

Metropolitan State University of Denver

Regular Course Syllabus

Fall 2016

CSS - 1751 - Computing and Security for Manufacturing

Status	completed
Tracking:	LAS1617-25
Department	Mathematical and Computer Sciences, Department of
Prefix:	CSS
Course Number:	1751
Course Type:	Computer Science Studies
Course Title:	Computing and Security for Manufacturing
Transcript Course Title:	Computing and Security for Mfg
Check All That Apply:	Elective
Credit Hours:	3
Schedule Type:	Lecture
Grade Mode:	Letter
Lecture:	45
Lab:	
Internship:	
Practicum:	
Other:	
Additional Student Work Hours per course:	90
Variable topics umbrella course:	No
If yes, number of credits/ repeats allowed	
Specified repeatable course:	No
If yes, number of credits/ repeats allowed	
Prerequisite(s):	CIS/CSS 1010 with a grade of "C" or better; or appropriate score on the computer literacy screening test.
Corequisite(s):	
Prerequisite(s) and/or Corequisite(s):	
Banner Prerequisite(s):	CSS 1010 or CIS 1010
Banner Corequisite(s):	
Banner Prerequisite(s) and/or Corequisite(s):	
Level	Undergraduate
Class	
Program/Major	
Student attribute	
Catalog Course Description:	As all aspects of manufacturing have become computerized, it is important that everyone involved become knowledgeable in computing in general and computer security specifically. This course gives a overview of what computing is and how programming is done. It covers how computers are connected to networks and the related networking protocols. It emphasizes manufacturing-specific concerns such as Industrial Control Systems and the Supervisory Control And Data Acquisition (SCADA) technology, protecting intellectual property at all phases, and

CSS 1751 - Fall 2016

	assuring the software supply chain.
Required Reading and Other Materials will be equivalent to:	Eric D. Knapp, Joel Thomas Langill, (2011), Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, ISBN-13: 978-1597496452
Specific, Measurable Student Behavioral Learning Objectives:	<ol style="list-style-type: none"> 1. Appraise the risks associated with the various software assets for manufacturing. 2. Assemble a set of controls to mitigate the computer security risks discovered. 3. Assess the variety of connections made to and within a manufacturing organization. 4. Construct a training program for a manufacturing organization. 5. Evaluate the types of programming performed and recommend appropriate security controls. 6. Analyze and manage the software supply chain. 7. Explain the basics of computer programming and networking. 8. Assess an organization's approach to ethical behavior.
Detailed Outline of Course Content (Major Topics and Subtopics) or Outline of Field Experience/ Internship	<ol style="list-style-type: none"> 1. Introduction to computing <ol style="list-style-type: none"> 1. Programming <ol style="list-style-type: none"> 1. Variables 2. Conditionals 3. Loops 4. Objects 5. Security issues 2. Networks <ol style="list-style-type: none"> 1. Packets 2. Topology 3. The Internet Protocol versions four and six 4. The Transmission Control Protocol 5. The User Datagram Protocol 2. Pervasive computing <ol style="list-style-type: none"> 1. Everything connected, and therefore vulnerable 2. Access and monitoring devices 3. Mobile device security 3. Necessary infrastructure <ol style="list-style-type: none"> 1. Water and waste water 2. Electricity 3. Telephony 4. Network providers 5. Emergency services 4. Manufacturing threats <ol style="list-style-type: none"> 1. Denial Of Service/production interruptions 2. Destruction of equipment and product. 3. Industrial espionage 5. The software supply chain <ol style="list-style-type: none"> 1. Securing software 2. Third party integrations 6. Securing intellectual property <ol style="list-style-type: none"> 1. Legal protections 2. Policy and procedural protections 3. Technical protections 7. Insider threats <ol style="list-style-type: none"> 1. Innocuous versus malicious 2. Securing the human 8. Industrial Control Systems <ol style="list-style-type: none"> 1. Embedded controllers 2. Networking 9. Supervisory Control And Data Acquisition (SCADA) <ol style="list-style-type: none"> 1. Threats 2. Connections 3. Isolation techniques 10. Securing hosts <ol style="list-style-type: none"> 1. Malware detection and mitigation

CSS 1751 - Fall 2016

	<ul style="list-style-type: none"> 2. Authentication 3. Authorization 11. Securing the network <ul style="list-style-type: none"> 1. Intrusion detection and prevention systems 2. Firewall 3. Monitoring and analysis 4. Partitioning 12. Computing ethics <ul style="list-style-type: none"> 1. Privacy 2. Anonymity 3. Proper use
Evaluation of Student Performance	Required: a midterm and final exam and four papers. Optional: quizzes, participation, classwork, homework, projects.
Learning Objectives	
Distribution of Credit Hours	3 (3+0)
Steps	
Originator	
Steve Beaty	APPROVED 09/12/2016 10:07AM
Department Curriculum Committee Chair	
Clark Dollard	APPROVED 09/12/2016 02:55PM
Department Chair	
Lindsay Packer	APPROVED 09/13/2016 04:21PM
Dean's Office Tracking Assignment	
Cynthia Philbrook	APPROVED 09/14/2016 08:34AM
Substantive College Level	
Linda Lang-Peralta	APPROVED 12/06/2016 04:21PM
Mona Mocanasu	APPROVED 09/28/2016 12:47PM
AVP Academic and Student Affairs	
Bernice Harris	APPROVED 12/07/2016 08:46AM