STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CYBR 455 – ACCESS CONTROL, AUTHENTICATION, and PUBLIC KEY INFRASTRUCTURE

Created by: Minhua Wang
Updated by: Minhua Wang

SCHOOL OF SCIENCE, HEALTH & CRIMINAL JUSTICE
CENTER FOR CRIMINAL JUSTICE, INTELLIGENCE AND CYBERSECURITY
SPRING 2020

A. **TITLE**: ACCESS CONTROL, AUTHENTICATION, and PUBLIC KEY INFRASTRUCTURE

B. **COURSE NUMBER:** CYBR 455

C. **CREDIT HOURS: (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity)**

 # Credit Hours: 3
 # Lecture Hours: 3 **per week**
 # Lab Hours: **per week**
Other: **per week**

Course Length: 15 **Weeks**

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

F. **SEMESTER(S) OFFERED:** Fall or Spring

G. **COURSE DESCRIPTION:** This course defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs. It looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them with risk mitigation strategies and techniques. Access control systems and stringent authentication are presented as ways to mitigate risk. It also covers Public Key Infrastructure (PKI) components and how the various components support e-business and strong security services.

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): CITA 360 Cryptology in Theory and Practice
b. Co-requisite(s): none
c. Pre- or co-requisite(s): none

I. **STUDENT LEARNING OUTCOMES:**

By the end of this course, the student will be able to:

Course Student Learning Outcome [SLO]	***PSLO***	***ISLO***
a. Specify fundamental concepts and components of access control, authentication, and public key infrastructure	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
b. Summarize and compare various methodologies in access control, authentication, and public key infrastructure	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA] 5
c. Recommend access control, authentication, and public key infrastructure solutions to specific electronic system implementations	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA, PS] 5

d. Exhibit examples of most current developments in access control, authentication, and public key infrastructure	6. Adapt to new situations and demands by applying and/or updating his/her knowledge and skills	5

KEY	**Institutional Student Learning Outcomes [ISLO 1 – 5]**
ISLO #	**ISLO & Subsets**
1	**Communication Skills** Oral [O], Written [W]
2	**Critical Thinking** *Critical Analysis [CA], Inquiry & Analysis [IA], Problem Solving [PS]*
3	**Foundational Skills** *Information Management [IM], Quantitative Lit,/Reasoning [QTR]*
4	**Social Responsibility** *Ethical Reasoning [ER], Global Learning [GL], Intercultural Knowledge [IK], Teamwork [T]*
5	**Industry, Professional, Discipline Specific Knowledge and Skills**

J. APPLIED LEARNING COMPONENT: **Yes** __X___ **No**_____

- Classroom/Lab

K. TEXTS: None

L. REFERENCES: Various online resource such as SUNY Canton Library Books24x7 ITPro Book Database

M. EQUIPMENT: Computer lab classroom with virtual machine software installed

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- Exams
- Quizzes
- Participation

P. DETAILED COURSE OUTLINE:

I. Introduction to Access Control, Authentication, and Public Key Infrastructure
   A. Access Control
   B. Authentication
   C. Public Key Infrastructure

II. Planning
   A. Access Control Framework
   B. Assessing Risk and Its Impact on Access Control
   C. Business Drivers for Access Controls
   D. Access Control Policies, Standards, Procedures, and Guidelines
   E. Unauthorized Access and Security Breaches

F. Mapping Business Challenges to Access Control Types
G. Human Nature, Organizational Behavior, and Considerations

III. Implementation

A. Access Control for Information Systems
B. Physical Security and Access Control
C. Access Control in the Enterprise
D. Access Control System Implementations
E. Access Control Solutions for Remote Workers
F. Public Key Infrastructure and Encryption
G. Testing Access Control Systems
H. Access Control Assurance

IV. Other Topics: As Defined by the Instructor (The topics on most recent Access Control, Authentication, and Public Key Infrastructure developments are strongly recommended.)

Q. <u>LABORATORY OUTLINE</u>: N/A