SCADA and Smart Meters. J. Pollet. Red Tiger Security White Paper. July 2010.

AMI Penetration Test Plan. J. Searle, G. Rasche, A. Wright, S. Dinnage. NESCOR White Paper. 2013.

Application of Sensor Network for Secure Electric Energy Infrastructure. Leon, Vittal, Manimaran. IEEE Transactions on Power Delivery. Voll 22, No. 2, April 2007

Smart-Grid Security Issues. Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah Frinckie. IEEE Security and Privacy Magazine, 2010.

Ranking Contingency Resulting from Terrorism by Utilization of Bayesian Networks, Tranchita, C.; Hadjsaid, N.; Torres, A., Electrotechnical Conference, 2006. MELECON 2006. IEEE Mediterranean, vol., no., pp.964,967, 16-19 May 2006

Privacy

Minimizing Private Data Disclosures in the Smart Grid. Weining Yang, Ninghui Li, Yuan Qi, Wahbeh Qardaji, Stephen McLaughlin and Patrick McDaniel. 19th ACM Conference on Computer and Communications Security (CCS). Raleigh, NC, USA. October 2012.

Protecting Consumer Privacy from Electric Load Monitoring. Stephen McLaughlin, Patrick McDaniel, and William Aiello. 18th ACM Conference on Computer and Communications Security (CCS), Chicago IL, USA. October 2011.

Virtual trip lines for distributed privacy-preserving traffic monitoring. Hoh, Baik, et al. Proceedings of the 6th international conference on Mobile systems, applications, and services. ACM, 2008.

Healthcare and Medical Devices

Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. M. Rostami, A. Juels, F. Koushanfar. Proc. ACM Computer and Communications Security Conference (CCS) 2013.

They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices. S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu. Proc. ACM Conf. SIGCOMM 2011.

Cyberconflict (Cyber-Activism, Espionage, Terrorism, and War)

Cyber War Will Not Take Place. Thomas Rid. Journal of Strategic Studies. Vol 35 no 1, 5-32. February 2011.

Cyber War is Inevitable (Unless We Build Security In). Gary McGraw. Journal of Strategic Studies. Vol 36 no 1, 109-119. 2013.

Cyber Conflict as an Emergent Social Phenomenon, Denning, D. E. Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (T. Hold and B. Schell eds.), IGI Global, 2011.

Stuxnet: What has Changed? Denning, D.E. Future Internet 2012.

APT1. Exposing One of China's Cyber Espionage Units. Mandiant Report. 2013.

International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. Michael N. Schmitt. Harvard International Law Journal, Dec. 2012.

[BOOK] We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Parmy Olson, June 2012.

Terrorist Attacks Against Critical Infrastructures

Diagnostic Tools to Estimate Consequences of Terrorism Attacks Against Critical Infrastructure. Rae Zimmerman, Carlos Restrepo, Nicole Dooskin, Jeremy Fraissinet, Ray Hartwell, Justin Miller, Wendy Remington. Proc. DHS security conference, Working Together: Research and Development Partnerships in Homeland Security. 2005.

Security Assistance. Efforts to Secure Colombia's Caño Limón-Coveñas Oil Pipeline Have Reduced Attacks, but Challenges Remain. Government Accountability Office. September 2005.

National Contingency Plan Against Oil Spills in Colombia, A Successful Preventive Environmental Instrument in Latin America. L.A. Leal-Castellanos. Interspill 2004.

Events Classification and Operation States Considering Terrorism in Security Analysis. A. Torres and C. Tranchita. IEEE PES Power Systems Conference and Explosition, 2004.

Risk Assessment for Power System Security with Regard to Intentional Events. C. Tranchita. Thesis L'Institut Polytechnique de Grenoble. 2008.

Water and Terrorism. P. Gleick. Water Policy 8. 2006.

Trusted Computing and Attestation for Embedded Devices

A Security Framework for Analysis and Design of Software Attestation. Proc ACM Computer and Communications Security (CCS) Conference 2013.

Cumulative Attestation Kernels for Embedded Systems. LeMay and Gunter. IEEE Transactions on Smart Grid. Vol 3, Iusse 2. 2012.

Mechanisms to Provide Integrity in SCADA and PCS Devices. A. Shah, A. Perrig, B. Sinopoli. International Workshop on Cyber-Physical Systems-Challenges and Applications. 2008.

Refutation of On the Difficulty of Software-Based Attestation of Embedded Devices. A. Perrig, L.V. Doorn. Based on the Paper of Castelluccia C. Francillon A (2010).

OMAP: One-way Memory Attestation Protocol for Smart Meters K. Song, D. Seo, H. Park, H. Lee, A. Perrig. 9th IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops. 2011.

SCADA and Control System Security: New Standards Protecting Old Technology. S. Howard. ISSE 2010 Securing Electronic Business Processes.

TNC IF-MAP Metadata for ICS Security. Trusted Computing Group. October 2012.

Transportation Security

Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond. Sampigethaya, Krishna, et al. Proceedings of the IEEE. 2011.

Security of ADS-B: State of the Art and Beyond. M. Strohmeier, V. Lenders, I. Martinovic. arXiv preprint arXiv:1307.3664 (2013).

Experimental Analysis of Attacks on Next Generation Air Traffic Communication. Matthias Schaefer, Vincent Lenders, and Ivan Martinovic. ACNS 2013.

On the requirements for successful GPS spoofing attacks. Tippenhauer, Nils Ole, et al. Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011.

Comprehensive Experimental Analyses of Automotive Attack Surfaces. Checkoway, Stephen, et al. USENIX Security Symposium. 2011.

Cyber-Security for the Controller Area Network (CAN) Communication Protocol. C-W. Lin, and A. Sangiovanni-Vincentelli. Science Journal 1, no. 2 (2012): 80-92.

Business Case for Securing Critical Infrastructures

Security Metrics and Security Investment. Bohme, Moore. Lecture Notes.

Bound to Fail: Why Cyber Security Risk Cannot Simply be "Managed" Away. Langner, Pederson. White Paper, Center for 21st Centurty Security and Intelligence. 2012.

The RIPE Framework. A Process-Driven Approach Towards Effective and Sustainable Industrial Control System Security. R. Langner, White Paper. Sept 2013.

Securing Wastewater Facilities from Accidental and Intentional Harm: A Cost-Benefit Analysis. S. Papa, W. Casper, T. Moore. International Journal of Critical Infrastructure Protection 6 (2013).

Investment Planning for Electric Power Systems Under Terrorist Threat. N. Romero, N. Xu, L. Nozick, I. Dobson. IEEE Transactions on Power Systems, Vol 27, No. 1. February 2012.

SCADA Security

[BOOK] Robust Control System Networks: How to Achieve Reliable Control After Stuxnet. R. Langner. Momentum Press, 2012.

A Taxonomy of Security Solutions for the SCADA Sector. Fovino, Coletta and Masera. ESCoRTS White Paper. March 2010.

A cyber-physical experimentation environment for the security analysis of networked industrial control systems. Bela Genge, Christos Siaterlis, Igor Nai Fovino, Marcelo Masera. Computers & Electrical Engineering. 2012

SABOT: Specification-based Payload Generation for Programmable Logic Controllers. Stephen McLaughlin and Patrick McDaniel. 19th ACM Conference on Computer and Communications Security (CCS). Raleigh, NC, USA. October 2012.

Difficulties in Modeling SCADA Traffic: A Comparative Analysis. Barbosa, Sadre, and Pras. PAM 2012.

Distributed Intrusion Detection System for SCADA Protocols. Fovino, Masera, Guglielmi, Carcano, Trombetta. Critical Infrastructure Protection IV. 2010.

Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems Genge, Siaterlis, Hohenadel. Int J. Comput. Comm. Vol 7 Nov. 4. November 2012.

A log mining approach for process monitoring in SCADA Hadziosmanovic, Bolzoni, Hartel. International Journal of Informaiton Security. April 2012.

Guide to Industrial Control Systems (ICS) Security. K. Stouffer, J. Falco, K. Scarfone. NIST SP 800-82. September 2008.

Industrial Control Systems Security: What is Happening?. M. Krotofil, D. Gollmann. IEEE 11th International Conference on Industrial Informatics. July 2013.

Process Safety

Highlights from the Literature on Accident Causation and System Safety: Review of Major Ideas, Recent Contributions, and Challenges. Saleh, Marais, Bakolas, Cowlagi. Reliability Engineering and System Safety 95, 2010.

Coordinability and Consistency in Accident Causation and Prevention: Formal System Theoretic Concepts for Safety in Multilevel Systems. Cowlagi, Saleh. Risk Analysis. Vol 22, No. 3, 2013.

Hazard and Operability (HAZOP) Analysis. A Literature Review. J. Dunjo, V. Fthenakis, J. Vilchez, J. Arnaldos. Journal of Hazardous Materials. Vol 173, Issues 1-3, January 2010.

Electricity Theft

Identification of Energy Theft and Tampered Meters Using a Central Observer Meter: A Mathematical Approach. Bandim, Alves, Pinto, Souza, Loureiro, Magalhaes, Galvez Durand. IEEE 2003.

Evaluating Electricity Theft Detectors in Smart Grid Networks. Daisuke Mashima and Alvaro Cardenas. Research in Attacks, Intrusions, and Defenses (RAID) 2012.

Situational Awareness

Situational Awareness and Safety. N.A. Stanton, P.R.G. Chambers, J. Piggott. Safety Science 39 2001.

INL Control System Situational Awareness Technology Final Report. Gordon Rueff, Bryce Wheeler, Todd Vollmer, and Tim McJunkin. January 2013.

Estimation and Control Theory

False Data Injection Attacks against State Estimation in Electric Power Grids. Yao Liu, Peng Ning, Michael Reiter. ACM TISSEC 2011.

False Data Injection Attacks in Control Systems. Mo and Sinopoli. First Workshop on Secure Control Systems. CPS Week, 2010.

Secure Control Systems: A Control -Theoretic Approach to Cyber-Physical Security. F. Pasqualetti Ph.D. Dissertation. 2012

Quantifying Cyber-Security for Networked Control Systems. Teixeira, André, Kin Cheong Sou, Henrik Sandberg, and Karl H. Johansson. In Control of Cyber-Physical Systems, pp. 123-142. Springer International Publishing, 2013.

Consensus of multi-agent networks in the presence of adversaries using only local information. LeBlanc, Heath J., et al. Proceedings of the 1st international conference on High Confidence Networked Systems. ACM, 2012.

Minimax control for cyber-physical systems under network packet scheduling attacks. Shoukry, Yasser, Jose Araujo, Paulo Tabuada, Mani Srivastava, and Karl H. Johansson. " In Proceedings of the 2nd ACM international conference on High confidence networked systems, pp. 93-100. ACM, 2013.

Revealing stealthy attacks in control systems. Teixeira, André, Iman Shames, Henrik Sandberg, and Karl H. Johansson. In Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on, pp. 1806-1813. IEEE, 2012.

Analytical Analysis of Cyber Attacks on Unmanned Aerial Systems. Kwon, Cheolhyeon, and Inseok Hwang. AIAA Guidance, Navigation, and Control Conference (2013).

Pipeline Security

Keeping America's Pipelines Safe and Secure. Key issues for Congress. P. Parfomak. Congressional Research Service. January, 2013.

Security Assistance. Efforts to Secure Colombia's Caño Limón-Coveñas Oil Pipeline Have Reduced Attacks, but Challenges Remain. Government Accountability Office. September 2005.

National Contingency Plan Against Oil Spills in Colombia, A Successful Preventive Environmental Instrument in Latin America. L.A. Leal-Castellanos. Interspill 2004.

Interdependencies and Cascading Failures

Catastrophic Cascade of Failures in Interdependent Networks. S. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, and S. Havlin. Nature, Vol 464, April 2010.

Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. S. Rinaldi, J. Peerenboom, and T. Kelly. IEEE Control Systems Magazine, Dec. 2001.

Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction. Rae Zimmerman, Carlos Restrepo. IEEE Conference on Technologies for Homeland Security, 2009.

Modeling Cascading Failures in the North American Power Grid. Kinney, Crucitti, Albert, and Latora.The European Physical Journal B 46, 2005.

Cascade-based Attack Vulnerability on the US Power Grid. Wang and Rong. Safety Science 47, 2009.

Student Conduct and Discipline	The University of Texas System and The University of Texas at Dallas have rules and regulations for the orderly and efficient conduct of their business. It is the responsibility of each student and each student organization to be knowledgeable about the rules and regulations which govern student conduct and activities. General information on student conduct and discipline is contained in the UTD publication, *A to Z Guide*, which is provided to all registered students each academic year. The University of Texas at Dallas administers student discipline within the procedures of recognized and established due process. Procedures are defined and described in the *Rules and Regulations, Board of Regents, The University of Texas System, Part 1, Chapter VI, Section 3*, and in Title V, Rules on Student Services and Activities of the university's *Handbook of Operating Procedures*. Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations (SU 1.602, 972/883-6391). A student at the university neither loses the rights nor escapes the responsibilities of citizenship. He or she is expected to obey federal, state, and local laws as well as the Regents' Rules, university regulations, and administrative rules. Students are subject to discipline for violating the standards of conduct whether such conduct takes place on or off campus, or whether civil or criminal penalties are also imposed for such conduct.
Academic Integrity	The faculty expects from its students a high level of responsibility and academic honesty. Because the value of an academic degree depends upon the absolute integrity of the work done by the student for that degree, it is imperative that a student demonstrate a high standard of individual honor in his or her scholastic work. Scholastic dishonesty includes, but is not limited to, statements, acts or omissions related to applications for enrollment or the award of a degree, and/or the submission as one's own work or material that is not one's own. As a general rule, scholastic dishonesty involves one of the following acts: cheating, plagiarism, collusion and/or falsifying academic records. Students suspected of academic dishonesty are subject to disciplinary proceedings. Plagiarism, especially from the web, from portions of papers for other classes, and from any other source is unacceptable and will be dealt with under the university's policy on plagiarism (see general catalog for details). This course will use the resources of turnitin.com, which searches the web for possible plagiarism and is over 90% effective.
Email Use	The University of Texas at Dallas recognizes the value and efficiency of communication between faculty/staff and students through electronic mail. At the same time, email raises some issues concerning security and the identity of each individual in an email exchange. The university encourages all official student email correspondence be sent only to a student's U.T. Dallas email address and that faculty and staff consider email from students official only if it originates from a UTD student account. This allows the university to maintain a high degree of confidence in the identity of all individual corresponding and the security of the transmitted information. UTD furnishes each student with a free email account that is to be used in all communication with university personnel. The Department of Information Resources at U.T. Dallas provides a method for students to have their U.T. Dallas mail forwarded to other accounts.

Withdrawal from Class	The administration of this institution has set deadlines for withdrawal of any college-level courses. These dates and times are published in that semester's course catalog. Administration procedures must be followed. It is the student's responsibility to handle withdrawal requirements from any class. In other words, I cannot drop or withdraw any student. You must do the proper paperwork to ensure that you will not receive a final grade of "F" in a course if you choose not to attend the class once you are enrolled.
Student Grievance Procedures	Procedures for student grievances are found in Title V, Rules on Student Services and Activities, of the university's *Handbook of Operating Procedures*. In attempting to resolve any student grievance regarding grades, evaluations, or other fulfillments of academic responsibility, it is the obligation of the student first to make a serious effort to resolve the matter with the instructor, supervisor, administrator, or committee with whom the grievance originates (hereafter called "the respondent"). Individual faculty members retain primary responsibility for assigning grades and evaluations. If the matter cannot be resolved at that level, the grievance must be submitted in writing to the respondent with a copy of the respondent's School Dean. If the matter is not resolved by the written response provided by the respondent, the student may submit a written appeal to the School Dean. If the grievance is not resolved by the School Dean's decision, the student may make a written appeal to the Dean of Graduate or Undergraduate Education, and the deal will appoint and convene an Academic Appeals Panel. The decision of the Academic Appeals Panel is final. The results of the academic appeals process will be distributed to all involved parties. Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations.
Incomplete Grades	As per university policy, incomplete grades will be granted only for work unavoidably missed at the semester's end and only if 70% of the course work has been completed. An incomplete grade must be resolved within eight (8) weeks from the first day of the subsequent long semester. If the required work to complete the course and to remove the incomplete grade is not submitted by the specified deadline, the incomplete grade is changed automatically to a grade of **F**.

Disability Services	The goal of Disability Services is to provide students with disabilities educational opportunities equal to those of their non-disabled peers. Disability Services is located in room 1.610 in the Student Union. Office hours are Monday and Thursday, 8:30 a.m. to 6:30 p.m.; Tuesday and Wednesday, 8:30 a.m. to 7:30 p.m.; and Friday, 8:30 a.m. to 5:30 p.m. The contact information for the Office of Disability Services is: The University of Texas at Dallas, SU 22 PO Box 830688 Richardson, Texas 75083-0688 (972) 883-2098 (voice or TTY) Essentially, the law requires that colleges and universities make those reasonable adjustments necessary to eliminate discrimination on the basis of disability. For example, it may be necessary to remove classroom prohibitions against tape recorders or animals (in the case of dog guides) for students who are blind. Occasionally an assignment requirement may be substituted (for example, a research paper versus an oral presentation for a student who is hearing impaired). Classes enrolled students with mobility impairments may have to be rescheduled in accessible facilities. The college or university may need to provide special services such as registration, note-taking, or mobility assistance. It is the student's responsibility to notify his or her professors of the need for such an accommodation. Disability Services provides students with letters to present to faculty members to verify that the student has a disability and needs accommodations. Individuals requiring special accommodation should contact the professor after class or during office hours.
Religious Holy Days	The University of Texas at Dallas will excuse a student from class or other required activities for the travel to and observance of a religious holy day for a religion whose places of worship are exempt from property tax under Section 11.20, Tax Code, Texas Code Annotated. The student is encouraged to notify the instructor or activity sponsor as soon as possible regarding the absence, preferably in advance of the assignment. The student, so excused, will be allowed to take the exam or complete the assignment within a reasonable time after the absence: a period equal to the length of the absence, up to a maximum of one week. A student who notifies the instructor and completes any missed exam or assignment may not be penalized for the absence. A student who fails to complete the exam or assignment within the prescribed period may receive a failing grade for that exam or assignment. If a student or an instructor disagrees about the nature of the absence [i.e., for the purpose of observing a religious holy day] or if there is similar disagreement about whether the student has been given a reasonable time to complete any missed assignments or examinations, either the student or the instructor may request a ruling from the chief executive officer of the institution, or his or her designee. The chief executive officer or designee must take into account the legislative intent of TEC 51.911(b), and the student and instructor will abide by the decision of the chief executive officer or designee.

Off-Campus Instruction and Course Activities	Off-campus, out-of-state, and foreign instruction and activities are subject to state law and University policies and procedures regarding travel and risk-related activities. Information regarding these rules and regulations may be found at http://www.utdallas.edu/BusinessAffairs/Travel_Risk_Activities.htm. Additional information is available from the office of the school dean.

Course Policies

These descriptions and timelines are subject to change at the discretion of the Professor.