CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus

Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

Instructor	MICHAEL CLEARY	**E-Mail**	mcleary@csudh.edu (CTC 428 in Subject)
Office	NSM E115	**Office Hours**	Tuesdays 4:50PM - 6:50PM in NSM E115 and/or by appointment
Phone	Use E-Mail		
Classroom	SCC 800	**Class Time**	Thursdays 7:00PM - 9:45PM
URL	http://toro.csudh.edu/ - CSUDH Blackboard		

CSUDH CATALOG DESCRIPTION:
This course takes an in depth look at operating system security concepts and techniques. It examines theoretical concepts that make the world of security unique. Also, this course will adopt a practical hands-on approach when examining operating system security techniques.

CSUDH COURSE PRE-REQUISITE:
CSC 116 Introduction to Computer Hardware and Tools

CSUDH COMPUTER SCIENCE DEPARTMENT COURSE RESTRICTIONS:
CTC 316 and CTC 428 cannot be taken at the same time. CTC 316 is a PRE-REQUISITE of CTC 428.

CSUDH DEGREE MAPPING:
Bachelor of Arts in Computer Technology (BACT), Homeland Security Track, Upper Division Required
Minor in Computer Technology, Upper Division Selection

REMINDER:
- Bachelor of Arts in Computer Technology (BACT) students must earn a grade of "C" or better in each course taken within the Computer Science department.

CSUDH COMPUTER SCIENCE DEPARTMENT CONTACT INFORMATION:
DR. MOHSEN BEHESHTI, Department Chair, mbeheshti@csudh.edu, NSM A-132, 310-243-3398
VIOLETA DIAZ, Department Secretary, vdiaz@csudh.edu, NSM A-132, 310-243-3398
MARISOL ROCHA, Department Student Assistant, cssa@csudh.edu, NSM A-132, 310-243-3398

REQUIRED TEXTBOOKS:
Introduction to the New Mainframe: Security, March 2007, SG24-6776-00, ISBN 0738489646
See http://www.redbooks.ibm.com/abstracts/sg246776.html?Open (No Cost PDF)
See http://store.vervante.com/c/v/referpard?pard=ibm&newrew=1&isbn=0738489646 Hardcopy $ 68.75

ABCs of IBM zOS System Programming Volume 6: Security, August 2014, SG24-6986-01, ISBN 0738439800
See http://www.redbooks.ibm.com/abstracts/sg246986.html?Open (No Cost PDF)
See http://store.vervante.com/c/v/referpard?pard=ibm&newrew=1&isbn=0738439800 Hardcopy $ 43.75

Common Criteria for Information Technology Security Evaluation v3.1. r4, September 2012
Part 1: Introduction and General Model

See http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (No Cost PDF)
Part 2: Security Functional Components
See http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf (No Cost PDF)
Part 3: Security Assurance Components
See http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf (No Cost PDF)

Common Criteria Overview
See https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/the-common-criteria

Design Principles and Guidelines for Security, NPS-CS-07-014, Naval Postgraduate School, November 2007
See http://cisr.nps.edu/downloads/techpubs/nps_cs_07_014.pdf (No Cost PDF)

Guide to IEEE 802.11i: Establishing Robust Security Networks, NIST SP-800-97, February 07, 2007
See http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50897 (No Cost PDF)

Guide to Securing WiMAX Wireless Communications, NIST SP-800-127, September 30, 2010
See http://www.nist.gov/customcf/get_pdf.cfm?pub_id=906186 (No Cost PDF)

Introduction to zOS Multilevel Security (MLS), June 2007
See ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/r07_mls_intro.pdf (No Cost PDF)

zOS MVS Initialization and Tuning Reference 2.2, September 2016, SA23-1380-08
See http://publibz.boulder.ibm.com/epubs/pdf/iea3e213.pdf (No Cost PDF)

zOS Planning for Multilevel Security and the Common Criteria 2.2, March 2016, GA32-0891-01
See http://publibz.boulder.ibm.com/epubs/pdf/e0z3e110.pdf (No Cost PDF)

zOS CA System Integrity Statement, September 2010
See http://www.ca.com/us/collateral/technical-documents/na/ca-technologies-mainframe-products-integrity-statement.aspx (No Cost PDF)

zOS IBM System Integrity Statement, 1973
See ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/zOS_System_Integrity_Statement.pdf (No Cost PDF)

zOS IBM System Integrity Statement, June 2015
See http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSL03361USEN&attachment=ZSL03361USEN.PDF (No Cost PDF)

REQUIRED SOFTWARE:
Vista tn3270 Terminal Emulator, Tom Brennan Software (for Windows)
See http://www.tombrennansoftware.com/download.html Lab System Access Free, otherwise $30

REFERENCE MATERIAL:
SUBPART 239.71--SECURITY AND PRIVACY FOR COMPUTER SYSTEMS (TEMPEST: U.S. DEPARTMENT OF DEFENSE)
See http://www.acq.osd.mil/DPAP/DARS/DFARS/HTML/CURRENT/239_71.HTM

CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus

Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

Build Security In (BSI), US Department of Homeland Security
See https://buildsecurityin.us-cert.gov/

CA ACF2 for zOS Best Practices Guide r15, April 2014
See https://support.ca.com/cadocs/0/CA%20ACF2%20%20r15-ENU/Bookshelf_Files/PDF/ACF2_BestPractices_zOS_ENU.pdf (No Cost PDF)

CA Top Secret for zOS Best Practices Guide r15, July 2014
See https://support.ca.com/cadocs/0/CA%20Top%20Secret%20%20Security%20for%20z%20OS%20r15-ENU/Bookshelf_Files/PDF/TSS_BestPractices_zOS_ENU.pdf (No Cost PDF)

Committee on National Security Systems Guidance/Directives
See http://www.cnss.gov/

Cybersecurity, US Department of Homeland Security
See https://www.dhs.gov/topic/cybersecurity

Cybersecurity Framework, U.S. National Institute of Standards and Technology
See http://www.nist.gov/cyberframework/

Electronic Authentication Guideline, NIST SP 800-63-1, December 12, 2011
See http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910006 (No Cost PDF)

Employment and Internship Opportunities:
See USAJOBS https://www.usajobs.gov/ for all federal government jobs most offer preference for Veterans
See Jobs at IBM http://www-03.ibm.com/employment/us/ for all IBM jobs

FIPS PUB 140-2 Security Requirements for Cryptographic Modules, November 15, 2001
See http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (No Cost PDF)
FIPS PUB 140-2 Annex A: Approved Security Functions
See http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf (No Cost PDF)
FIPS PUB 140-2 Annex B: Approved Protection Profiles
See http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf (No Cost PDF)
FIPS PUB 140-2 Annex C: Approved Random Number Generators
See http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf (No Cost PDF)
FIPS PUB 140-2 Annex D: Approved Key Establishment Techniques
See http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf (No Cost PDF)
Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
See http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf (No Cost PDF)

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP-800-137, September 30, 2011
See http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909726 (No Cost PDF)

Introduction to the New Mainframe: zOS Basics, March 2011, SG24-6366-02, ISBN 0738435341
See http://www.redbooks.ibm.com/abstracts/sg246366.html?Open (No Cost PDF)
See http://store.vervante.com/c/v/referpard?pard=ibm&newrew=1&isbn=0738435341 Hardcopy $87.50

Introduction to the New Mainframe: Networking, August 2006, SG24-6772-00, ISBN 0738494798

CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus

Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

See http://www.redbooks.ibm.com/abstracts/sg246772.html?Open (No Cost PDF)
See http://store.vervante.com/c/v/referpard?pard=ibm&newrew=1&isbn=0738494798 Hardcopy $56.25

ISO/IEC 15408 Information Technology, Security Techniques, Evaluation Criteria for IT Security
Part 1: Introduction and General Model
See http://standards.iso.org/ittf/PubliclyAvailableStandards/c050341_ISO_IEC_15408-1_2009.zip
Part 2: Security Functional Components
See http://standards.iso.org/ittf/PubliclyAvailableStandards/c046414_ISO_IEC_15408-2_2008.zip
Part 3: Security Assurance Components
See http://standards.iso.org/ittf/PubliclyAvailableStandards/c046413_ISO_IEC_15408-3_2008.zip

Making Security Measurable (MSM), Mitre
See http://measurablesecurity.mitre.org/

National Strategy for Trusted Identities in Cyberspace (NSTIC), U.S. National Institute of Standards and Technology
See http://www.nist.gov/nstic/

Rainbow Series For Trusted Computers Networks, NSA/NCSC
See http://www.fas.org/irp/nsa/rainbow.htm
CSC-STD-003-85 Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments
CSC-STD-004-85 Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements
NCSC-TG-011 Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation

TCP/IP Tutorial and Technical Overview, December 2006, GG24-3376-07 (Wireless), ISBN 0738494682
See http://www.redbooks.ibm.com/abstracts/gg243376.html?Open (No Cost PDF)
See http://store.vervante.com/c/v/referpard?pard=ibm&newrew=1&isbn=0738494682 Hardcopy $106.25

United States Computer Emergency Readiness Team (US-CERT), US Department of Homeland Security
See http://www.us-cert.gov/

zOS UNIX Security Fundamentals, February 2007, REDP-4193-00
See http://www.redbooks.ibm.com/abstracts/redp4193.html?Open (No Cost PDF)

COURSE GOALS:
• Discuss the fundamentals of operating system and network security
• Support the planning, implementation, and auditing of a system's security
• Be able to discuss security as it applies specifically to the IBM Mainframe, and generically to all computing environments
• Understanding of Government Guidance involving Trusted Computers and TEMPEST Architecture

COURSE OUTCOMES:
• Understand the fundamentals of operating system and network security
• How to support the planning, implementation, and auditing of a system's security
• How to discuss security as it applies specifically to the IBM Mainframe, and generically to all computing

CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus
Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

environments
• Understand Government Guidance involving Trusted Computers and TEMPEST Architecture
• How to write, compile, and execute programs on a z/OS System
• How to use a 3270 Terminal Emulator (e.g., Vista tn3270) to access a zOS System
• How to use TSO/ISPF on a zOS System

AMERICANS WITH DISABILITIES ACT:
CSUDH adheres to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations for students with temporary and permanent disabilities. If you have a disability that may adversely affect your work in this class, I encourage you to register with Disabled Student Services (DSS) and to talk with me about how I can best help you. All disclosures of disabilities will be kept strictly confidential. NOTE: no accommodation can be made until you register with the DSS. For information call (310) 243-3660 or to use the Telecommunications Device for the Deaf, call (310) 243-2028 or goto: http://www4.csudh.edu/dss/

C**OMPUTER INFORMATION LITERACY EXPECTATIONS:**
It is expected that students will:
• Be able to access websites and online course materials which may require Flash and other plug-ins
• Be familiar with using a Learning Management System and check Blackboard at least every other day
• Be familiar with using email as a communication tool and check your official campus email account at least every other day
• Find Term Paper References and Extra Credit Articles using an Internet search engine (e.g., Google)
• Have regular access to a computer and internet access for the term of this course
• Use Microsoft Word for word processing unless otherwise approved by the instructor
• Use the library databases to find articles, journals, books, databases and other materials

ACADEMIC INTEGRITY:
Academic integrity is of central importance in this and every other course at CSUDH. You are obliged to consult the appropriate sections of the University Catalog and obey all rules and regulations imposed by the University relevant to its lawful missions, processes, and functions. ***All work turned in by a student for a grade must be the students' own work***. Plagiarism and cheating (e.g. stealing or copying the work of others and turning it in as your own) will not be tolerated, and will be dealt with according to University policy. The consequences for being caught plagiarizing or cheating range from a minimum of a zero grade for the work you plagiarized or cheated on, to being dropped from the course.

BEHAVIORAL STANDARDS:
Behavior that persistently or grossly interferes with classroom activities is considered disruptive behavior and may be subject to disciplinary action. Such behavior inhibits other students' ability to learn and an instructor's ability to teach. The instructor may require a student responsible for disruptive behavior to leave class pending discussion and resolution of the problem and may also report a disruptive student to the Student Affairs Office (WH A-410, 310-243-3784) for disciplinary action.

COURSE POLICIES:
This course uses the lecture format. Reading, projects and homework will be assigned, and all problems will be graded. It is expected that you will need to spend at least two hours studying outside the class for each hour spent in the class. That means you should plan to devote a minimum of nine (9) hours per week for this class (3-hours in class, 6-hours outside class). Note taking is very important in this course and students are asked to keep an organized notebook. A notebook will help you to organize your work for easy access when preparing for tests.

CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus

Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

HOMEWORK ASSIGNMENTS:
Please be aware that all homework assignments must be handed to the instructor in person and in class. The computer-print out homework is preferable, but hand- writing is also acceptable. However, it is the student's responsibility to make your writing clear enough for the instructor to grade.

PROJECT ASSIGNMENTS:
The standards for submission of projects will be made available per project assignment. Each project should be presentable and submitted with a cover sheet. Reports should include name of the student, section number, instructor, and class meeting time.

TERM PAPER:
The detailed requirements for the Term Paper will be posted on Blackboard at the beginning of the semester. The Term Paper must be on an Operating Systems Security Topic. Here are examples of topics:
- Cryptography Methodologies
- Electronic Authentication (e-Authentication) Methodologies
- Filesystem Security Methodologies
- Information Security Continuous Monitoring (ISCM) Methodologies
- zOS Security CICS, DB2 and IMS
- zOS Security RACF and SAF
- zOS Security SNA Security

LATE HOMEWORK/PROJECTS:
All assignments are due at midnight on the scheduled dates. No late assignment will be accepted.

ASSESSMENTS:
Two exams will be given; one Midterm Exam and one Final Exam. Missed exams MIGHT be able to be made up at the discretion of the professor. Quizzes will be given every class session that there is no exam. Quizzes CANNOT be made up no matter what the circumstances. The assessment material that does not appear in the textbooks will be presented in lectures. Students are responsible for the additional materials that will be presented in the class.

ASSESSMENT RULES:
Assessments are to test your own personal knowledge of a subject so during an assessment...
- No Additional Open Windows are allowed, so close all windows except one Blackboard window
- No Assessment Password Sharing with those not physically present in the assigned classroom
- No Assessment Password Usage when not physically present in the assigned classroom
- No Electronic Devices of any kind are allowed, so they all need to be put away or turned off (Cell phones, iPads, Tablets, etc…)
- No Leaving Classroom, so take care of everything outside of the classroom before the assessment. If you need to leave the classroom during an assessment, let the instructor know and your attempt will be zeroed out and you can take the assessment completely over when you return to the classroom.
- No Looking at other students answers
- No Notes of any kind are allowed
- No Reference Material of any kind is allowed
- No Student Owned Computers can be used to take the assessment
- No Talking for any reason
- No Textbooks of any kind are allowed

When you are done with the assessment…

CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus
Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

- At the Beginning of the Class Period - Leave the classroom until the instructor tells you to return
- At the End of the Class Period, Midterm and Final - Leave the classroom as class is over for the day

GRADING SCALE:
Between 95.5% and 100% = A
Between 89.5% and Less Than 95.5% = A-
Between 86.5% and Less Than 89.5% = B+
Between 82.5% and Less Than 86.5% = B
Between 79.5% and Less Than 82.5% = B-
Between 76.5% and Less Than 79.5% = C+
Between 72.5% and Less Than 76.5% = C
Between 69.5% and Less Than 72.5% = C-
Between 64.5% and Less Than 69.5% = D+
Between 60.5% and Less Than 64.5% = D
Between 00% and Less Than 60.5% = F

EVALUATION TECHNIQUES:
Quizzes, 26%
IBM Master the Mainframe Contest (Lab), 15%
Term Paper on Operating Systems Security, 15%
Exam 1, 19%
Final Exam, 20%
Curriculum Vitae (CV), 5%
Stand Alone Extra Credit, 10% (maximum)

Stand Alone Extra Credit Options
- Assignment Extra Credit Article Summary - ECAS
- Assignment Extra Credit CSUDH Cyber Security Awareness Week Workshops (5% maximum) - ECCW
- Assignment Extra Credit CSUDH Cyber Security Club (CSC) Lab (5% maximum) - ECCL
- Assignment Extra Credit Local Information Technology User Groups (5% each) - ECUG

Note Regarding Extra Credit:
For ECAS and ECUG there is no double dipping. You need to tell Michael Cleary which courses get the extra credit.
For ECCW and ECCL there is no double dipping. You need to tell CSC Lab which courses get the extra credit.
For ECUG if you arrive late or leave early you will not get any extra credit at all. Dress Code is Business Casual.

IBM Master the Mainframe Contest 2015 (October 2015 through December 2015):
Assembler, C, C++, COBOL , Data Representation (ASCII, binary, bit, byte, decimal, EBCDIC, hexadecimal, octal, Unicode), IBM Bluemix (a Platform as a Service (PaaS) based on the Cloud Foundry open source project and built on IBM Softlayer's infrastructure), ISPF DSLIST (3.4), ISPF Editor, ISPF, Java, JCL, JSON (JavaScript Object Notation), MongoDB, OMVS Shell, RACF Dataset Protection, SDSF (System Display and Search Facility), SSH Client (PuTTY), Telnet 3270 Emulator (Vista tn3270), TSO, z/OS System Commands, z/TPF Database Facility, zLinux Shell.

Registration URL http://ibm.biz/masterthemainframe
Contest URL http://mtm2016.mybluemix.net/

CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus

Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

CV Entry - CTC 428 Operating System Security

After reviewing zOS Operating System and zOS Network, the focus shifts to security. zOS Security topics include: Overview of Security Fundamentals, Hardware & Networking Security, Securing Operating Systems on System z, Security in Middleware & Applications, and Information Security Program & Compliance. Students gain hands on zOS experience by using TSO/ISPF during lab exercises and the IBM Master the Mainframe Contest. Additional topics include Build Security In (BSI), Common Criteria (CC), Confidentiality Integrity Availability (CIA), Confidentiality Models (Access Control, Flow), Cryptographic Algorithms (Asymmetric, One Way, Symmetric), DBMS Security Options, Federal Risk and Authorization Management Program (FedRAMP), Health Insurance Portability and Accountability Act (HIPAA), Information Security Continuous Monitoring (ISCM), Integrity Control Principles (Need to Know, Rotation of Duties, Separation of Duties), Intrusion Detection Services (IDS), Making Security Measurable (MSM), National Initiative for Cybersecurity Education (NICE), OLTP Security Options, Point of Entry (POE), RACF User Privileges (Auditor, Operations, Special), Sarbanes-Oxley (SOX), Security Integrity Models (Biba, Brewer Nash, Clark Wilson, Goguen Meseguer), Software Protection Initiative (SPI), Statement on Auditing Standards No. 70 (SAS 70), Statement on Standards for Attestation Engagements No. 16 (SSAE 16). Students are encouraged to attend Southern California Information Technology User Group meetings.

TIMELINE:

Topic	**Date**
W01, Review Syllabus, Review References, Q01	08/25/2016
W02, Review zOS Textbook (C01-C17) and zNetwork Textbook (C01-C07), Q02	09/01/2016
W03, E01, zOS Textbook (C01-C17) and zNetwork Textbook (C01-C07) (152 questions)	09/08/2016
W04, zSecurity L1 Security Concepts C01-C04, Q03	09/15/2016
W05, zSecurity L2 Architecture and Hardware C05-C06, Q04	09/22/2016
W06, zSecurity L3 Operating Systems Security C09, Q05	09/29/2016
W07, Design Principles and Guidelines for Security (DPGS), zOS System Integrity Statement, Q06, IBM Master the Mainframe Contest begins 10/03/2016, LAADB2UG 10/06/2016	10/06/2016

CTC 428-01 (40941) Operating System Security Fall 2016 Syllabus

Thursdays 7:00PM - 9:45PM in SCC 800 from 08/20/2016 to 12/19/2016

W08, zSecurity L4 Security Elements of zOS C07, C12, C14, Q07	10/13/2016
W09, zSecurity L5 SAF and RACF C10, Q08	10/20/2016
W10, zSecurity L6 zOS Unix System Services Security C11, Q09	10/27/2016
W11, zSecurity L7 Communications and Network Security C08, Q10, Term Papers Due, Master the Mainframe Contest Part 1 and 2 Due	11/03/2016
W12, zSecurity L8 Application Security C17-C19, Q11, Curriculum Vitae Due, Extra Credit Article Summaries Due	11/10/2016
W13, zSecurity Lesson 9 Standards and Policies C22-C24, Q12, SCzSUG 11/22/2016	11/17/2016
W14, Thanksgiving Day Holiday, Campus Closed, No Classes	11/24/2016
W15, Information Security Continuous Monitoring (ISCM), Q13	12/01/2016
W16, E02, Entire zSecurity Textbook, plus CC, DPGS, MLS (nnn questions), 7:45PM - 9:45PM	**12/08/2016**