UNIVERSITY AT ALBANY
State University of New York

Office of the Senior Vice President for Academic Affairs &
Provost

April 17, 2018

Elizabeth Bringsjord, Ph.D.
Vice Provost and Vice Chancellor for Academic Affairs
State University of New York
State University Plaza
Albany, NY 12246

Dear Dr. Bringsjord,

On behalf of the faculty at the University at Albany, I am transmitting the attached proposal for revision of our undergraduate B.S. program in Digital Forensics. The updated curriculum responds to the guidelines provided by the National Institute of Standards and Technology's National Initiative for Cyber Education and to suggestions made by the industry advisory board for this program. These changes have been fully considered and approved through our campus governance system.

We are appreciative of anticipated efforts by staff in your Office of Program Review for the consideration of the proposal. Should there be any technical questions or the need for additional materials, please have inquiries directed to Celine LaValley (clavalley@albany.edu).

Thank you for your consideration and assistance.

Sincerely,

James R. Stellar
Provost and Senior Vice President for Academic Affairs

Attachment

c. Vice Provost Jeanette Altarriba, Undergraduate Education
Dean Hany Shawky, School of Business
Professor Sanjay Goel, Information Security and Digital Forensics

Program Revision Proposal: Changes to an Existing Program

Form 3A

Version 2016-10-13

SUNY approval and SED registration are required for many changes to registered programs. To request a change to a registered program leading to an undergraduate degree, a graduate degree, or a certificate that does not involve the creation of a new program,[1] a Chief Executive or Chief Academic Officer must submit **a signed cover letter and this completed form** to the SUNY Provost at *program.review@suny.edu*.

Section 1. General Information		
a) Institutional Information	Institution's 6-digit SED Code:	210500
	Institution's Name:	University at Albany, State University of New York
	Address:	*1400 Washington Ave. Albany, NY*
b) Program Locations	List each campus where the entire program will be offered (with each institutional or branch campus 6-digit SED Code):	
	List the name and address of off-campus locations (i.e., extension sites or extension centers) where courses will offered, **or check here [X] if not applicable**:	
c) Registered Program to be Changed	Program Title:	Digital Forensics
	SED Program Code	36827
	Award(s) (e.g., A.A., B.S.):	B.S.
	Number of Required Credits:	Minimum [120] If tracks or options, largest minimum [ ]
	HEGIS Code:	0799
	CIP 2010 Code:	11.1003
	Effective Date of Change:	Fall 2018
	Effective Date of Completion[2]	
d) Campus Contact	Name and title: Celine LaValley, Assistant to the Vice Provost for Undergraduate Education Telephone and email: (518) 492-3950 clavalley@albany.edu	
e) Chief Executive or Chief Academic Officer Approval	**Signature affirms that the proposal has met all applicable campus administrative and shared governance procedures for consultation, and the institution's commitment to support the proposed program.** ***E-signatures are acceptable.*** Name and title: James R. Stellar, Ph.D. Provost and Vice President for Academic Affairs Signature and date: 4/17/18	
	If the program will be registered jointly[3] with one or more other institutions, provide the following information for each institution:	
	Partner institution's name and 6-digit SED Code: Name, title, and signature of partner institution's CEO (or **append** a signed letter indicating approval of this proposal):	

[1] To propose changes that would create a new program, Form 3B, Creating a New Program from Existing Program(s), is required.

[2] If the current program(s) must remain registered until enrolled students have graduated, the anticipated effective date by which continuing students will have completed the current version of the program(s).

[3] If the partner institution is non-degree-granting, see SED's CEO Memo 94-04.

Section 2. Program Information

Section 2.1. Changes in Program Content

[ ] No changes in program content. *Proceed to Section 2.2.*

a) Check all that apply. Describe each proposed change and why it is proposed.

[X] Cumulative change from SED's last approval of the registered program of one-third or more of the minimum credits required for the award (e.g., 20 credits for associate degree programs, 40 credits for bachelor's degree programs)
[X] Changes in a program's focus or design

The program changes are being done to align the curriculum with the NIST/NICE guidelines as well as in response to the suggestions of the industry advisory board for the program. The market is increasingly dominated by the need from the private sector to support cyber security analytics and incident response. The changes will put our students in a better position to capitalize on the market opportunities. The following changes are proposed:

Dropped three classes from the program and added three new classes to the program; the number of credits for the major remains the same. The classes were dropped to shift the program away from law enforcement where student placements were not strong. Two of the three classes added were previously electives but very necessary for the students and so were added to the core requirements. The programming analytics course was added to help students become more adept with analytic techniques that help with security and forensics, e.g., data cleanup, sorting, searching etc.

Dropped:
CRJ 201 Introduction to Criminal Justice
CRJ 203 Criminology
ASOC 101 Introduction to Sociology

Added:
BFOR 206 Programming for Analytics (New)
BFOR 412 Cyber Incident Response (Previously Elective)
BFOR 413 Multimedia Forensics (Previously Elective)

Additionally, content of some classes was revised to focus more on cyber security (NIST/NICE)

Changed:
Retired BFOR 300 Databases for Digital Forensics
Split the course into two portions, BFOR 205 Introduction to Database Systems and BFOR 306 Database Security and Forensics. Previously all this was crunched into one course that did not allow students to get a deeper understanding of this important area.

Moved Content from BFOR 302 eDiscovery Forensics to BFOR 402 eDiscovery and Moot Courts. We did this to better align the legal aspects of forensics together and to provide more room for cyber security curriculum.

Created a new course BFOR 305 Cyber Defense that filled the gaps in BFOR 204 Introduction to Cyber Security. Earlier the content of BFOR 204 was very compressed and splitting that into two classes provides the right level of coverage for the topic.

Combined the content of BFOR 400 Forensic Accounting and Fraud Examination and BFOR 404 Forensic Accounting Investigative Techniques into a single class and retired BFOR 404 Forensic Accounting Investigative Techniques. Both these classes were very light with redundancy that resulted in high student dissatisfaction. The combined class has adequate amount of content. This also allows room for a new class that has been created i.e. BFOR 403 Risk Analysis and Security Policies. This topic was found to be missing by the advisory board and through an analysis of the suggested NIST/NICE framework.

[ ] Adding or eliminating one or more options, concentrations or tracks
[ ] Eliminating a requirement for program completion (such as an internship, clinical placement, cooperative education, or other work or field-based experience). Adding such requirements must remain in compliance with SUNY credit cap limits.
[ ] Altering the liberal arts and science content in a way that changes the degree classification of an undergraduate program, as defined in Section 3.47(c)(1-4) of Regents Rules

b) **Provide** a side-by-side comparison of all the courses in the existing and proposed revised program that clearly indicates all new or significantly revised courses, and other changes.

REGISTERED PROGRAM (July 2014)	PROPOSED REVISION
APSY101 Introduction to Psychology	No change
ASOC 115 Introduction to Sociology	Course removed
BACC 211 Financial Accounting	No change
BFOR 100 Introduction to Information Systems	No change
BITM 215 Information Technologies for Business	No change
RCRJ 201 Introduction to the Criminal Justice Process	Course removed
RCRJ 203 Criminology	Course removed
RCRJ 281 Introduction to Statistics in Criminal Justice	No change
RCRJ 202 Introduction to Law and Criminal Justice	No change
BFOR 203 Networking – Introduction to Communications	Course title changed to Networking and Cryptography
BFOR 204 Fundamentals of Information and Cybersecurity	Course title changed to Introduction to Cybersecurity; course content revision
BFOR 300 Databases for Digital Forensics	Course removed
BFOR 400 Forensic Accounting and Fraud Detection	Course content revision
BFOR 201 Introduction to Digital Forensics	No change
BFOR 202 Cyber Crime Investigation	Course removed
BFOR 301 Computer Forensics 1	Course title changed to Computer Forensics
BFOR 302 eDiscovery	Course removed
BFOR 303 Computer Forensics 11	Course title changed to Computer and Memory Forensics
BFOR 304 Network and Mobile Forensics	Course title changed to Mobile Forensics
BACC 404 Forensic Accounting Investigative Techniques	Course removed
BFOR 401W Advanced Digital Forensics	No change
BFOR 402 Digital Forensics Moot Court	Course title changed to eDiscovery Forensics and Moot Court; course content revision
	New Course: BFOR 205 Introduction to Database Systems
	New Course: BFOR 206 Programming for Analytics

	New Course: BFOR 305 Cyber Defense
	New Course: BFOR 306 Database Security and Forensics
	New Course: BFOR 403 Risk Analysis and Security Policies
	New Course: BFOR 412 Cyber Incident Response and Penetration Testing
	New Course: BFOR 413 Multimedia Forensics
	Elective offerings
	New Course: BFOR 410 International Cyber Conflicts
	New Course: BFOR 411 SCADA Forensics
	New Course: BFOR 416 Advanced Data Analytics
	New Course: BFOR 418 Assembly Language & Malware Reverse Engineering
	New Course: BFOR 419 System Administration and Operating Systems Concepts
	New Course: BFOR 420 National Cyber Security Challenge Problems

c) For each new or significantly revised course, **provide** a syllabus at the end of this form, and, on the ***SUNY Faculty Table*** provide the name, qualifications, and relevant experience of the faculty teaching each new or significantly revised course. NOTE: *Syllabi for all courses should be available upon request. Each syllabus should show that all work for credit is college level and of the appropriate rigor. Syllabi generally include a course description, prerequisites and corequisites, the number of lecture and/or other contact hours per week, credits allocated (consistent with SUNY policy on credit/contact hours), general course requirements, and expected student learning outcomes.*

Please see Appendix 1.

d) What are the additional costs of the change, if any? If there are no anticipated costs, explain why.

There will be no cost implications since the program is restructured to align with NSA and NIST/NICE curricular guidelines. No extra resources are needed.

Section 2.2. Other Changes

Check all that apply. Describe each proposed change and why it is proposed.

[ ] Program title
[ ] Program award
[ ] Mode of delivery
NOTES: *(1) If the change in delivery enables students to complete 50% of more of the program via distance education, submit a Distance Education Format Proposal* as part of this proposal. *(2) If the change involves adding an accelerated version of the program that impacts financial aid eligibility or licensure qualification, SED may register the version as a separate program.*
[ ] Format change(s) (e.g., from full-time to part-time), based on SED definitions, for the **entire** program

1) State proposed format(s) and consider the consequences for financial aid
2) Describe availability of courses and any change in faculty, resources, or support services.

[ ] A change in the total number of credits in a certificate or advanced certificate program

[ ] Any change to a registered licensure-qualifying program, or the addition of licensure qualification to an existing program. **Exception:** Small changes in the required number of credits in a licensure-qualifying program that do not involve a course or courses that satisfy one of the required content areas in the profession.

Section 3. Program Schedule and Curriculum

a) For **undergraduate programs**, complete the ***SUNY Undergraduate Program Schedule*** to show the sequencing and scheduling of courses in the program. If the program has separate tracks or concentrations, complete a ***Program Schedule*** for each one.

NOTES: *The* ***Undergraduate Schedule*** *must show* ***all curricular requirements*** *and demonstrate that the program conforms to SUNY's and SED's policies.*

- *It must show how a student can complete all program requirements within SUNY credit limits, unless a longer period is selected as a format in Item 2.1(c): two years of full-time study (or the equivalent) and 64 credits for an associate degree, or four years of full-time study (or the equivalent) and 126 credits for a bachelor's degree. Bachelor's degree programs should have at least 45 credits of upper division study, with 24 in the major.*
- *It must show how students in A.A., A.S. and bachelor's programs can complete, within the first two years of full-time study (or 60 credits), no fewer than 30 credits in approved SUNY GER courses in the categories of Basic Communication and Mathematics, and in at least 5 of the following 8 categories: Natural Science, Social Science, American History, Western Civilization, Other World Civilizations, Humanities, the Arts and Foreign Languages*
- *It must show how students can complete Liberal Arts and Sciences (LAS) credits appropriate for the degree.*
- *When a SUNY Transfer Path applies to the program, it must show how students can complete the number of SUNY Transfer Path courses shown in the Transfer Path Requirement Summary within the first two years of full-time study (or 60 credits), consistent with SUNY's Student Seamless Transfer policy and MTP 2013-03.*
- *Requests for a program-level waiver of SUNY credit limits, SUNY GER and/or a SUNY Transfer Path require the campus to submit a Waiver Request –with compelling justification(s).*

EXAMPLE FOR ONE TERM: Undergraduate Program Schedule

Term 2: Fall 20xx	Credits per classification						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Prerequisite(s)**
ACC 101 Principles of Accounting	4			4	4		
MAT 111 College Mathematics	3	M	3	3			MAT 110
CMP 101 Introduction to Computers	3						
HUM 110 Speech	3	BC	3			X	
ENG 113 English 102	3	BC	3				
Term credit total:	16	6	9	7	4		

b) *For* ***graduate programs****, complete the* ***SUNY Graduate Program Schedule****. If the program has separate tracks or concentrations, complete a* ***Program Schedule*** *for each one.*

NOTE: *The* ***Graduate Schedule*** *must include all curriculum requirements and demonstrate that expectations from Part 52.2(c)(8) through (10) of the Regulations of the Commissioner of Education are met.*

SUNY Undergraduate Program Schedule (*OPTION: You can paste an Excel version of this schedule AFTER this line, and delete the rest of this page.)*

Program/Track Title and Award:_______Digital Forensics BS____

a) Indicate **academic calendar type**: [X] Semester [ ] Quarter [ ] Trimester [ ] Other (describe):

b) **Label each term in sequence**, consistent with the institution's academic calendar (e.g., Fall 1, Spring 1, Fall 2)

c) **Name of SUNY Transfer Path, if one exists: ____n/a___________________________________ See Transfer Path Requirement Summary for details**

d) Use the table to show **how a typical student may progress through the program**; copy/expand the table as needed. **Complete all columns that apply to a course.**

Fall 1:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
BFOR 201 Intro to Digital Forensics	3			3			
APSY 101 Intro to Psychology	3	SS	3	3			
US History Gen Ed	3	AH	3				
Foreign Language Gen Ed	4	FL	4				
Basic Communication Gen Ed	3	BC	3				
Term credit totals:	16	13	13	6			

Spring 2:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
RCRJ 281 Intro to Statistics in CJ	3	M	3	3			
RCRJ 202 Intro to Law and CJ	4		4	4			
BFOR 100 Intro to Information Systems	3			3			
International Perspectives Gen Ed	3	OW	3				
Natural Science Gen Ed	3	NS	3				
Term credit totals:	16	9	13	10			

Fall 2:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
BFOR 203 Networking & Cryptography	3			3			
BFOR 205 Intro to Database Systems	3			3		X	BFOR 100
BACC 211 Financial Accounting	3			3			
Humanities Gen Ed	3	H	3				
Challenges Gen Ed	3	Local	3				
Term credit totals:	15	6	6	9			

Spring 2:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
BITM 215 Info Technologies for Business	3			3			
BFOR 204 Intro to Cyber Security	3			3			BFOR 203
BFOR 206 Programming for Analytics	3			3		X	BFOR 100, 203
Arts Gen Ed	3	AR	3				
Liberal Arts Elective	3		3				
Term credit totals:	15	3	6	9			

Fall 3:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
BFOR 301 Computer Forensics	3			3			BFOR 201
BFOR 304 Mobile Forensics	3			3			BFOR 201
BFOR 305 Cyber Defense	3			3		X	BFOR 204
U/L Liberal Arts Elective	3		3				
U/L Liberal Arts Elective	3		3				
Term credit totals:	15		6	9			

Spring 3:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
BFOR 303 Computer and Memory Forensics	3			3			BFOR 201
BFOR 306 Database Security and Forensics	3			3		X	BFOR 204, 205
BFOR 412 Cyber Incident Response and Pen Testing	3			3		X	BFOR 204, 206, 305
Liberal Arts Elective U/L	3		3				
Liberal Arts Elective	3		3				
Term credit totals:	15		6	9			

Fall 4:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
BFOR 401 Advanced Digital Forensics	4			4			BFOR 301, 303
BFOR 403 Risk Analysis & Security Policies	3			3		X	BFOR 204, 305
BFOR 413 Multimedia Forensics	3			3		X	BFOR 201
Liberal Arts Elective	3		3				
Liberal Arts Elective U/L	2		2				
Term credit totals:	15		5	10			

Spring 4:	See KEY.						
Course Number & Title	**Cr**	**GER**	**LAS**	**Maj**	**TPath**	**New**	**Co/Prerequisites**
BFOR 402 eDiscovery Forensics and Moot Courts	4			4			BFOR 201
BFOR 400 Forensic Accounting and Fraud Examination	3			3			BACC 211
Liberal Arts Elective	3		3				
Liberal Arts Elective	3		3				
Term credit totals:	13		6	7			

Program Totals (in credits):	**Total Credits: 120**	**SUNY GER: 31**	**LAS:61**	**Major:69**	**Elective & Other: 48**	**Upper Division: 46**	**Upper Division Major: 35**	**Number of SUNY GER Categories:**
								9

KEY Cr: credits **GER:** SUNY General Education Requirement (Enter Category Abbreviation) **LAS:** Liberal Arts & Sciences (Enter credits) **Maj:** Major requirement (Enter credits) **TPath:** SUNY Transfer Path Courses (Enter credits) **New:** new course (Enter X) **Co/Prerequisite(s):** list co/prerequisite(s) for the noted courses **Upper Division:** Courses intended primarily for juniors and seniors **SUNY GER Category Abbreviations:** American History (AH), Basic Communication (BC), Foreign Language (FL), Humanities (H), Math (M), Natural Sciences (NS), Other World Civilizations (OW), Social Science (SS), The Arts (AR), Western Civilization (WC)

Section 4. SUNY Faculty Table

a) If applicable, provide information on faculty members who will be teaching new or significantly revised courses in the program. Expand the table as needed.

b) Append at the end of this document position descriptions or announcements for each to-be-hired faculty member

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
PART 1. Full-Time Faculty					
Fabio R. Auffant II	100%	BFOR 301 Computer Forensics BFOR 303 Computer and Memory Forensics BFOR 401W Advanced Digital Forensics	M.S. Champlain College	Digital Forensics Management	Extensive technical training and over 27 years' experience in criminal investigations, court testimony, Cyber Crime, Digital Forensics, and lab management – Computer Crime Unit – NY State Police Certified trainer – NYS Police *See Resume for more qualifications.
Devipsita Bhattacharya	100%	BFOR 305 Cyber Defense BFOR 412 Cyber Incident Response and Pen Testing	Ph.D. University of Arizona	Management Information Systems Emphasis (Minor: Information Resources and Library Sciences)	
Liyue Fan	100%	BFOR 205 Introduction to Database Systems BFOR 306 Database Security and Forensics	Ph.D. Emory University	Computer Science and Informatics	
Victoria Kisekka	100%	BFOR 403 Risk Analysis & Security Policies BFOR 400 Forensic Acct. and Fraud Examination	Ph.D. University of Buffalo	Management Science and Systems	
Jungwon Kueng	100%	BFOR 202 Intro to Cyber Security: Threats & Vul.	Ph.D. University of Wisconsin – Madison	Operation and Information Management	

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
Lee Spitzley	50%	BFOR 206 Programming for Analytics BFOR 416 Advanced Data Analytics BFOR 418 System Administration and Operating Systems Concepts	Ph.D. University of Arizona	Business Administration-Management Information Systems	
Suryadipta Majumdar	50%	BFOR 101 Introduction to Information Systems	Ph.D. Concordia University, Canada	Information & Systems Engineering	
*Sanjay Goel, Program Director	25%	BFOR 203 Networking & Cryptography BFOR 204 Intro to Cyber Security BFOR 410 International Cyber Conflicts BFOR 420 National Cybersecurity Challenge Problems	Ph.D. RPI	Mechanical Engineering	Dr. Goel is the founder of the Digital Forensics program has a background in engineering, computer science, and software development. He worked for several years at GE research laboratories writing software for engine design. He has worked in the area of technical and behavioral cyber security for the last 14 years and is world-renowned in the field. He has several million dollars in funded research in cyber security. He is also an international expert in cyber warfare. Professional Experience: 2016 – present, Associate Dean of Information Security and Digital Forensics, University at Albany, SUNY 2016 – present, Professor, Information Technology Mgmt, University at Albany, SUNY 2012 – present, Chair, Info. Tech. Mgt. Department, University at Albany, SUNY

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
					2008 – 2016, Associate Professor, University at Albany, SUNY 2001– 2007, Assistant Professor, University at Albany, SUNY 1996 – 2001 Mechanical Engineer, GE Global Research (Schenectady, NY) Publications: 1. Goel, S., Williams, K., Dincelli, E., Got Phished: Internet Security and Human Vulnerability, Journal of the AIS. 2. Giboney, J., Proudfoot, J.G., Goel, S., Valacich, J.S., The Security Expertise Assessment Measure (SEAM): Developing a Scale for Hacker Expertise, Computers & Security. 3. Goel, Sanjay (2015): Anonymity vs. Security: The Right Balance for the Smart Grid," Communications of the Association for Information Systems, 36(2), Available online at http://aisel.aisnet.org/cais/vol36/iss1/2 4. Hong, Y., Sanjay Goel and Wen Ming Liu, "An Efficient and Privacy Preserving Scheme for Energy Exchange among Smart Microgrids", International Journal of Energy Research, Wiley, 2015. 5. Hong, Y., Vaidya, J., Lu, H., Karras, P., and Goel, S., (2014). Collaborative Search Log Sanitization: Toward Differential Privacy and Boosted Utility", IEEE Transactions on

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
					Dependable and Secure Computing (TDSC), IEEE Computer Society.
Part 2. Part-Time Faculty					
Joseph M. Donohue	50%	BFOR 201 Introduction to Digital Forensics	AS – Columbia-Greene Community College State University of New York – Plattsburgh	Computer Science Computer Science	Extensive technical training and over 29 years' experience in criminal investigations, court testimony, Cyber Crime, Digital Forensics, and lab management – Computer Crime Unit – NY State Police Certified trainer – NYS Police Professional Experience: Uniform Trooper October 1983 – September 1989 Fishkill,NY – New Lebanon, NY – Claverack, NY Responsibilities included the investigation and enforcement of NYS Vehicle & Traffic Laws, Penal Law and applicable selected laws. Field Training Officer training newly assigned State Police Academy graduates. Investigator – Bureau of Criminal Investigation September 1989-October 2006 Fishkill, NY – Dover Plains, NY Investigation of all NYS Penal Law felonies, including but not limited to rape, burglary, grand larceny, homicides, counterfeiting and child abuse. Trained Arson-Cause and Origin investigator. Computer Crime Unit – Albany, NY

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
					33%Investigation of all technology related crimes and conducting computer forensics on all related evidence received from across New York State. Training law enforcement across the state to investigate technology crimes. Lead investigator on the New York State Internet Crimes Against Children Task Force. Author and execute search warrants related to technology crimes. Lieutenant – October 2006 – November 2012 Computer Crime Unit – Albany, NY Supervise all field assigned CCU investigators conducting technology investigations and computer forensics. Alternate Task Force Commander for the NYS Internet Crimes Against Children Task Force. Train law enforcement in technology crime investigation and computer forensics.
John M. Gallo	33%	BFOR 304 Mobile Forensics	AAS Hudson Valley Community College	Criminal Justice	Extensive technical training and over 18 years' experience in criminal investigations, court testimony, Cyber Crime, Digital Forensics, and lab management – Computer Crime Unit – NY State Police Professional Experience: Gallo is currently employed by New York State Police as an

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
					Acting Senior Investigator assigned to the Computer Forensic Laboratory at the Forensic Identification Center. Before being appointed at his current position he was assigned as an Investigator in the CFL at the FIC, as a Senior Forensic Examiner. Prior to being promoted to Investigator, Gallo was assigned to SP Kinderhook. During his assignment at SP Kinderhook he was assigned as the School Resource Officer at Ichabod Crane Central School District. At the time, he was also a troop K zone 1 crime scene technician. Prior to his employment with the NYS Police he was employed with the City of Hudson Police Department from July 1995. In 2002, Gallo was promoted to the position of Detective where he was assigned until 2005 when he began his current job with the NYS Police. Certifications: EnCase Certified Examiner: EnCase Access Data Certified Examiner: Access Data Level III Cellular Master Technician: Wild PCS Cellebrite UFED Logical Certified: Teel Technologies Cellebrite UFED Physical Certified: Teel Technologies XRY Certified: Micro Systemation

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
Kevin C. Kingsley	33%	BFOR 203 Networking & Cryptography	B.S. Siena College	Physics	Kevin Kingsley has very strong background in Computer Networking and has been working in the field over the last 10 years. Professional Experience: ITS-4 Information Security – Health Cluster: May 2016 – Present Experience: NYS ITS supporting Health Cluster networks, 44 Holland Avenue, Albany, N.Y. Operates multiple internal and external network scanning devices across multiple agencies and networks. Consolidates results and provides reporting with goal to both train people and remediate hardware and web application vulnerabilities. Uses technical and security experience to provide RFP responses and follow up. ITS-3 Data Communications – Enterprise ITS: Sep 2015 – May 2016 NYS ITS supporting DOCCS network, 50 Wolf Road, Albany, N.Y. Worked with multiple teams to establish network and application availability. Analyzed, recommended, and implemented network solutions to meet connectivity and access requirements. Maintained and updated network and project documentation. Presented formal

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
					and informal training to colleagues and customers. ITS-3 Information Security - Enterprise ISO Office: Aug 2014 – Sep 2015 NYS Enterprise ISO, Building 8, W. A. Harriman State Campus, Albany, N.Y. Collaborated with peers to develop a multi-layered and adaptive approach to counter a dynamic information security threat environment. As a member of the Secure Architecture/Secure Engineering Team, ensured the implementation, enhancement, and monitoring of secure enterprise-wide offerings. Documented security standards and guidelines. Promoted security and risk assessment awareness.
Kevin Salhoff	33%	BFOR 413 Multimedia Forensics BFOR 411 SCADA Forensics	B.S. RPI	Computer and Systems Engineering and Psychology	Extensive technical training and over 13 years’ experience in Cyber Crime, Digital Forensics and court testimony – Computer Crime Unit – NY State Police Certified trainer – NYS Police Professional Experience: Kevin is a 10-year civilian employee of the New York State Police. He has been in the computer forensics field since 2002. Prior to becoming an employee, Kevin worked with the New York State Police as an intern in the Quality Assurance office and consultant in the Computer Crime Unit. In his capacity as a Computer Forensic

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
					Analyst IV, he performs forensic analysis on computers and mobile devices, mentors and trains new employees, and develops software for use by the Computer Crime Unit. He also participates in search warrants when technical assistance is needed and provides support to the Computer Crime Unit field offices.
Sean Smith	33%	BFOR 402 eDiscovery Forensics and Moot Court	JD, Quinnipiac University, School of Law	Law	Over 20 years' legal experience and lecturer for the NYS Prosecutors Training Institute in trial preparation in cyber crime, electronic research, ethics, and technology. Professional Experience: Sean Smith has been an attorney with the New York Prosecutors Training Institute in Albany, New York since 1997 and was named Deputy Director in 2013. In this capacity, Sean assists NY's prosecutors with issues arising in felony cases, and assists prosecutors across the country by providing them with valuable information on expert witnesses. Sean actively helps prosecutors make better use of today's technology, and has been a part of NYPTI's always evolving online portfolio of legal resource tools including: Strike - Online Redaction Tool, Prosecutors' Encyclopedia, Prosecutors Case Management System (PCMS), Document Management Bridge,

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title and/or Rank at the Institution (Include and identify Program Director.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications and licenses and professional experience in field.**
					NYPTI CLE & Registration Online, CrimeTime Online, and NYPTI's Website.
William Augustine	16%	BFOR 419 System Administration and Operating System Concepts	MBA, School of Business, University at Albany, 12222	Master of Business	He has been a System Administrator for the University at Albany for over 20 years and has a deep knowledge of the relevant concepts. He is currently pursuing his Ph.D. in Information Science with a track of Information Security.
Part 3. To-Be-Hired Faculty (List as TBH1, TBH2, etc., and provide expected hiring date instead of name.)					

University at Albany
Program Revision
Digital Forensics

Appendix 1 Syllabi for New and Substantially Revised Courses

BFOR 204	Introduction to Cybersecurity
BFOR 205	Introduction to Database Systems
BFOR 206	Programming for Analytics
BFOR 305	Cyber Defense
BFOR 306	Database Security and Forensics
BFOR 400	Forensic Accounting and Fraud Detection
BFOR 402	eDiscovery Forensics and Moot Court
BFOR 403	Risk Analysis and Security Policies
BFOR 410	International Cyber Conflicts
BFOR 411	SCADA Forensics
BFOR 412	Cyber Incident Response and Penetration Testing
BFOR 413	Multimedia Forensics
BFOR 416	Advanced Data Analytics
BFOR 418	Assembly Language & Malware Reverse Engineering
BFOR 419	System Administration and Operating Systems Concepts
BFOR 420	National Cyber Security Challenge Problems

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

BFOR 204

Introduction to Cyber Security

Syllabus

BFOR 204 Introduction to Cyber Security
3 credits
M W 1:15 – 2:35
Instructor: Sanjay Goel

COURSE DESCRIPTION

This course provides you with foundation for future learning in information security. You will be exposed to information security terminology and concepts and apply them through labs and exercises throughout the course. First, you will be given a recap of networking concepts related to information system including the OSI/Internet models and TCP/IP protocol suite. Subsequently, you will learn of different threats and motivations as well as the types of cyberattacks. Attacks covered in the course include, malware, protocol based attacks (spoofing, session hijacking, caches poisoning, etc.), Denial-of-Service, and attacks on the web. Also included in this course, are psychological aspects of information security, vulnerabilities of computer networks and cyber warfare.

Prerequisite: BFOR 203

LEARNING OBJECTIVES

Overarching Goal: Learn of various information security threats as foundational elements to understand network security concepts.

Sub-Objectives: Student will learn how to:

1. Analyze and assess the motivations and goals of different adversaries in cyber attacks
2. Relate network threats to vulnerabilities in the TCP/IP network stack
3. Identify the attacks and the possible mechanisms of launching them
4. Understand psychological manipulations by hackers for social engineering attacks
5. Analyze cyber warfare in context of International Laws
6. Perform scholarly writing and research in the focused area of computer networks and information security.

TEXTBOOKS AND READINGS

INSTRUCTOR CONTACT

Type	Information	Availability
Email	goel@albany.edu	I will try to answer your questions within 24 hours. In case you feel that your email gets buried in my mailbox feel free to send a reminder.
Phone	(518) 956-8323 (Office) (518) 956-8333 (Lab) (518) 387-9090 (Goel Mobile)	Typically, I am in the office / lab from 8:30am (08:30) to 4:30 (16:30) EDT Mondays – Fridays when not in class or meetings. If unavailable I can generally be reached via mobile, but only in cases of dire emergency.
Secretary	Set up an appointment by phone or email.	Please stop by Jennifer North, in the Dean's Suite to set up an appointment in case you can't reach me.
Virtual Chat	Skype (goelsahib) Google Hangout/Chat (goelsa@gmail.com)	Times can be scheduled by phone or email for individuals or groups.

TECHNICAL RESOURCES

If you experience technical problems that interrupt your ability to complete class work, it's important that you know where to seek help immediately. Here is a simple guide for where you should direct questions and calls for help.

Problems with…	You should contact…
Logging into your ISP (Internet Service Provider); connecting to websites; launching web browser (e.g. Internet Explorer, Firefox)	Your ISP. The following links are provided to a couple of local ISP providers contact pages. If yours is not on this list, look up your ISP in a search engine and find a "Contact Us" page: Time Warner (Road Runner) & Verizon (FIOS)
Connecting & logging into to the UAlbany BLS website; accessing your course(s); interacting or participating in course activities, submission of assignment or file attachments in course.	The ITS Help Desk by using the ITS Help Request Form (http://www.albany.edu/its/help) or call (518) 442-4000. Press "1" for students. Then, press "2" for help with Blackboard.
Forgotten PIN when trying to get forgotten password.	The ITS HelpDesk at (518) 442-3700 or go to Lecture Center (LC) 27 at the UAlbany main campus with your SUNYCard and another form of identification. Press "1" for assistance when calling.

Please note that your instructor is not on this list. If you send inquiries about these technical problems, you will be referred to the resources listed above.

COURSE ACTIVITIES

Lectures / Readings: The course will feature assigned chapters, articles, or other PowerPoint readings as well as presentations.

Cases: Case studies using actual examples to provide real-world relevance to class topics.

Assignments: There will be several assignments in this class and you are expected to work alone or in teams as suggested in the assignment.

Hands-On Laboratory Exercises: Laboratory exercises will be offered where students get hands-on experience using tools and techniques in the field. Laboratory associated exercises take around 1 – 1 ½ hour to complete and will have associated questions for which your answers will be graded. Lab exercises will often require installation of software on computers and completing the corresponding exercises. At the end of the exercise, you should delete the software installed on the machines.

GRADING AND ASSESSMENT

The instructor will try to grade discussions, assignments, and exams fairly and return them within a reasonable time period with relevant comments and be available to discuss questions. Students are expected to set up an appointment to talk with the grader within a week of receiving a grade. Please let us know if there is a mistake in calculation – mistakes happen!

Late assignments, labs, or papers will receive 15% off per day late from the final possible grade for the exercise unless there is a legitimate excuse. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. Please also send any documentation to the instructor(s) as early as possible if you want to request any reasonable accommodations based on a disability.

Final grades will be graded on a curve using the following weightages. Based on the natural distribution of grades, students will be assigned final letter grades. Grading on a curve generally gives the person who performs the best in the class an “A” and other grades are decided based on their relative closeness to the score of the top performer and other students in the class.

Activity	Portion of Grade
Exam 1	25%
Exam 2:	25%
Assignments & Hands-On Laboratories	50%

The instructor is expected to get approval of the entire class prior to making any changes regarding the grading rubric.

COURSE SCHEDULE

Unit	Course Activities
Class 1	**Introductions, Getting Started, & Cyber Ethics** - Introduction to the Course - What is Information Security (CIA)? - Why is Information Security Important? - Adversaries: Motivations, Targets, and Techniques **Lab: Case Analysis**
Class 2	**Networking Primer** - Networking Fundamentals - Internet / OSI Model (Network Protocols, Addressing Scheme, Reliability / Congestion) - IPSEC / VPNs **Lab: Networking Lab**
Class 3	**Network Security Threats / Protocol Based Attacks** - IP Spoofing / Man-in-the-Middle - Session Hijacking & Buffer Overflow Attacks - Denial-Of-Service & Botnets - ARP Cache / DNS Poisoning - Wireless Security Protocols and Threats (MAC filtering) **Lab: Denial of Service Exercise**
Class 4	**Malware and Social Engineering Threats** - Malware (Viruses, Worms, Spyware, Adware, Trojans) - Email and Web Spoofing - Social Engineering & Psychology - Phishing, Spear Phishing - Protection against Malware **Lab: Malware Analysis (Due July 2)**
Class 5	**Web based Security Threats** I - Malicious HTML code and web attacks - Cookies, Web bugs and SpyWare - Code Injection - Cross-Site Scripting - Malicious Scripts - Trojan Downloaders - Watering Hole Attacks - Clickjacking **Lab: Code-Injection Attack**
Class 6	**Web based Security Threats** II - Cross-Site Scripting - Malicious Scripts - Trojan Downloaders - Watering Hole Attacks - Clickjacking **Lab: Cross-Site Scripting**

Class 7	**EXAM**
Class 8	**Software Vulnerabilities** - Genesis of the Problem - Software Security Threats - Emerging Software Security Threats **Lab Exercise: Buffer Overflow Attack**
Class 9	**Wireless Network Vulnerabilities** - Understanding wireless (WiFi) / Bluetooth protocols - Rogue Access Points (Evil Twin) - WEP Key Cracking - WAR Driving - MAC Spoofing - Eaves Dropping - Man-in-the-Middle **Lab Exercise: WEP Cracking**
Class 10	**Cloud Security Vulnerabilities** - Brief overview of Cloud Architecture - Failure of cloud services - Legal Issues and Data Sovereignty **Lab Exercise:**
Class 11	**SCADA Vulnerabilities** - Brief overview of SCADA systems - SCADA Vulnerabilities - Smart Grid, Connected Vehicles, Medical Devices **Lab Exercise: Research Project**
Class 12	**Insider Threats** - Motivations and Psychological Drivers of Malicious Insider - Insider data exfiltration cases - Detection of Insider Activity (surveillance and probes) **Lab Exercise: Ethics of Insider Threats**
Class 13	**International Cyber Warfare** - Nation States and Transnational Groups - Detection and Attribution - International Law and Applicability to Cyber Warfare **Lab Exercise: Case International Cyber Crime**
Class 14	**EXAM**

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of**

academic integrity." Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

“GREAT” EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.
- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

BFOR 205 Introduction to Databases

Instructor: Liyue Fan
Office: BB-346
Office Hours: MW 11:45AM-1:15PM or by appointment
E-mail: liyuefan@albany.edu

Prerequisites: BFOR 100
Credits: 3
Meets: T TH 4:15PM-5:35 PM, BB121

Textbook:

- "Modern Database Management (12th ed.)," Jeffrey A. Hoffer, V. Ramesh and Heikki Topi. Prentice Hall (Pearson Educational), 2015.

Sample external readings (can expand to include most recent research):

- T. F. Lunt, "Aggregation and inference: facts and fallacies," *Proceedings. 1989 IEEE Symposium on Security and Privacy*, Oakland, CA, 1989, pp. 102-109.
- B. MACQ, J. DITTMANN and E. J. DELP, "Benchmarking of image watermarking algorithms for digital rights management," in *Proceedings of the IEEE*, vol. 92, no. 6, pp. 971-984, June 2004.
- Muhammad Naveed, Seny Kamara, and Charles V. Wright. 2015. Inference Attacks on Property-Preserving Encrypted Databases. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15).

Course Objectives

This course introduces principles and techniques for managing data resources, covering the functions of Relational Database Management Systems (RDBMS), and their use. Specifically, students will be able to:

- Describe fundamental data and database concepts
- Create databases and database objects using popular database management systems, e.g., MySQL
- Solve problems by constructing database queries using Structured Query Language (SQL)
- Design databases using ER and relational modeling and data normalization techniques
- Develop insights into advance database topics and technique trends for digital forensics applications, such as security and applied systems.

Course Topics

Topic	Reading	Activity
Conceptual Design	Ch 2 & 3	ER model lab, HW1
Logical Design & Normalization	Ch 4	Relational model lab, HW2
SQL and Advanced SQL	Ch 6 & 7	MySQL lab, HW3
Database Security	Ch 12	Authorization lab
Security Issues in Inference and Aggregation	Research papers	Presentations
Applied Systems	Research papers	Presentations

Grading

In-Class Quizzes and Lab Activities	14%
Assignments	24%
Presentations	6%
Term Project	29%
Midterms (First @12%, Second @15%)	27%

Class Participation:
Class participation be based upon involvement in quizzes and activities. Additionally, students will work in groups and present their solutions on whiteboard. (individual/group work)

Assignments:
Three assignments will be announced throughout the course. You will turn in computer generated output from your work. (individual work)

- HW1: ER model in draw.io
- HW2: Relational data model in draw.io
- HW3: SQL queries in MySQL

Midterms:
There will be two midterm tests where you will perform data modeling, SQL, and data analysis. (individual work)

Presentations:
Students will read extended materials, e.g., most recent research papers, on topics in statistical inference control, data analysis, and applied systems, such as spatial databases and multimedia databases. Student will present the read materials to the class. (individual work)

Project:
The term project will be the "cap stone" of the semester and requires the design of a database application and the implementation of this design using a database management system. The project will apply most of the issues/concepts covered during the semester and will enable you to obtain first-hand experience in designing and implementing a basic DBMS application using MySQL. It will be your responsibility to find a suitable project. (group work)

Grade Scale	**Conversion**	**Grade Scale**	**Conversion**
93-100	A	73-76	C
90-92	A-	70-72	C-
87-89	B+	67-69	D+
83-86	B	63-66	D
80-82	B-	60-62	D-
77-79	C+	< 60	E

Academic Integrity & Honesty

Students MUST comply with all **University at Albany's standards of academic integrity**. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor, submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

Syllabus

BFOR 206
Programming for Security Analytics (3 credits)

Course Description

In this course, students will learn the principles scripting that are necessary for cybersecurity professionals. Scripting will be learned that is useful for penetration testers and security analysts alike. Linux Shell Scripting and PowerShell scripting will be covered, as well as the use of Python for Offensive Security.

Class Time and Location: This class has yet to be scheduled. As a 3 credit course, it will meet either 3 times per week for one hour or two times per week for 90 minutes.

Instructor: Lee Spitzley
Office Hours: TBD

Website: Blackboard will be used to provide essential course materials, the most current syllabus, and assignments. No separate course website will be maintained.

Prerequisites: BFOR 100 Introduction to Information Systems, BFOR 203 Networking and Cryptography
This course will build upon your existing knowledge of Python, Information Systems, and Networking.

Required Textbooks:
Advanced Bash-Scripting Guide: An in-depth exploration of the art of shell scripting
Public Domain 2014
Mendel Cooper
http://www.tldp.org/LDP/abs/abs-guide.pdf

Getting Started with Microsoft PowerShell
Public Domain 2016
James E. Jarvis
http://www.docs.is.ed.ac.uk/skills/documents/3835/3835.pdf

Black Hat Python: Python Programming for Hackers and Pentesters 1st Edition
Copyright 2014
Justin Seitz
ISBN-10: 1593275900
ISBN-13: 978-1593275907

Supplemental readings will be distributed via Blackboard and/or in class.

Attendance

Attendance is mandatory for every class. Your in-class performance is key to your success in this course. Attendance, itself, is not graded. Instead, graded in-class activities and assignments constitute an important part of the course grade. It is unlikely you can maintain a passing average without consistent attendance. Missing class means the student earns an automatic zero for the activities or assignments missed. Because of the nature of the assignments, no make-up opportunities will be available.

Tardiness
Missing an assignment or activity that happened before a student arrives or after a student leaves also earns a zero. No make-up opportunities will be available.

If you know that it will be difficult for you to consistently get to class on time and stay for the entire period, you should take this course at a time that better fits your schedule. Being late frequently will likely negatively impact your grade for the course.

Withdrawal from the course
The drop date for the ???? semester is ???? for undergraduate students. That is the last date you can drop a semester length course and receive a 'W'. It is your responsibility to take action by this date if you wish to drop the course. In particular, grades of "incomplete" will not be awarded to students because they missed the drop deadline.

All important dates can be found in the University academic calendar, which is available online : http://www.albany.edu/registrar/????-academic-calendar.php

Academic Integrity
It is every student's responsibility to become familiar with the standards of academic integrity at the University. Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity. See http://www.albany.edu/undergraduate_bulletin/regulations.html

Course work and examinations are considered individual exercises. Copying the work of others is a violation of university rules on academic integrity. Individual course work is also key to your being prepared and performing well on tests and exams. Forming study groups and discussing assignments and techniques in general terms is encouraged, but the final work must be your own work. For example, two or more people may not create an assignment together and submit it for credit. If you have specific questions about this or any other policy, please ask.

The following is a list of the types of behaviors that are defined as examples of academic dishonesty and are therefore unacceptable. Attempts to commit such acts also fall under the term academic dishonesty and are subject to penalty. No set of guidelines can, of course, define all possible types or degrees of academic dishonesty; thus, the following descriptions should be understood as examples of infractions rather than an exhaustive list.

- Plagiarism
- Allowing other students to see or copy your assignments or exams

- Examining or copying another student's assignments or exams
- Lying to the professor about issues of academic integrity
- Submitting the same work for multiple assignments/classes without prior consent from the instructor(s)
- Getting answers or help from people, or other sources (e.g. research papers, web sites) without acknowledging them.
- Forgery
- Sabotage
- Unauthorized Collaboration (just check first!)
- Falsification
- Bribery
- Theft, Damage, or Misuse of Library or Computer Resources

Any incident of academic dishonesty in this course, no matter how "minor" will result in:
1. No credit for the affected assignment.
2. A written report will be sent to the appropriate University authorities (e.g. the Dean of Undergraduate Studies)

And may result in:
3. One of –
   o A final mark reduction by at least one-half letter grade (e.g. B →B-, C- →D+),
   o A Failing mark in the course, and referral of the matter to the University Judicial System for disposition.

Policies from Undergraduate Bulletin:
http://www.albany.edu/undergraduate_bulletin/regulations.html

Responsible Use of Information Technology
Students are required to read the University at Albany Policy for the Responsible Use of Information Technology available at the ITS Web Site:
https://wiki.albany.edu/display/public/askit/Responsible+Use+of+Information+Technology+Policy

Available Support Services - Reasonable accommodation
Reasonable accommodation will be provided for students with documented physical, sensory, cognitive, learning and psychiatric disorders. If you believe you have a disability requiring accommodation in this class, please notify the Disability Resource Center (CC130, 442-5490). That office will provide the course instructor with verification of your disability, and will recommend appropriate accommodations. In general, it is the student's responsibility to contact the instructor at least one week before the relevant assignment to make arrangements.

Missing Deadlines Due to Illness
Please be familiar with the University rules regarding missing deadlines due to health:
http://www.albany.edu/health_center/medicalexcuse.shtml

Assessment: By default, this is an A-E graded course.
Your achievement of these objectives will be assessed through in-class activities, assignments

and exams. Material submitted late without prior approval will be penalized 20% for every day or part thereof.

COURSE SCHEDULE

Date	Topics	Readings
Week 1	Bash Scripting Basics	ABS Chapters 1-6
Week 2	Testing and Operations	ABS Chapter 7-8
Week 3	Variables	ABS Chapters 9-10
Week 4	Loops	ABS Chapters 11-14
Week 5	Functions	ABS Chapter 24
Week 6	PowerShell Week 1	Getting Started with Microsoft PowerShell
Week 7	PowerShell Week 2	
Week 8	PowerShell Week 3	
Week 9	Python and Networks 1: Network Basics	Black Hat Chapters 2-3
Week 10	Python and Networks 2: Python for Network Attacks	Black Hat Chapter 4-5
Week 11	Burp Suite	Black Hat Chapter 6
Week 12	Windows Trojans	Black Hat Chapters 8-9
Week 13	Windows Privilege Escalation	Black Hat Chapter 10
Week 14	Automation of Offensive Forensics	Black Hat Chapter 11
Finals Week	*Final Exam*	

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, either announced in-class or through email.

Grading
This class will feature daily assignments as a part of the class structure. Each class activity will feature an equal weighting. As a safety net, your three lowest

class assignment grades will be dropped. You are expected to come to class prepared, which includes reading prior to class.

Assignments:

HW 1: Bash Scripting Assignment – Bash scripting is essential for automating tasks in Unix environments. For this assignment you will be tasked with picking a task to automate and writing a script to automate its actions.

HW 2: Python for Network Analysis – In this assignment you will be tasked with using Python to interact with TCP/IP Networks and analyze the results.

Final Project: Offensive Programming – Create a Python program to automate an offensive security task.

UALBANY SUNY | BFOR 305 Cyber Defense and Secure Communications Syllabus

BFOR 305 Cyber Defense and Secure Communications

Semester: **Fall 2017**
Classroom**: Business Building, #123**
Day & Time: **Tuesdays, 05:45 PM - 08:35 PM**
Credit Hours: **3**
Grading Scheme: **A-E**

Instructor: **Dr. Devi Bhattacharya**
Office: **Business Building, #325**
Office Hours: **Mondays, 12 pm – 1 pm or by appointment**
Email: dbhattacharya@albany.edu
Phone: (518) 956-8335

CLASS DESCRIPTION

This course provides you with a deep dive into cyber security tools. Topics covered in this class include techniques for protecting networks and data, basic elements of symmetric and asymmetric cryptography, secure e-commerce, secure transmission, authentication, digital signatures, digital certificates and Public Key Infrastructure (PKI). The course will also discuss current legislation and standards related to information security and their relevance to the international workplace.

PREREQUISITE BFOR 204 Introduction to Cyber Security

LEARNING OBJECTIVES

Overarching Goal: Gain a foundation in information security to work towards and discuss the protection of IT infrastructure.

Sub-Objectives: Students will learn how to:

1. Deploy and configure tools for ensuring network and data security.
2. Relate network threats to vulnerabilities in the TCP/IP network stack.
3. Read and interpret log files.
4. Learn and apply cryptographic concepts to security e.g., confidentiality, integrity, availability.
5. Critically think via debates on the ethical and legal issues related to information security.
6. Perform scholarly writing and research in the focused area of computer networks and information security.

TEXT

Security in Computing (5th Edition), Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies
Prentice Hall; 5 edition (February 5, 2015), ISBN-10: 0134085043

COURSE ACTIVITIES

- **Lectures / Readings:** The course will feature assigned chapters, articles, or other PowerPoint readings as well as presentations.
- **Cases:** Case studies using actual examples to provide real-world relevance to class topics.
- **Assignments:** There will be several assignments in this class and you are expected to work alone or in teams as suggested in the assignment.
- **Hands-On Laboratory Exercises:** Laboratory exercises will be offered where students get hands-on experience using tools and techniques in the field. Laboratory associated exercises take around 1 – 1 ½ hour to complete and will have associated questions for which your answers will be graded. Lab exercises will often require installation of software on computers and completing the corresponding exercises. At the end of the exercise, you should delete the software installed on the machines.

GRADING AND ASSESSMENT

- The instructor will try to grade discussions, assignments, and exams fairly and return them within a reasonable time period with relevant comments and be available to discuss questions.
- Students are expected to set up an appointment to talk with the grader within a week of receiving a grade. Please let me know if there is a mistake in calculation – mistakes happen!
- Assignments and Hands-On Laboratories can be individual or group based. In case they are group based, the group grade will be considered as the grade of the individual team members.
- Late assignments, labs, or papers will receive 15% off per day late from the final possible grade for the exercise unless there is a legitimate excuse.
- Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. Please also send any documentation to the instructor(s) as early as possible if you want to request any reasonable accommodations based on a disability.
- Final grades will be graded on a curve using the following weightages. Based on the natural distribution of grades, students will be assigned final letter grades. Grading on a curve generally gives the person who performs the best in the class an "A" and other grades are decided based on their relative closeness to the score of the top performer and other students in the class.

Activity	Portion of Grade
Exam 1	25%
Exam 2:	25%
Assignments & Hands-On Laboratories	50%

The instructor is expected to get approval of the entire class prior to making any changes regarding the grading rubric.

TECHNICAL RESOURCES

If you experience technical problems that interrupt your ability to complete class work, it's important that you know where to seek help immediately. Here is a simple guide for where you should direct questions and calls for help.

Problems with…	You should contact…
Logging into your ISP (Internet Service Provider); connecting to websites; launching web browser (e.g. Internet Explorer, Firefox)	Your ISP. The following links are provided to a couple of local ISP providers contact pages. If yours is not on this list, look up your ISP in a search engine and find a "Contact Us" page: Time Warner (Road Runner) & Verizon (FIOS)
Connecting & logging into to the UAlbany BLS website; accessing your course(s); interacting or participating in course activities, submission of assignment or file attachments in course.	The ITS Help Desk by using the ITS Help Request Form (http://www.albany.edu/its/help) or call (518) 442-4000. Press "1" for students. Then, press "2" for help with Blackboard.
Forgotten PIN when trying to get forgotten password.	The ITS HelpDesk at (518) 442-3700 or go to Lecture Center (LC) 27 at the UAlbany main campus with your SUNYCard and another form of identification. Press "1" for assistance when calling.

Please note that your instructor is not on this list. If you send inquiries about these technical problems, you will be referred to the resources listed above.

TENTATIVE COURSE CALENDAR

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

COURSE CONTENT	
Unit	Course Activities
1	**Introduction to the Course** - CIA Triad and Mission Assurance Strategy - IT Management – Patches, procedures and policy - Defense in Depth Strategy & Secure Network Design - Network Attacks – DDoS, Cross-Site Request Forgery, Buffer Overflow, Code Injections, Insider Threats - Malicious Software (Standalone, Host-Dependent) and Antivirus **Reading**: The 60-minute Network Security Guide, pages 6-10, Chapter 10 - Textbook **Lab: Hardening the computer system – Patches application** - Setup of Kali VM, Metasploitable VM, Windows VM - Hardening a Windows 8 machine - Hardening a Debian (Linux Machine) - Role of Windows Antivirus
2	**Vulnerability Scanning and Threat Analysis** - Deploying VS tools - Running VS tools for scanning - Analyzing Results from VS - Cobalt Strike and Penetrating Testing **Lab: Using Nmap, Nessus for Vulnerability Scanning** **Homework:** Students using the Kali Machine to Analyze vulnerabilities in Metasploitable VM
3	**Authentication, Authorization and Access Control – Operational Hardening** - Password Storage & Authentication, Introduction to Hashes - Password Security Threats (Dictionary, Brute-force, guessing) & Controls (Single Sign-On, etc.) - Biometrics - Security Models (Biba, Bell-La Padula Clark-Wilson) - User Privileges / Security Classifications - Types of Access Control (Role-based, Rule-based, Discretionary,

	Mandatory) **Reading**: Encyclopedia of Cryptography – Access Control - Pages 3-17, Authentication – Pages 61-63, Authorization – Pages 65-67 **Lab**: Password Cracking on Kali (John the Ripper). Discussion on using shadow password files on Linux. Students are given demonstration of comparison of hash signatures and time complexity of hash algorithms. **Homework** – Students research real world scenarios that demonstrate how authentication, authorization and access controls were compromised to cause harm to systems
4	**Network Hardening** - Firewalls – Iptables and Windows - Whitelisting vs. Blacklisting - Intrusion Detection Systems – Network and Host-Based - Honeynets, Sandboxing & Introduction to Darknets **Lab: Introduction to SNORT, Iptables and KeyFocus (HoneyPot) for Windows Demonstration** **Reading**: Encyclopedia of Cryptography – Firewall pages 471 – 474, Chapters -11, 12 Textbook **Homework:** Configuration of Windows Firewall (Windows VM) and Iptables tests (Kali and Metasploitable VMs) and building SNORT rules. Students submit screen shots and complete a lab sheet describing their learnings.
5	**Web Applications and Network Communications** - Understanding HTTP, GET and POST and Web Server Attacks - Designing Secure Websites - Secure Session Management with Cookies - SSL/TLS and HTTPS – Introduction to Public Key Infrastructure and Key Exchange - Virtual Private Networks - IPSec **Readings – Encyclopedia of Cryptography: SSL -1135 -1138, IPSec – 635-638, Sandboxing 1075-1078, Cookie Pages 254-256, Chapter 6, 9 – Textbook** **Lab: SSH from Linux to Linux (Kali to Metasploitable), Using Wireshark for SSH Traffic Analysis, SSH from Windows to Linux (Putty), Wireshark for Traffic Analysis** **Homework: Students write down the sequence of events (using Wireshark) during establishment of SSL connection.**

6	**Cryptography – Part I** **- Cryptography Basics** **- Symmetric Encryption Algorithms Overview - Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard** **- Diffie Hellman Key Exchange** **Lab: Using Python module pycrypto, cryptography to simulate symmetric encryption algorithms.** **Readings: Textbook – Chapter 2, Chapter 4 (Pages 123-124)**
7	**Cryptography – Part II** - **Message Digests & Message Authentication Codes** - **Public Key Infrastructure (PKI) -Authentication and Confidentiality** - **El-Gamal and RSA Algorithms** - **Digital Signatures & Digital Certificates** - **Hashing** - **Certificate Authorities** **Homework – Asymmetric Cryptographic Problems Using Modulus Arithmetic** **Readings – Textbook Chapter 3, Chapter 4 (Pages 137-139, 146-149)** **Lab: Viewing digital certificates for SSL in Kali Machine. Using Python module pycrypto, cryptography to simulate asymmetric encryption algorithms.**
8	**Programming Security in a Client-Server Architecture** - Program Content Locations - Functionality Used, Application Type and Point of Entry - Client-Side Controls - Authentication Mechanisms - Session Management - Revisiting Program related attacks – Code Injection, Cross Site Forgery, Semantic Attacks, Logic Bombs **Reading:** Source Code Analysis Tools - https://www.owasp.org/index.php/Source_Code_Analysis_Tools The OWASP Source Code Flaws Top 10

	https://www.owasp.org/index.php/OWASP_Source_Code_Flaws_Top_10_Project_Index OWASP Secure Coding Practices - Quick Reference Guide https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf **Lab:** Using Bandit Software to Analyze program security
9	**Malware** - Types of Malware with focus on rootkits, crime ware kits, spyware - Common attack vectors of Malware (Social Engineering, Fake Software, Pretending Through Email) - Understanding Malware code and building malware testbed - Introduction to HEX editors - Malware Analysis (Static and Dynamic Analysis) **Readings: Practical Malware Analysis - Black Hat** https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Presentation/bh-dc-07-Kendall_McMillan.pdf **Lab: Malware Labs Using Windows XP - to view code injections and hooking**
10	**Log Analysis** - Understanding Operating Systems (Linux / Windows) - Analyze individual log files - Analyze multiple log files - Using data aggregation and Visualization Tools **Project:** Data Collection and Log Analysis for Windows - Nirsoft for data collection. Students use the various VM snapshots of Malware Lab to generate detailed system logs **Homework –** Students use Tableau to visualize and analyze the data. Students analyze the log files from the Malware files to build a comprehensive story of the attack**.**
11	**Attack Trees** - Understanding the structure of trees - Developing Attack Trees **Reading**: Using Attacks to identify Malicious attacks from insiders - **Lab: Develop Attack Trees for given scenario**
12	**Ethics & Cyber Security** - Whitehat vs. Blackhat Hacking **Assignment: Ethics Case**

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. For a detailed description of what the standards of academic integrity are, please visit the webpage at http://www.albany.edu/undergraduateeducation/academic_integrity.php

As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Dean of Undergraduate Studies Office AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

"GREAT" EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.
- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

Syllabus

BFOR 306
Database Security and Forensics (3 credits)

Course Description
In this course, students will learn the principles of database security, as well as the processes necessary to forensically audit a database across a range of industry standard database management systems. The attack vectors on a database, including SQL injection will also be covered as well. Finally, students will learn techniques and strategies for conducting penetration tests against a database.

Class Time and Location: This class has yet to be scheduled. As a 3 credit course, it will meet either 3 times per week for one hour or two times per week for 90 minutes.

Instructor: Liyue Fan
Office Hours: TBD

Website: Blackboard will be used to provide essential course materials, the most current syllabus, and assignments. No separate course website will be maintained.

Prerequisites:
BFOR 204 Introduction to Cyber Security
BFOR 205 Introduction to Database Systems

Course Goals

By the end of the semester, you should be able to
1. Identify ways to securely configure a database
2. Understand what SQL injection is and how to prevent it
3. How do perform a forensic examination of a database
4. How to test a database's security

Required Textbook:
Database Security 1st Edition
Copyright 2011
Alfred Basta | Melissa Zgola
ISBN-10: 1435453905
ISBN-13: 978-1435453906

Supplemental readings will be distributed via Blackboard and/or in class.

Attendance

Attendance is mandatory for every class. Your in-class performance is key to your success in this course. Attendance, itself, is not graded. Instead, graded in-class activities and assignments constitute an important part of the course grade. It is unlikely you can maintain a passing average without consistent attendance. Missing class means the student earns an automatic zero for the activities or assignments missed. Because of the nature of the assignments, no make-up opportunities will be available.

Tardiness

Missing an assignment or activity that happened before a student arrives or after a student leaves also earns a zero. No make-up opportunities will be available.

If you know that it will be difficult for you to consistently get to class on time and stay for the entire period, you should take this course at a time that better fits your schedule. Being late frequently will likely negatively impact your grade for the course.

Withdrawal from the course

The drop date for the **????** semester is **????** for undergraduate students. That is the last date you can drop a semester length course and receive a 'W'. It is your responsibility to take action by this date if you wish to drop the course. In particular, grades of "incomplete" will not be awarded to students because they missed the drop deadline.

All important dates can be found in the University academic calendar, which is available online : http://www.albany.edu/registrar/????-academic-calendar.php

Academic Integrity

It is every student's responsibility to become familiar with the standards of academic integrity at the University. Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity. See http://www.albany.edu/undergraduate_bulletin/regulations.html

Course work and examinations are considered individual exercises. Copying the work of others is a violation of university rules on academic integrity. Individual course work is also key to your being prepared and performing well on tests and exams. Forming study groups and discussing assignments and techniques in general terms is encouraged, but the final work must be your own work. For example, two or more people may not create an assignment together and submit it for credit. If you have specific questions about this or any other policy, please ask.

The following is a list of the types of behaviors that are defined as examples of academic dishonesty and are therefore unacceptable. Attempts to commit such acts also fall under the term academic dishonesty and are subject to penalty. No set of guidelines can, of course, define all possible types or degrees of academic dishonesty; thus, the following descriptions should be understood as examples of infractions rather than an exhaustive list.

- Plagiarism
- Allowing other students to see or copy your assignments or exams
- Examining or copying another student's assignments or exams
- Lying to the professor about issues of academic integrity
- Submitting the same work for multiple assignments/classes without prior consent from the instructor(s)
- Getting answers or help from people, or other sources (e.g. research papers, web sites) without acknowledging them.
- Forgery
- Sabotage
- Unauthorized Collaboration (just check first!)
- Falsification
- Bribery
- Theft, Damage, or Misuse of Library or Computer Resources

Any incident of academic dishonesty in this course, no matter how "minor" will result in:
1. No credit for the affected assignment.
2. A written report will be sent to the appropriate University authorities (e.g. the Dean of Undergraduate Studies)
And may result in:
3. One of –
    o A final mark reduction by at least one-half letter grade (e.g. B →B-, C- →D+),
    o A Failing mark in the course, and referral of the matter to the University Judicial System for disposition.

Policies from Undergraduate Bulletin:
http://www.albany.edu/undergraduate_bulletin/regulations.html

Responsible Use of Information Technology
Students are required to read the University at Albany Policy for the Responsible Use of Information Technology available at the ITS Web Site:
https://wiki.albany.edu/display/public/askit/Responsible+Use+of+Information+Technology+Policy

Available Support Services - Reasonable accommodation
Reasonable accommodation will be provided for students with documented physical, sensory, cognitive, learning and psychiatric disorders. If you believe you have a disability requiring accommodation in this class, please notify the Disability Resource Center (CC130, 442-5490). That office will provide the course instructor with verification of your disability, and will recommend appropriate accommodations. In general, it is the student's responsibility to contact the instructor at least one week before the relevant assignment to make arrangements.

Missing Deadlines Due to Illness
Please be familiar with the University rules regarding missing deadlines due to health:
http://www.albany.edu/health_center/medicalexcuse.shtml

Syllabus

Assessment: By default, this is an A-E graded course.
Your achievement of these objectives will be assessed through in-class activities, assignments and exams. Material submitted late without prior approval will be penalized 20% for every day or part thereof.

COURSE SCHEDULE

Date	Topics	Readings	Assignments	
			Given	Due
Week 1	Databases and Security	Chapters 1,2		
Week 2	MySQL Database Security	Chapter 3	HW 1	
Week 3	MySQL Database Security			
Week 4	SQL Server Database Security	Chapter 4		HW 1
Week 5	SQL Server Database Security		HW 2	
Week 6	Oracle Database Security	Chapter 5		
Week 7	***First Exam***			
Week 8	Password Management	Chapter 6		HW 2
Week 9	SQL Injection	Chapter 7	HW 3	
Week 10	SQL Injection	Chapter 8		
Week 11	Database Forensics - MySQL	Chapter 9	Final Project	HW 3
Week 12	Database Forensics -SQL Server		HW 4	
Week 13	Database Security Testing	Chapter 10		HW 4
Week 14	Database Security Testing			Final Project
Finals Week	***Second Exam***			

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, either announced in-class or through email.

HW Project #1: Secure deployment of a database in MySQL.
HW Project #2: Secure deployment of a database in SQL Server
HW Project #2: SQL injection activity on hackthissite.com.
HW Project #3: Penetration test on a model database.
Final Project: Database forensics project with report and presentation.

GRADING RUBRIC		
Type	**% of Grade**	**Description**
2 Exams	40%	Two exams worth 20% each.
Homework Assignments	40%	There will be 3 assignments. The lowest grade will be dropped leaving four submissions (worth 10% of the total grade each). Late submissions will be penalized 20% of the assignment grade per day or part thereof.
Final Project	20%	Various assessments that may include short (unannounced) quizzes based on the text and/or additional readings or directed in-class activities.

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

BFOR 400

Forensic Accounting & Fraud Examination

Instructor:	Victoria Kisekka, PhD
Office Location:	Business Building 371
Office Hours:	Mondays and Wednesdays – 3pm to 4:30 pm Or by appointment
E-mail:	vkisekka@albany.edu
Telephone:	956-8361

COURSE

BFOR 400 Forensic Accounting and Fraud Examination (3 credits)
Fall 2017 Semester: Mondays & Wednesdays 11:45am -1:05pm in BB 368
Mondays & Wednesdays 1:15 pm - 2:35pm in BB 205
Verify that you are in the correct section by checking your UAlbany.
Each student must attend the section they officially registered for. No exceptions!
Course Prerequisite(s): BACC 211 (Financial accounting)

COURSE DESCRIPTION

This course provides an overview of occupational fraud including misappropriation of assets, financial statement fraud and corruption as well as other forensic accounting engagements. The course will explore the characteristics of specific fraud schemes along with the characteristics of those who perpetrate them (according to the Annual Report to the Nations compiled by the Association of Certified Fraud Examiners). Students will acquire an understanding of how fraudulent conduct can be deterred and how cases of fraud should be investigated and solved.

LEARNING OBJECTIVES

The course will teach students to detect and investigate accounting fraud. After completing this course, you should be able to:

1. Define fraud
2. Identify the different types of fraud schemes and ways in which they are concealed
3. Understand various roles undertaken by forensic accountant examiners, as well as the requirements for obtaining certifications
4. Identify internal controls and other methods that can be used to deter fraud.
5. Describe and practice “professional skepticism”
6. Investigate fraud cases to identify the perpetrators, evaluate amount of damage, and suggest recommendations for preventing fraud
7. Reviewing documentary evidence and using inferences to draw conclusions
8. Understand how to effectively conduct interviews

COURSE RESOURCES

Type	Information
Course Website	https://blackboard.albany.edu/ (All announcements will be communicated through blackboard).
Textbook(s)	Forensic Accounting and Fraud Investigation for Non-Experts, 3rd Edition by Stephen Pedneault; Frank Rudewicz; Howard Silverstone; Michael Sheetz Publisher: John Wiley & Sons ISBN -13: 9780470879597
Reference Books(s) - optional	Principles of fraud examination, 4th edition by Joseph T. Wells. Case Studies in Forensic Accounting and Fraud Auditing, 1E Publisher: Wolters Kluwer

COURSE ACTIVITIES

Active Learning: In order to reinforce mastery of the material, I will promote active learning in the classroom. An active learning environment is where students are involved and highly engaged in the learning process other than simply acquiring knowledge passively. As part of this strategy, you are expected to read the textbook and assigned readings before class. PowerPoint slides are only intended to facilitate classroom discussion and also communicate additional relevant information not covered in the required textbook. For this reason, PowerPoint slides based on textbook material will be posted to Blackboard after class unless otherwise communicated. You are expected to take notes during the lectures.

Reading: The readings in this course are not an end in themselves, but rather, the material you read will be used for in-class discussions, assignments, and even writing. Some of the forensic accounting and fraud examination concepts in the readings are complex, and will require persistence on your part. In order for you to be productive in the in-class activities, you will need to prepare before class and come to class ready to discuss.

Lectures: Instructor-led lectures that may be supplemented with expert guest lectures on course-related topics will be offered in class. The lecture material should summarize and expand on the knowledge obtained from the assigned readings and assignments.

Classroom participation and discussions: Students are expected to participate in classroom discussions in an insightful manner. Part of your participation grade will be based on your involvement in in-class discussions. Discussions topics and/or questions may also be assigned and graded. Obtaining the maximum contribution in the class occurs when students consistently join the discussion and offer opinions. Contribution in one single class or some of the classes does not equate to maximizing the points available. You will be evaluated on the QUALITY of your contributions and insights. Quality comments possess one or more of the following properties:

- Offers a different and unique, but relevant, perspective;
- Contributes to moving the discussion and analysis forward;
- Builds on other comments;
- Transcends the “I feel” syndrome. That is, it includes some evidence, argumentation, or recognition of inherent tradeoffs. In other words, the comment demonstrates some reflective thinking.

While your classroom participation grade is subjective, it will not be random or arbitrary. And, clearly, more frequent quality comments are better than less frequent quality comments.

Homework Assignments: Several assignments will be given during the semester. These will include take-home assignments or in class exercises. Completed assignments should be handed in by the time and date specified on blackboard, on the course schedule or verbally communicated during class.

Assignments that are one day late will be reduced by 20%
Assignments that are two days late will be reduced by 40%
Assignments that are three days late will be reduced by 60%
Assignments that are more than three days late will be given no credit unless when there is a legitimate excuse for the lateness.

Missed assignments will receive no credit unless there is a legitimate excuse for not completing the assignment. When an assignment is missed due to a legitimate excuse, it must be made up at a time specified by the instructor or the grade of “0” is recorded. Legitimate excuses include illnesses requiring professional attention and personal or family emergencies. It is the responsibility of the student to initiate 1) a consultation with the instructor regarding a missed assignment in a timely fashion (within 2 class periods) and 2) to present verifiable written documentation. It is the responsibility of the student to keep a record of missed assignments and work that must be made up. To obtain the required documentation for absences, visit the office of the Provost for Undergraduate Education. The contact information for this office and more details can be found here http://www.albany.edu/undergraduateeducation/attendance.php

If you become seriously ill during the semester, or become derailed by unforeseeable life problems, and have to miss so many assignments that will ruin your grade, you and the instructor will schedule a special meeting in order to make arrangements for you to withdraw from the course with the documentation needed to try to save your grade point average. Do not wait until it's too late to arrange this meeting if you see that you are getting in trouble.

Attendance: Your in-class performance is crucial to your success in this course. Attendance itself is not graded, but there will be graded in-class activities, such as quizzes and **opportunities**. *Opportunity is used to refer to any unannounced graded in-class activity. These may include but are not limited to writing assignments, group activities, individual activities, etc.* Keeping a passing average on these is not possible without consistent attendance. Missing class means earning an automatic "0" for the activities or assignments missed. The lowest score of the graded in-class assignments (i.e., quiz or opportunity) will be dropped. Because the lowest score of a quiz or opportunity is dropped, if you miss a quiz or opportunity, it will be the quiz or opportunity score that is dropped. For example, if we have 5 graded in class assignments consisting of quizzes and opportunities, your lowest score of the 5 assignments will be dropped.

No make-up assignments will be available for in-class activities except in documented cases of extreme extenuating circumstances. For an approved absence, the student will be given a makeup graded assignment by the instructor within one week of the original assignment date. To obtain the required documentation for absences, visit the office of the Provost for Undergraduate Education. The contact information for this office and more details can be found here http://www.albany.edu/undergraduateeducation/attendance.php.

Lateness-Tardiness Policy: Missing an assignment or activities that happened at the beginning of class before you arrive or at the end of class after you leave early will also earn a "0", and there will be no make-up assignments. *If you know that it will be difficult for you to consistently get to* *class on time and stay for the entire period, you should drop this course and take it at a later date, when your life's circumstances are more manageable.*

Cell Phone Policy: Please show respect for you fellow students by making sure your cell phone is turned off or is in a silent mode (e.g., vibrate or do not disturb) before entering the classroom.

EMAIL ETIQUETTE

This is a business school and I whole heartedly believe that some behaviors become habits. All of you aspire to have successful carriers and as part of your training, communication is key. All your emails to me must be professional. I will try to respond to all emails within 24 hours. Here are some guidelines for writing professional emails.

1.Your email should start with a proper salutation. E.g., Dear or Hi Dr. Last name, Dear or Hi Professor Last name. **Emails that do not open with a proper salutation will not be read**. I typically assume that the email was not intended for me.
2. Use proper grammar, spelling, and punctuation. Refrain from using slangs and acronyms such as LOL, ROFL, BTW, ASAP, TTYL, IMO, ION, etc. Do not use ALL CAPITAL LETTERS. The assumption here is that you are yelling at the recipient.
3. Never leave the subject line blank.
4. Your email should end with a proper signature. Provide your full name at the end of the email.
5. Be respectful. Avoid intimidating emails. And remember, your email message shapes the recipient's professional impression about you.

OFFICE HOURS: Don't be a stranger! Take advantage of my scheduled office hours to go over material you do not understand. I am here to help you.

EXAMS: Three exams will be offered. Exams are to be completed in the classroom on the date and time specified on the course schedule. The content of these exams will be based on the material in the textbook, other assigned readings, and in-class discussions. There will be no final exam. Exams must be completed on the communicated date. No make up exams shall be given except in cases of extreme extenuating circumstances. To obtain the required documentation for absences, visit the office of the Provost for Undergraduate Education. The contact information for this office and more details can be found here http://www.albany.edu/undergraduateeducation/attendance.php

Note: If you request your exam to be reviewed for errors, the instructor will independently evaluate the exam. Exam scores can increase, decrease, or remain the same.

GROUP PROJECT AND PRESENTATION: The group project will be case, which will be based on a real organization. Each team will work on a different case as assigned by the instructor. You will be required to conduct a complete fraud examination, by following the investigative methods and steps covered in the classroom and/or the textbook. The requirements are as follows:

1. Case files: You are required to maintain a case file of your findings at each step of the investigation. The case files will be reviewed by the instructor throughout the semester. Further details will be communicated in class.
2. Final Report: After completing the investigation, you will create a final report of your findings and recommendations.
    a. The report should describe in detail, the actual investigative procedures that were undertaken by the team.
    b. Provide a comprehensive account of the fraud that occurred, including details of who was involved. Be sure to discuss what went wrong (e.g., the management issues that may have allowed the fraud to occur).
    c. Provide recommendations to management, auditors, and investors to prevent similar fraud from happening again. In your recommendations, make sure you address what could have prevented the fraud from happening in the first place.
    d. Note: The report should be written from the point of view of a fraud examiner reporting to the management/board of the victim company.
    e. Develop a response plan for the organization (as part of the report). Details of how to develop a response plan will be provided in class.
    f. Submission requirements: The report should be 4-5 pages in length, not including the cover page and the references. Use 1-inch margins all around, Times New Roman, font 12 and single spaced, formatted in APA style. The report should include a reference page, with at least 4 references. In addition, you may use footnotes or endnotes as needed.
3. Presentations: You will be required to present your report. Each team will make a 10-minute presentation to the class. Each team member is expected to speak. The grading rubric for the presentations will be distributed along with the project details in class. There will also be peer evaluations to evaluate each group members' performance and contributions.
4. Peer Review: At the end of the semester, students will evaluate and rank order the participation and contribution level of each team member. The peer review forms will be distributed in class on the day of the presentations.

GRADING

Your assignments will be graded on correctness, not just completion. I try to grade assignments and exams fairly and return them within a reasonable time-period with relevant comments, and to be available to discuss questions. If you have a question about your assignment/homework scores, please contact the instructor in writing, within a week of receiving the grade. Your email must follow the email guidelines stated in the syllabus. In addition, describe to the instructor why you believe you deserve a higher grade. Also, please let me know if there is a mistake in calculation – mistakes happen!

STUDENTS WITH DISABILITIES: Students with disabilities should register with the Disability Resource Center and inform me of their disability status and their need for academic accommodations as soon as possible. Sufficient prior notification will enable me to make the necessary arrangements through the Disabled Student Services Office.

ACADEMIC INTEGRITY: Plagiarism and cheating.

As an instructor, I am required to report any student behavior that has the appearance of cheating or plagiarism to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies). Penalties for cheating and plagiarism can be quite severe, and can include 1) failure of course; 2) suspension from the university; 3) expulsion from the university and 4) a notation in your permanent transcripts. ***You cannot afford to enter professional life with any of these stains on your permanent record.***

As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** If you have questions about academic integrity **- ASK!**

Here are some examples of acceptable collaboration:

- Clarifying ambiguities or vague points in class handouts, textbooks, or lectures.
- Discussing or explaining the general class material.
- Discussing the assignments to better understand them.
- Properly citing and document any sources (using APA style) from which you have borrowed ideas or language.

Now for the dark side. As a general rule, if you do not understand what you are handing in, you are probably cheating. If you have given somebody the answer, you are probably cheating. To help you draw the line, here are some examples of clear cases of cheating:

- Copying homework answers from another person or source, including retyping their answers, copying without explicit citation from previously published works (except the textbook), etc.
- Allowing someone else to copy your work, either in draft or final form.
- Getting help from someone whom you do not acknowledge on your homework.
- Copying from another student during an exam, quiz, or midterm. This includes receiving exam-related information from a student who has already taken the exam.
- Inappropriately obtaining course information from instructors.
- Looking at someone else’s files containing draft solutions, even if the file permissions are incorrectly set to allow it.
- Receiving help from students who have taken the course in previous years.
- Copying on quizzes or exams.
- Reviewing any course materials from previous years (except for the course textbook which can be purchased in used condition).
- Reading the assignment solutions handed out if you will be handing in the current assignment late.

GRADING AND EVALUATION

Your grade in this course will be determined as follows

ACTIVITY	PERCENTAGE OF GRADE
Classroom Participation (i.e., In-class participation and discussions)	10%
Graded in-class assignments, opportunities, and quizzes	10%
Homework assignments	20%
Group Project and Presentation	20%
Exams	40%

Your final grade in the course will be a letter grade. Letter grade equivalents for numerical grades are as follows:

A	= 93–100	B–	= 80–82
A–	= 90–92	C+	= 78–79
B+	= 88–89	C	= 73–77
B	= 83–87	F	= Below 73

Note: For the graded in-class assignments component, the lowest score will be dropped.

Tentative Course Schedule

Date	***Topic***
Aug 28 & 30	Course Overview and Introductions, Chapter 1: Forensic Accounting Overview
Sept 6 & 11	Chapter 2: Fraud in Society, Skimming (notes will be provided on blackboard) Form teams of 2-3. Instructor will assign teams.
Sept 13 & 18	Corruption (notes will be provided on blackboard).
Sept 20	Finish Corruption, Start Chapter 3
Sept 25	**EXAM 1**
Sept 27	Chapter 3: Understanding the basics of financial accounting.
Oct 2	Inventory Fraud. Assign Case 1
Oct 4 & 9	Check Fraud (notes will be provided on blackboard).
Oct 11, 16 & 18	Chapter 5: Fundamental principles of financial analysis
Oct 23	**Exam 2**
Oct 25	Chapter 9: The investigation Process, Case 2 will be assigned.
Oct 30	No Lecture. Complete Case Studies.
Nov 1 & 6	Chapter 10: Interviewing Financially Sophisticated Witnesses
Nov 8 & 13	Chapter 11: Proving cases through documentary evidence
Nov 15	Chapter 12: Analysis tools for investigators
Nov 20	Commercial Damages (notes will be provided on blackboard)
Nov 27	Chapter 13: Inferential analysis for investigators, Social network analysis for fraud investigation (notes will be provided.
Nov 29	**Exam 3**
Dec 4 & 6	Presentations
Dec 11	Course wrap up, Guest Speaker

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

Final Notes:

A syllabus is an outline and guide to help you plan your semester. It also documents course policies, procedures, and expectations. Please keep a copy of it in your notebook to refer to it throughout the semester.

The instructor reserves the right to make changes to the syllabus based on the direction of the course, cancelled classes and assignment dates/weight to assignments.

Have a great semester!

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

BFOR 402

eDiscovery & Digital Forensics Moot Court

Syllabus

Course ID: **BFOR 402**
Course Name: **eDiscovery & Digital Forensics Moot Court**
Credit Hours: **4**
Semester: **TBA**
Instructor: **TBA**
Course Prerequisite(s): **BFOR 201**
Textbook: **TBA**

COURSE DESCRIPTION

Students will learn how to prepare for and give expert witness testimony related to digital evidence, including how to deal with opposing counsel cross-examinations and how to effectively relay such information to a lawyer, judge and jury. Case law and pertinent statutes related to legal proceedings will be reviewed and discussed to ensure understanding of legal and ethical responsibilities of a forensic and eDiscovery specialist. This course also provides an overview of the technology used in the identification and preservation, review, production, and trial presentation of electronic information pursuant to eDiscovery proceedings. Students will utilize analytical tools for searching, culling and presenting corporate data, pursuant to administrative and civil eDiscovery cases.

LEARNING OBJECTIVES

After completing this class the student should be able to:

- Become familiar with civil and criminal proceedings, as well as courtroom procedures.
- Prepare to provide testimony in legal proceedings related to eDiscovery and digital forensics investigations.
- Prepare court exhibits derived from eDiscovery and digital forensics investigations.
- Identify federal and state statutes and case law decisions related to eDiscovery data and digital evidence.
- Develop policies and procedures for corporate managers and IT personnel to ensure compliance with data preservation statutes and regulations.
- Utilize analytical tools for searching, culling and presenting corporate data, pursuant to administrative and civil eDiscovery cases.

COURSE FORMAT

Hybrid Learning Environment: The course is offered through online and classroom delivery of coursework to offer a more flexible learning experience and facilitate self-reliance in finding, evaluating, and applying learned information during structured class discussions, exercises, and other class activities.

INSTRUCTOR CONTACT

Type	Information	Availability
Email		Dates and times TBA
Virtual		Dates and times TBA

COURSE RESOURCES

Course Website	
Reference Material and External Readings	To be posted by instructor during course activities
Technical Support	

COURSE OUTLINE

Week	Topic	Activities
1	Professional Ethics in Legal Proceedings	Discussions Assignments Exercises
2	Federal Rules of Civil Procedures	
3	Federal Rules of Criminal Procedures	
4	Establishing Technical & Expert Witness Credentials	
5	eDiscovery & Digital Forensics statutes & Case Law	
6	Preparing & Using Court Exhibits	
7	**MID TERM EXAM**	
8	Information Governance and Litigation Preparedness	Discussions Assignments Exercises
9	eDiscovery Planning and Data Analysis Tools	
10	eDiscovery & Digital Forensics Report Review	
11	Case Study 1 – eDiscovery – Investigation to Trial	
12	eDiscovery Moot Court	Practicum
13	Case Study 2 – Digital Forensics – Investigation to Trial	
14	Digital Forensics Moot Court	Practicum
15	**FINAL EXAM**	

***** Depending on course activities, sequence of week-by-week topics may be re-arranged at the discretion of the instructor.

COURSE ACTIVITIES

Discussions: Students must engage in topic-related discussions in order to facilitate knowledge-sharing and communications involving class peers, the instructor and guest speakers.

Exercises: Students will be required to complete class exercises completed in classroom and/or online environments, as directed by instructor.

Assignments: Students will be required to complete assignments based on the relevant course topic and learning objective, as directed by instructor.

Project: Project may be assigned and graded by the instructor, based on individual, team and/or class requirements. Presentation to class peers may be part of the project requirements.

GRADING AND ASSESSMENT

We try to grade assignments fairly and return them within a reasonable time period with relevant comments and to be available to discuss questions. Students are expected to set up an appointment to talk with the grader within a week of receiving a grade. Please let us know if there is a mistake in calculation – mistakes happen!

Late assignments, projects, or papers will receive 25% off per day late from the final possible grade for the exercise unless there is a legitimate excuse.

Students at UAlbany should contact the Disabled Student Services Center and the relevant professor at least a week before each F2F exam if requiring additional assistance. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. F2F Exams are expected to be closed-book unless otherwise specified and all personal electronic devices (laptops, cell phones, PDA's, etc.) should be put away.

Activity	Portion of Grade	Description
Discussion	10%	
Assignments	20%	
Exercises	20%	
Project	20%	
Exams	30%	

Overall Accumulative Point Evaluation:

Point Range	Letter Grade
96-100	**(A)**
90-95	**(A-)**
85-89	**(B+)**
80-84	**(B)**
74-79	**(B-)**
70-73	**(C+)**
65-69	**(C)**
62-64	**(C-)**
60-61	**(D)**

Below 60	**(E)**

Syllabus

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany’s standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

“GREAT” EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.
- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.

- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

BFOR 403
Risk Analysis & Security Policies

Instructor:	Victoria Kisekka, PhD
Office Location:	Business Building 371
Office Hours:	Mondays and Wednesdays – 1:30pm to 3:00 pm Or by appointment
E-mail:	vkisekka@albany.edu
Telephone:	956-8361

COURSE

BFOR 403 Risk Analysis & Security Policies (3 credits)
Spring 2018 Semester: Mondays & Wednesdays 8:45am -10:05am in BB 121
Mondays & Wednesdays 10:15 am - 11:35am in BB 121
Verify that you are in the correct section by checking your UAlbany.
Each student must attend the section they officially registered for. No exceptions!
Course Prerequisite(s):

COURSE DESCRIPTION

As the pervasiveness and frequency of security attacks continue to become commonplace, every organization needs to have a strategy for managing security risks. Cybersecurity and Digital Forensics professionals need to have the expertise to assist organizations manage security risks. This course is designed to introduce students to the field of information security risk. The course will explore the phases of a risk management program, focusing on the processes for analyzing and assessing risk. Students will learn how to quantitatively and qualitatively assess risk, how to measure risk, and how to develop security policies for mitigating risk. The course will incorporate cases to provide a holistic view of how to properly use tools to calculate the costs and benefits of security investments.

LEARNING OBJECTIVES

The course will teach students to develop risk management plans, assess security risk, and identify security controls. After completing this course, you should be able to:

1. Define risk and understand the importance of risk management
2. Identify threats, vulnerabilities, and exploits in an organization’s assets
3. Identify the laws relevant to security risks and controls
4. Develop a risk management plan
5. Perform qualitative and quantitative risk assessments
6. Identify security controls for mitigating risk
7. Develop a risk mitigation plan

COURSE RESOURCES

Type	Information
Course Website	https://blackboard.albany.edu/ (All announcements will be communicated through blackboard).
Textbook(s)	Managing Risk in Information Systems. Second Edition by Darril Gibson Publisher: Jones & Bartlett Learning ISBN -978-1-284-05595-5
Reference Books(s) - optional	TBD

COURSE ACTIVITIES

Active Learning: In order to reinforce mastery of the material, I will promote active learning in the classroom. An active learning environment is where students are involved and highly engaged in the learning process other than simply acquiring knowledge passively. As part of this strategy, you are expected to read the textbook and assigned readings before class. PowerPoint slides are only intended to facilitate classroom discussion and also communicate additional relevant information not covered in the required textbook. For this reason, PowerPoint slides based on textbook material will be posted to Blackboard after class unless otherwise communicated. You are expected to take notes during the lectures.

Reading: The readings in this course are not an end in themselves, but rather, the material you read will be used for in-class discussions, assignments, and even writing. Some of the concepts in the readings are complex, and will require persistence on your part. In order for you to be productive in the in-class activities, you will need to prepare before class and come to class ready to discuss.

Lectures: Instructor-led lectures that may be supplemented with expert guest lectures on course-related topics will be offered in class. The lecture material should summarize and expand on the knowledge obtained from the assigned readings and assignments.

Classroom participation and discussions: Students are expected to participate in classroom discussions in an insightful manner. Part of your participation grade will be based on your involvement in in-class discussions. Discussions topics and/or questions may also be assigned and graded. Obtaining the maximum contribution in the class occurs when students consistently join the discussion and offer opinions. Contribution in one single class or some of the classes does not equate to maximizing the points available. You will be evaluated on the QUALITY of your contributions and insights. Quality comments possess one or more of the following properties:

- Offers a different and unique, but relevant, perspective;
- Contributes to moving the discussion and analysis forward;
- Builds on other comments;
- Transcends the "I feel" syndrome. That is, it includes some evidence, argumentation, or recognition of inherent tradeoffs. In other words, the comment demonstrates some reflective thinking.

While your classroom participation grade is subjective, it will not be random or arbitrary. And, clearly, more frequent quality comments are better than less frequent quality comments.

Homework Assignments: Several assignments will be given during the semester. These will include take-home assignments or in class exercises. Completed assignments should be handed in by the time and date specified on blackboard, on the course schedule or verbally communicated during class.

Assignments that are one day late will be reduced by 20%
Assignments that are two days late will be reduced by 40%
Assignments that are three days late will be reduced by 60%
Assignments that are more than three days late will be given no credit unless when there is a legitimate excuse for the lateness.

Missed assignments will receive no credit unless there is a legitimate excuse for not completing the assignment. When an assignment is missed due to a legitimate excuse, it must be made up at a time specified by the instructor or the grade of "0" is recorded. Legitimate excuses include illnesses requiring professional attention and personal or family emergencies. It is the responsibility of the student to initiate 1) a consultation with the instructor regarding a missed assignment in a timely fashion (within 2 class periods) and 2) to present verifiable written documentation. It is the responsibility of the student to keep a record of missed assignments and work that must be made up. To obtain the required documentation for absences, visit the office of the Provost for Undergraduate Education. The contact information for this office and more details can be found here http://www.albany.edu/undergraduateeducation/attendance.php

If you become seriously ill during the semester, or become derailed by unforeseeable life problems, and have to miss so many assignments that will ruin your grade, you and the instructor will schedule a special meeting in order to make arrangements for you to withdraw from the course with the documentation needed to try to save your grade point average. Do not wait until it's too late to arrange this meeting if you see that you are getting in trouble.

Attendance: Your in-class performance is crucial to your success in this course. Attendance itself is not graded, but there will be graded in-class activities, such as quizzes and **opportunities**. *Opportunity is used to refer to any unannounced graded in-class activity. These may include but are not limited to writing assignments, group activities, individual activities, etc.* Keeping a passing average on these is not possible without consistent attendance. Missing class means earning an automatic "0" for the activities or assignments missed. The lowest score of the graded in-class assignments (i.e., quiz or opportunity) will be dropped. Because the lowest score of a quiz or opportunity is dropped, if you miss a quiz or opportunity, it will be the quiz or opportunity score that is dropped. For example, if we have 5 graded in class assignments consisting of quizzes and opportunities, your lowest score of the 5 assignments will be dropped.
No make-up assignments will be available for in-class activities except in documented cases of extreme extenuating circumstances. For an approved absence, the student will be given a makeup graded assignment by the instructor within one week of the original assignment date. To obtain the required documentation for absences, visit the office of the Provost for Undergraduate Education. The contact information for this office and more details can be found here http://www.albany.edu/undergraduateeducation/attendance.php.

Lateness-Tardiness Policy: Missing an assignment or activities that happened at the beginning of class before you arrive or at the end of class after you leave early will also earn a "0", and there will be no make-up assignments. *If you know that it will be difficult for you to consistently get to class on time and stay for the entire period, you should drop this course and take it at a later date, when your life's circumstances are more manageable.*

Cell Phone Policy: Please show respect for you fellow students by making sure your cell phone is turned off or is in a silent mode (e.g., vibrate or do not disturb) before entering the classroom.

EMAIL ETIQUETTE

This is a business school and I whole heartedly believe that some behaviors become habits. All of you aspire to have successful carriers and as part of your training, communication is key. All your emails to me must be professional. I will try to respond to all emails within 24 hours. Here are some guidelines for writing professional emails.

1.Your email should start with a proper salutation. E.g., Dear or Hi Dr. Last name, Dear or Hi Professor Last name. **Emails that do not open with a proper salutation will not be read**. I typically assume that the email was not intended for me.

2. Use proper grammar, spelling, and punctuation. Refrain from using slangs and acronyms such as LOL, ROFL, BTW, ASAP, TTYL, IMO, ION, etc. Do not use ALL CAPITAL LETTERS. The assumption here is that you are yelling at the recipient.

3. Never leave the subject line blank.

4. Your email should end with a proper signature. Provide your full name at the end of the email.

5. Be respectful. Avoid intimidating emails. And remember, your email message shapes the recipient's professional impression about you.

OFFICE HOURS: Don't be a stranger! Take advantage of my scheduled office hours to go over material you do not understand. I am here to help you.

EXAMS: Two exams will be offered. Exams are to be completed in the classroom on the date and time specified on the course schedule. The content of these exams will be based on the material in the textbook, other assigned readings, and in-class discussions. There will be no final exam. Exams must be completed on the communicated date. No make-up exams shall be given except in cases of extreme extenuating circumstances. To obtain the required documentation for absences, visit the office of the Provost for Undergraduate Education. The contact information for this office and more details can be found here http://www.albany.edu/undergraduateeducation/attendance.php

Note: If you request your exam to be reviewed for errors, the instructor will independently evaluate the exam. Exam scores can increase, decrease, or remain the same.

FINAL PROJECT AND PRESENTATION: A final project will be assigned. Details of the project are forthcoming.

GRADING

Your assignments will be graded on correctness, not just completion. I try to grade assignments and exams fairly and return them within a reasonable time-period with relevant comments, and to be available to discuss questions. If you have a question about your assignment/homework scores, please contact the instructor in writing, within a week of receiving the grade. Your email must follow the email guidelines stated in the syllabus. In addition, describe to the instructor why you believe you deserve a higher grade. Also, please let me know if there is a mistake in calculation – mistakes happen!

STUDENTS WITH DISABILITIES: Students with disabilities should register with the Disability Resource Center and inform me of their disability status and their need for academic accommodations as soon as possible. Sufficient prior notification will enable me to make the necessary arrangements through the Disabled Student Services Office.

ACADEMIC INTEGRITY: Plagiarism and cheating.

As an instructor, I am required to report any student behavior that has the appearance of cheating or plagiarism to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies). Penalties for cheating and plagiarism can be quite severe, and can include 1) failure of course; 2) suspension from the university; 3) expulsion from the university and 4) a notation in your permanent transcripts. ***You cannot afford to enter professional life with any of these stains on your permanent record.***

As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** If you have questions about academic integrity **- ASK!**

Here are some examples of acceptable collaboration:

- Clarifying ambiguities or vague points in class handouts, textbooks, or lectures.
- Discussing or explaining the general class material.
- Discussing the assignments to better understand them.
- Properly citing and document any sources (using APA style) from which you have borrowed ideas or language.

Now for the dark side. As a general rule, if you do not understand what you are handing in, you are probably cheating. If you have given somebody the answer, you are probably cheating. To help you draw the line, here are some examples of clear cases of cheating:

- Copying homework answers from another person or source, including retyping their answers, copying without explicit citation from previously published works (except the textbook), etc.
- Allowing someone else to copy your work, either in draft or final form.
- Getting help from someone whom you do not acknowledge on your homework.
- Copying from another student during an exam, quiz, or midterm. This includes receiving exam-related information from a student who has already taken the exam.
- Inappropriately obtaining course information from instructors.
- Looking at someone else's files containing draft solutions, even if the file permissions are incorrectly set to allow it.
- Receiving help from students who have taken the course in previous years.
- Copying on quizzes or exams.
- Reviewing any course materials from previous years (except for the course textbook which can be purchased in used condition).
- Reading the assignment solutions handed out if you will be handing in the current assignment late.

GRADING AND EVALUATION

Your grade in this course will be determined as follows

ACTIVITY	PERCENTAGE OF GRADE
Classroom Participation (i.e., In-class participation and discussions)	10%
Graded in-class assignments, opportunities, and quizzes	10%
Homework assignments	25%
Final Project and Presentation	25%
Exams	30%

Your final grade in the course will be a letter grade. Letter grade equivalents for numerical grades are as follows:

A	= 93–100	B–	= 80–82
A–	= 90–92	C+	= 78–79
B+	= 88–89	C	= 73–77
B	= 83–87	F	= Below 73

Note: For the graded in-class assignments component, the lowest score will be dropped.

Tentative Course Schedule

Date	Topic	Reading	Assessment
Jan 24 & 29	Risk Management Fundamentals	Chapter 1	
Jan 31	Managing Risk: Threats, Vulnerabilities, and Exploits	Chapter 2	Identifying threats and vulnerabilities
Feb 5 & 7	Identifying Assets and Activities to be Protected	Chapter 7	Exercise for critical assets related to the 7 domains of IT infrastructure
Feb 12	Identifying and Analyzing Threats, Vulnerabilities and Exploits	Chapter 8	Conduct security audits; Vulnerability assessments; Exploit assessments
Feb 14	**Exam1**	**Exam1**	**Exam 1**
Feb 19 & 21	Risk Assessment Approaches	Chapter 5	Conducting qualitative and quantitative assessment
Feb 26 & 28	Security Controls	Chapter 9	Identifying procedural, technical and physical controls; mapping controls to vulnerabilities
March 5 & 7	Security Standards & Compliance	Chapter 3	
March 12 & 14	**SPRING BREAK**	**NO CLASS**	
March 19	**EXAM 2**	**EXAM 2**	
March 21 & 26	Risk Mitigation Planning	Chapter 10 NIST SP-30	Mitigation planning exercise
March 28 & April 9	NIST Methods	Notes provided	
April 11 & 16	FRAAP Method	Notes provided	FRAAP Exercise
April 18 & 23	OCTAVE Method, NICE Framework	Notes provided	OCTAVE approach exercise
April 25 & 30, May 1 & 9	Final project presentations	Final project presentations	

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

Final Notes:

A syllabus is an outline and guide to help you plan your semester. It also documents course policies, procedures, and expectations. Please keep a copy of it in your notebook to refer to it throughout the semester.

The instructor reserves the right to make changes to the syllabus based on the direction of the course, cancelled classes and assignment dates/weight to assignments.

Have a great semester!

UALBANY

BFOR 410/610
International Cyber Conflicts

Syllabus

International Issues in Information Security 3 credits
LOCATION: Asynchronous MOOC –
Segment 1: https://www.coursera.org/learn/cyberconflicts
Segment 2: TBD
Instructor: Sanjay Goel & Kevin Williams

This course is delivered online and asynchronously. It meets or exceeds the total amount of instructional and studenwork time expected in a traditional in-class course in every week of a 15 week semester: three 55 minute sessions of classroom or direct faculty instruction for every 3 credit course.

I. CLASS DESCRIPTION

Cyber Security is an international problem where the perpetrators and victims of attacks may be in completely disparate locations. Cyber attacks have morphed from cyber crime and amateur display of prowess into cyber warfare and espionage among nations. While the issues are international there is little consensus on how to investigate them, create universally acceptable norms, and create international laws across multiple countries to manage them. This course investigates the nature of cyber threats and conflicts, the international efforts to reduce and improve cyber security, and the psychological and political factors at play in both conflicts and efforts to address them. The material presented will allow students to evaluate causes for conflicts, enable them to explain the actors and their motivations and analyze characteristics of cyber conflicts based on international treaties and principles of war. The hope is to improve understanding between professionals and students across countries in order to foster cooperation in resolving cyber conflicts. The class will include cases and discussions that will touch on the sensitive security related topics.

II. LEARNING OBJECTIVES

To improve understanding of international issues in Cyber Security and Cyber Warfare, capacity to evaluate behavior of nations and assess international efforts to address conflicts.

After this course you will be able to:

- Identify the different threat actors and the different types of cybercrime.
- Provide preliminary analysis of cybercrime by understanding basic psychological mechanisms of motivation.
- Define main components of the Internet infrastructure, the main issues in governance and compare different approaches to international internet policy.
- Recognize the different types of cyber threats and the modes of attacks among states and discuss the motivations of state and non-state actors.
- Describe the principles of just war, basic aspects of International Humanitarian Law and international treaties concerning cyber security
- Evaluate the main particularities of dealing with state and non-state actors and how to apply legal principles to solutions for cyber conflicts.
- Explain the psychological mechanisms of how people react in situations of reciprocal activity and of trust.
- Describe and discuss how confidence building measures may be formulated and applied in the domain of cyber security.

INSTRUCTOR CONTACT

Type	Information	Availability
Email	goel@albany.edu kwilliams@albany.edu	Will attempt to respond within 24 hours.
Virtual Chat	Skype (goelsahib)	Times can be scheduled.

III. COURSE ACTIVITIES

Lectures: Video lectures will be posted through the learning management system.

Readings: Chapters, articles, and other readings when assigned in the class are meant to supplement and reinforce course material.

Discussions: Every module will have a discussion that will cover different topics related to cyber security. Students may be asked to act for or against a particular side of an issue. Criteria will be provided for developing your arguments. Discussions will require an initial position paper stating your positions and subsequenty responding to the viewpoints of other students.

Cases: Case studies will use actual examples to provide real-world relevance to the topics in the class.

Quizzes: Quizzes will be assigned periodically (typically one per module).

Research Paper: Depending on the section to which you enroll this course may require a research paper as part of course activities and grading assessment.

IV. GRADING AND ASSESSMENT

Students will be able to take the class for credit or without credit.
For students who take this for credit: Late assignments, projects, or papers will be penalized 15% per day unless there is a legitimate excuse. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. We try to grade assignments fairly and return them within a reasonable time period with relevant comments and to be available to discuss questions. Students are expected to meet with the faculty in case there is a grading concern.
For students who do not take this class for credit: They will be expected to participate in discussions and rate each others postings and responses.

Type	Grad/UG	Description
Quizzes	25%/35%	Quizzes will be offered at the end of each module. The quiz may contain multiple choice or short-answer questions.
Case Exercises / Discussions	50%/65%	Students will be asked to analyze cases (long and vignettes) that will be evaluated through peer-evaluation for COURSERA subscribers and by the course instructors/TAs for students taking the class for SUNY credit.
Research Paper	25% / 0	Research paper (6-8 pages, 12 pt. font, single spaced) will be expected in any area of international cyber conflict with approval of the instructor

Research Paper: For graduate students a research paper is required; the paper should be on a topic dealing with International Cyber Conflicts; you may work in teams of 2-3 students on the paper. The paper should be at least 6 pages long (about 3000 words), single spaced, 12-pt font, with 1-inch margin (not more than 8 pages long (about 8000 words). First select a topic and make an outline; make sure that the outline and topic are correct with the instructor prior to emarking on writing the paper.

Submissions will be evaluated based on originality, strength of argument and recommendations, adherence to the norms of spelling, grammar, and syntax, and clarity.

- Originality: Has the author identified and defined the central issue? Is the issue relevand and important? Is the perspective of the author unique? (25%)
- Research and Analysis: Has the author researched prior work thoroughly and is the prior work appropriately cited and quoted when using exact quotes. Has the authors comprehensively covered all aspects of the argument. Are the facts and opinions make a coherent argument to prove the authors position? (35%)
- Clarity: Is the paper clearly presented and well organized? Is the writing clear and lucid? Is the issue clearly described with the recommendations and proposed outcomes precisely laid out? (30%)
- Spelling, Grammar, and Syntax: Is the paper grammatically correct and properly edited? (10%)

V. SCHEDULE (PART 1)

Modules	Lectures	Learning Objectives
Module 1 - Intro to Cybercrime	Lecture 1: Intro to cybercrime and fundamental issues	This module is intended to introduce you to a set of actors and motivations in the area of cyber security. After this module you will be able to identify the different threat actors and the different types of cybercrime. You will also be able to provide some preliminary analysis of cybercrime by understanding basic psychological mechanisms of motivation.
	Lecture 2: Evolution and types of cybercrime	
	Lecture 3: Types of cybercrime actors	
	Lecture 4: Understanding motivated behavior	
	Lecture 5: Motives for hacking	
	Lecture 6: Cyber-attacks in a global context	
Module 2 - Internet Governance	Lecture 1: What is the Internet?	This module covers technical aspects of the Internet and the domain name system, and efforts toward internet governance. After this module you should be able to define main components of the Internet infrastructure, identify the main issues in governance and compare different approaches to international internet policy.
	Lecture 2: Domain Name System	
	Lecture 3: Internet Governance	
	Lecture 4: Importance of Internet Governance	
	Lecture 5: Current issues in Internet Governance	
Module 3 - Cyber Warfare & International Conflicts	Lecture 1: Introduction to Cyberwarfare	In this module we cover the main types of attacks, actors and conflicts that may be considered aspects of cyberwarfare. After this module you will recognize the different types of cyber threats and the modes of attacks and discuss the motivations of state and non-state actors in this domain.
	Lecture 2: Modes of attacks	
	Lecture 3: Cyberwarfare actors	
	Lecture 4: Actors motivation	
	Lecture 5: Types of attacks	
	Lecture 6: Critical Infrastructure	
	Lecture 7: Internet Censorship	
Module 4 - Cyber Warfare & International Law	Lecture 1: Principles of Just War	This modules covers political theories and legal arrangements pertinent to cyber security. After this module you will be able to describe principles of just war, basic aspects of International Humanitarian Law and treaties. You will be able to evaluate the particularities of dealing with states and non-state actors and the potential international solutions.
	Lecture 2: Law of Neutrality & Humanitarian Law	
	Lecture 3: Ambiguity & Attribution	
	Lecture 4: International Treaties	
	Lecture 5: Characteristics of CBMs	
Module 5 - Interpersonal Trust and Trust among Nations	Lecture 1 - Ultimatum game and social preferences	This module deals more specifically with psychological explanations for individual trust and trust among nations. After this module you will be able to explain how people react in situations of giving and of trust. You will also be able to identify and discuss how confidence building measures may be applied in the domain of cyber security.
	Lecture 2 - Components of Trust and Social Capital	
	Lecture 3 - Trust between Nations and Prisoner's dilemma	
	Lecture 4 - Psychological Perspective on CBM	

VI. SCHEDULE (PART 2)

Modules	Lectures	Learning Objectives
Module 1 – Internet Sovereignty	Lecture 1: The Problem	This module is intended to introduce you to indroduce you to the concept of Intenet Sovereignty and its implications for the Internet users. It discusses the technical feasibility as well as the political connotations of Internet Sorvereignty. After this module students will have a better understanding of the drivers behind the sovereignty debate.
	Lecture 2: Transformation of the Internet	
	Lecture 3: Models For Internet Ownership: Sovereignty Vs. Community	
	Lecture 4: Global Resource - Global Responsibilities	
	Lecture 5: Feasibility of Soverign Internet	
	Lecture 6: Conclusions	
Module 2 – Hacktivism	Lecture 1: Genesis Of Hacktivism	Hacktivism is a recent phenomenon wherein hackers are using their skills to hack into government and corporate websites to protest against unfialr practices. Some of their activities are borderline with the law. This module discusses the evolution of hacktivism and how the law is evolvoing around it.
	Lecture 2: History Of Hactivism	
	Lecture 3: Hacktivism and Law	
	Lecture 4: Types of Hacktivists	
	Lecture 5: Conclusion	
Module 3 – Propaganda and Social Media Revolutions	Lecture 1: Propaganda	Arab spring transformed the image of the Internet as a tool for social communication, commerce, and knowledge acquisition to a potent tool for fomenting unrest and instigating political change. In this module we revisit arab spring and study the role of social media in that.
	Lecture 2: Arab Spring	
	Lecture 3: Role of Social Media in Arab Spring	
	Lecture 4: Foreign Intervention via Social Media	
	Lecture 5: Social Media as Intelligence Source for Governments	
	Lecture 6: Conclusions	
Module 4 – Cyber Espionage	Lecture 1: Cyber Espionage	This modules covers how how espionage has transformed through the Internet and how government and private corporations are leveraging it. After this module you will understand the different types of espionage activities on the Internet and legal issues around these activities.
	Lecture 2: Corporate Espionage	
	Lecture 3: Government Espionage	
	Lecture 4: Domestic Surveillance	
	Lecture 5: Cyber Espionage and Law	
	Lecture 6: Conclusions	
Module 5 – Intellectual Property Issues on Internet	Lecture 1: Intellectual Property and the Internet	There is a continuous debate on how to reconcile the traditional intellectual property norms and laws on the Internet. Enforcement via technical means via possible but cumbersome and breakable. International laws pertaining to copyright issues need to be considered.
	Lecture 2: Copyright and Related Rights	
	Lecture 3: Trademarks and Distinctive Signs on the Internet	
	Lecture 4: Media Piracy	
	Lecture 5: International Copyright Law	

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards will result in the student being reported to the Office of Graduate Admissions, or the Dean of Undergraduate Studies Office (whichever applies) AND receiving a lowering of a paper or project grade of at least one full grade; receiving a failing grade for the project containing plagiarized material or examination in which cheating occurred; receiving a lowering of course grade by one full grade or more; a failing grade for the course;, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s); submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; destroying, damaging, or stealing of another's work or working materials; or presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). Misrepresenting another's work as one's own includes paraphrasing or summarizing without acknowledgment; submission of another student's work as one's own; purchase of prepared research, papers or assignments; and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

"GREAT" EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion, lack of understanding, or need for assistance in dealing with course matters. In turn, the instructor will attempt to assist in clarification.
- If the instructor is unable to attend meeting times or office hours due to a personal emergency, students can expect to be informed in as a timely a manner as possible.

- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all work on time as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

BFOR411 Syllabus

Course ID: **BFOR411**
Course Name: **SCADA Forensics**
Credit Hours: **3**
Semester: **Spring 2018**
Instructor: **TBA**
Mode of Delivery: **Hybrid-Blended (online/classroom)**
Course Prerequisite(s): **R CRJ 281, A MAT 108, or equivalent; recommended B FOR 201 & 202**
Textbook: **TBA**

COURSE DESCRIPTION

This course prepares students to understand how to defend critical infrastructure systems (**Supervisory Control and Data Acquisition**) such as electric utilities, water, oil, natural gas, transportation and other vital systems. The course builds student knowledge in the unique protocols and applications that are the foundation of industrial control systems. We will discuss the unique challenges facing critical infrastructure and the threats that target these systems.

LEARNING OBJECTIVES

After completing this class the student should be able to:

- Define the unique protocol and application characteristics of industrial control systems
- Assess risks and vulnerabilities within an industrial control system using standardized methodology
- Understand the common attack methodologies used to compromise industrial networks
- Define the regulatory compliance standards applicable to industrial network security

TOOLS

Wireshark - http://www.wireshark.org

COURSE FORMAT

Online/Classroom Hybrid: The course may be offered as a combination of online and/or classroom environments. Students are provided with an interactive learning environment through instructor led lessons, online discussion groups and other learning assessments. The course is spread over several weeks but it is important to stay on schedule to allow the student to participate in class discussions.

COURSE OUTLINE

Week	Topic	Activities
1	Introduction to Industrial Networks	Assignment
2	Industrial Cyber Security History and Trends	Assignment
3	Industrial Control Systems and Operations	Assignment
4	Industrial Network Design and Architecture	Assignment

5	Industrial Network Protocols	Assignment
6	Hacking Industrial Systems	Assignment
7	**MIDTERM EXAM**	
8	Risk and Vulnerability Assessments	Assignment
9	Establishing Zones and Conduits	Assignment
10	Implementing Security and Access Controls	Assignment
11	Exception, Anomaly and Threat Detection	Assignment
12	Security Monitoring of Industrial Control Systems	Assignment
13	Standards and Regulations	Assignment
14	**FINAL EXAM**	

COURSE ACTIVITIES

Assignments: Assignments will be assigned and graded by the instructor and will be based on the weekly discussion topic(s). Students will be required to complete and submit Assignments to the instructor by a specific date and grading assessment will be outlined in the Assignment instructions.

GRADING AND ASSESSMENT

We grade assignments fairly and return them with relevant comments within a reasonable time period. The instructor will be available for discussions concerning course work and grading. Students are expected to set up an appointment to talk with the instructor within a week of receiving a grade. Please let us know if there is a mistake in calculation – mistakes happen!

Late assignments, lab exercises, or projects will receive 25% off per day late from the final possible grade for the exercise unless authorized by the instructor.

Students at UAlbany should contact the Disabled Student Services Center and the relevant professor at least a week before each exam if requiring additional assistance. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. Exams are expected to be closed-book unless otherwise specified and all personal electronic devices (laptops, cell phones, PDA's, etc.) should be put away.

Activity	Portion of Grade
Assignments	25%
Quizzes	20%
Exams	50%
Participation	5%

Overall Accumulative Point Evaluation:

Point Range	Letter Grade
97-100	**(A)**
91-96	**(A-)**
86-90	**(B+)**
81-85	**(B)**
76-80	**(B-)**
71-75	**(C+)**
66-70	**(C)**
63-65	**(C-)**
60-62	**(D)**
Below 60	**(F)**

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity – ASK!**

"GREAT" EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.

- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.

- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.

- Students are expected to provide reliable contact information and inform the instructor of any updates.

- Students are expected to contact the instructor via email, phone, or in person for reliable response.

- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary.

- It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

Syllabus

BFOR 412 Cyber Incident Response and Pen Testing

Instructor: Sanjay Goel
Office: BB-301G
Office Hours: By Appointment
Phone: (518) 956 - 8323
Email: goel@albany.edu
Classroom: BB121

Course Objectives

In this course, students will learn attack detection and penetration testing tools. Students will learn intrusion detection techniques and how to handle intrusions. Techniques such as network analysis, log analysis, and network monitoring as well as how to respond to cyber incidents will be covered. Students will also learn the tools, attacks, techniques, strategies and tactics to jumpstart their penetration testing career and infiltrate any network or system. This hands-on, how-to course gives students an in-depth overview of penetration testing and how to test for computer/network/web vulnerabilities. From internal to external hacking, one will be able to understand the vulnerabilities that an attacker could exploit. Throughout the course, the students will have the opportunity to work with various tools, attacks, software, and tactics.

Specific topic coverage includes:

- Introduction to Kali Linux
- Security & Networking Foundations
- External Network Hacking
- Internal Network Hacking
- Wireless Network Hacking
- Social Engineering

Prerequisites

Student are expected to have taken the following classes:

BFOR 204	Introduction to Cyber Security
BFOR 206	Programming for Analytics
BFOR 305	Cyber Defense

Textbook & Readings

N/A

Website and Course Materials

This course material is available at UAlbany Blackboard. It contains class notes, PowerPoint slides, class announcements, course syllabus, and other information for the course.

Instructor Contact

Please set up an appointment to discuss any class related material by phone or email.

Type	Information	Availability
Email	goel@albany.edu	I will try to answer your questions within 24 hours. In case you feel that your email gets buried in my mailbox feel free to send a reminder.
Phone	(518) 956-8323 (Office) (518) 387-9090 (Mobile)	
Virtual Chat	Skype (goelsahib) Google Hangout/Chat (goelsa@gmail.com)	Times can be scheduled by phone or email for individuals or groups.

TECHNICAL RESOURCES

If you experience technical problems that interrupt your ability to complete class work, it's important that you know where to seek help immediately. Here is a simple guide for where you should direct questions and calls for help.

Problems with…	You should contact…
Logging into your ISP (Internet Service Provider); connecting to websites; launching web browser (e.g. Internet Explorer, Firefox)	Your ISP. The following links are provided to a couple of local ISP providers contact pages. If yours is not on this list, look up your ISP in a search engine and find a "Contact Us" page: Time Warner (Road Runner) & Verizon (FIOS)
Connecting & logging into to the UAlbany BLS website; accessing your course(s); interacting or participating in course activities, submission of assignment or file attachments in course.	The ITS Help Desk by using the ITS Help Request Form (http://www.albany.edu/its/help) or call (518) 442-4000. Press "1" for students. Then, press "2" for help with Blackboard.
Forgotten PIN when trying to get forgotten password.	The ITS HelpDesk at (518) 442-3700 or go to Lecture Center (LC) 27 at the UAlbany main campus with your SUNYCard and another form of identification. Press "1" for assistance when calling.

Please note that your instructor is not on this list. If you send inquiries about these technical problems, you will be referred to the resources listed above.

COURSE ACTIVITIES

Lectures & Readings: The course will feature assigned chapters, articles, or other PowerPoint readings as well as presentations.

Assignments: There will be several assignments in this class and you are expected to work alone or in teams as suggested in the assignment.

Hands-On Laboratory Exercises: Laboratory exercises will be offered where students get hands-on experience using tools and techniques in the field. Laboratory associated exercises take around 1 – 1 ½ hour to complete and will have associated questions for which your answers will be graded. Lab exercises will often require installation of software on computers and completing the corresponding exercises. At the end of the exercise, you should delete the software installed on the machines.

Project: Red Team-Blue Team project. Using the Cyber Innovation Lab, students will work in teams in which they will adopt a defense (Blue Team) or offense posture (Red Team). The Red Team will adopt a hacker mindset to attack a system utilizing methods that will be learned throughout the course, with specific challenges that need to be accomplished. The Blue Team will work to prevent the Red Teams attacks and detect and triage successful attacks. A report on activities will be presented to the class at the conclusion of the project.

GRADING AND ASSESSMENT

The instructor will try to grade discussions, assignments, and labs fairly and return them within a reasonable time period with relevant comments and be available to discuss questions. Students are expected to set up an appointment to talk with the grader within a week of receiving a grade. Please let us know if there is a mistake in calculation – mistakes happen!

Late assignments, labs, or papers will receive 15% off per day late from the final possible grade for the exercise unless there is a legitimate excuse. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. Please also send any documentation to the instructor(s) as early as possible if you want to request any reasonable accommodations based on a disability.

Final grades will be graded on a curve using the following weightages. Based on the natural distribution of grades, students will be assigned final letter grades. Grading on a curve generally gives the person who performs the best in the class an "A" and other grades are decided based on their relative closeness to the score of the top performer and other students in the class.

Activity	Portion of Grade
Participation	10%
Assignments	30%
Hands-On Laboratories	20%
Project	40

The instructor is expected to get approval of the entire class prior to making any changes regarding the grading rubric.

COURSE SCHEDULE	
Unit	Course Activities
Week 1	**Lecture:** Introduction to Network Monitoring and Incident Analysis a) Governance: Organizational Incident Response Policies b) Types of Incidents c) Responding to Incidents: Protocols, Teams, Equipment **Case:** Develop CERT policies and Team
Week 2	**Lecture:** Network Monitoring (Understanding Data Sources) a) Network Protocols b) Router Based Monitoring (SNMP, RMON, Netflow) c) Non-Router Based Monitoring (Active, Passive, WREN) **Lab:** Network Traffic Visualization
Week 3	**Lecture:** Packet Analysis a) Cyber Warfare and Recent Incidents b) Modes of Cyber Warfare c) Cyber Warfare Actors d) Models of Escalation and De-escalation **Lab:** Packet Capture and Analysis (Wireshark)
Week 4	**Lecture:** Log Analysis I – Understanding Log Files a) Windows Log Files b) Mac Log Files c) Linux Log Files **Lab:** Scripting exercise for analyzing log files
Week 5	**Lecture:** Log Analysis I – Understanding Log Files a) Windows Log Files b) Mac Log Files c) Linux Log Files **Lab:** Scripting exercise for analyzing log files
Week 6	Lecture: Log Analysis III – Log Correlation a) Multiple Log Sources b) Timing of Events **Lab:** Analyzing and Visualizing multiple log sources (Splunk and Snort)
Week 7	**Lecture:** Traffic Analysis a) Analyzing Traffic to identify anomalies b) Fingerprinting operating systems **Lab:** Netflow Lab
Week 8	**EXAM**
Week 9	**Security & Networking Foundations Review** - Networking Basics - Essential Network Tools - netcat, nmap, masscan, tcpdump, wireshark, wget, curl - SecLists - Networking Services (SSH, HTTP / HTTPS, Netcak

	- Hacking Methodology & Phases (Recon, Enumeration, Exploitation, Post Exploitation, Backdooring, Lateral mov ementgs) - Vulnerability Scanning In Depth (Nessus) - Metasploit Framework Foundations - Password Cracking Foundations Lab: Metasploit Laboratory
Week 10	**External Network Hacking** - External Network Hacking Overview - Unique Elements - Noise, fewer hosts/services, types of enum, types of valid/common attacks/exploits - Phases - Demo of noise – web/ssh - Passive External Reconnaissance - Arin, Whois, BGP, DNS - Google Dorking Big Data Stores - Shodan, sonar, Adobe, LinkedIn - Active External Reconnaissance - Network scanning & Port Scanning; nmap, masscan, common services - DNS Reconnaissance - Brute Forcing, Record Lookups, Reverse Lookups - zone transfer – zonetransfer.me (dnsrecon –t axfr –d zonetransfer.me, livedoor.com) Lab: Network/Port Scanning Lab
Week 11	**External Hacking Cont.** - SNMP - SNMP Scanning & Enumeration - SMTP Enumeration - Banner, location, EXPN, VRFY - Web Service Enumeration - Scanning - Screenshotting - Exploring - File/Directory Bruteforce - Social Reconnaissance - Search Engines, commands - Social Networking - Email Harvesting, linkedin, theharvester, manual, simplyemail - Meta Data, foca, metagoofil - Wardialing - Methods & Tools - Wardialing success stories - External Exploitation - Unique characteristics - Firewalls & Calling Home - Common ports to use, encryption

Week 12	**Internal Network Hacking** - Internal Network Overview - Noise, CandyShell - Active Directory - LAN/WAN Architecture - Segmentation / Firewalling - Common Paths - Spoof / Pop / Pass / Win - Scan / Pop / Pass / win - File / Data / Asset owning - Passive Reconnaissance - Network Sniffing, wireshark - DHCP, ARP, CDP, NBNS, WPAD, HSRP, STP, SNMP, Multicast, Unicast - Active Internal Recon & Enumeration - Common Internal Services - masscan and ports - Active Directory & LDAP - ldapper dan, adexplorer - SMB & File sharing - SNMP - braa & snmpwalk - Administration Services - web, telnet, ssh, rdp - Outbound port scanning
Week 13	**Internal Network Hacking Cont.** - Internal Exploitation - Low Hanging Fruit Identification - Using results from Nessus - 2016 Common Exploits - NBNS, Java Deserialize, Default Creds - SMB Exploits - ms08_067, point and shoot - Web Service Vulnerabilities - Credential Reuse & Poor choices - Season16, Same as user - Bypassing AntiVirus - Man In the Middle Attack Techniques - MITM Overview - ARP Poisoning - NBNS Spoofing - WPAD, ICMP, DHCP, HSRP, OSPF - Password Attacks - Bruteforcing Methods - Service Dependent - Hydra, metasploit, SMTP, POP, SMB, RDP, Telnet - Pass The Hash
Week 14	**Social Engineering Cont.** - Social Engineering Foundations - Sources of Information

	- Goals Definition - Attack Vectors - Phishing Targets & Methods - Phishing, Spear Phishing, Whaling - Smishing, Vishing - Client Side Attacks - Reconnaissance & Enumeration - Target Selection - Directory Examples - Social Engineering Tactics - Pretexting - Legitimacy Triggers - Authority & Supplication - Phishing Construction - Spear Phishing - Client Side Exploits - File Format, Java Signed Applets
Week 15	**Project Summary - Presentations**

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

"GREAT" EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.
- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

BFOR 413/613

Multimedia Forensics

Syllabus

Course ID: **BFOR 413/613**
Course Name: **Multimedia Forensics**
Credit Hours: **3**
Semester: **TBA**
Instructor: **Kevin Salhoff**
Mode of Delivery: **Online**
Course Prerequisite(s): **BFOR 201**
Textbook: **TBA**

COURSE DESCRIPTION

This course prepares students to conduct digital forensic examinations on multimedia evidence, specifically images, videos and audio files. The course builds student knowledge from the basics of multimedia types to being able to recognize anomalies in the files and identify file creation attributes. Students will learn how to examine multimedia files manually and through automated processes utilized by digital forensic tools. Students will prepare written reports outlining their findings of analysis, in a professionally acceptable manner, pursuant to administrative, civil and criminal legal proceedings. Graduate students will be expected to do extra or more advanced assignments.

LEARNING OBJECTIVES

After completing this class the student should be able to:

- Perform forensic analysis on common image, video and audio file types.
- Define forensically accepted practices in the analysis of multimedia files.
- Utilize forensically accepted tools to analyze multimedia evidence.
- Prepare written reports derived from forensic analysis of multimedia files.

TOOLS

Ghiro - http://www.getghiro.org/ - http://www.imageforensic.org/
Oxygen Forensic Suite - http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/
Forensic Analysis of Surveillance Videos: http://www.forevid.org/

COURSE FORMAT

Online/Classroom Hybrid: The course may be offered as a combination of online and/or classroom environments. Students are provided with an interactive learning environment through instructor led lessons, online discussion groups and other learning assessments. The course is spread over several weeks but it is important to stay on schedule to allow the student to participate in class discussions.

COURSE OUTLINE

Week	Topic	Activities
1	Class introduction / Overview of image, audio &video files	Class discussion
2	Analysis of image file types pt. 1	Assignment
3	Analysis of image file types pt. 2	Lab Exercise
4	Image metadata examination	Assignment
5	Analysis of audio file types	Assignment
6	Audio enhancement	Lab Exercise
7	**MIDTERM EXAM**	
8	Analysis of video file types pt. 1	Assignment
9	Analysis of video file types pt. 2	Lab Exercise
10	Observational analysis of multimedia files	Assignment
11	Determining alteration of multimedia files	Assignment
12	Steganography/watermarking	Assignment
13	**COURSE PROJECT**	Student Presentations
14	**FINAL EXAM**	

COURSE ACTIVITIES

Lab Exercises: Lab Exercises will be assigned and graded by the instructor. Students will be required to complete Lab Exercises and submit to the instructor by a specific date. Grading assessment will be based on the analysis of sample data and satisfactory completion of forensic reports.

Assignments: Assignments will be assigned and graded by the instructor and will be based on the weekly discussion topic(s). Students will be required to complete and submit Assignments to the instructor by a specific date and grading assessment will be outlined in the Assignment instructions.

Project: Course project will be assigned and graded by the instructor. Students will be required to complete and submit to the instructor by a specific date for grading and assessment.

GRADING AND ASSESSMENT

We grade assignments fairly and return them with relevant comments within a reasonable time period. The instructor will be available for discussions concerning course work and grading. Students are expected to set up an appointment to talk with the instructor within a week of receiving a grade. Please let us know if there is a mistake in calculation – mistakes happen!

Late assignments, lab exercises, or projects will receive 25% off per day late from the final possible grade for the exercise unless authorized by the instructor.

Students at UAlbany should contact the Disabled Student Services Center and the relevant professor at least a week before each exam if requiring additional assistance. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. Exams are expected to be closed-book unless otherwise specified and all personal electronic devices (laptops, cell phones, PDA's, etc.) should be put away.

Activity	Portion of Grade
Assignments	20%
Lab Exercises	20%
Project	15%
Research Paper	15%
Exams	30%

Overall Accumulative Point Evaluation:

Point Range	Letter Grade
97-100	**(A)**
91-96	**(A-)**
86-90	**(B+)**
81-85	**(B)**
76-80	**(B-)**
71-75	**(C+)**
66-70	**(C)**
63-65	**(C-)**
60-62	**(D)**
Below 60	**(F)**

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany’s standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity – ASK!**

"GREAT" EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.
- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary.
- It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

Syllabus

BFOR 416 Advanced Data Analytics

Instructor: Sanjay Goel
Office: BB-301G
Office Hours: By Appointment
Phone: (518) 956 - 8323
Email: goel@albany.edu
Classroom: BB121

Course Objectives

This is a course with primary application to data analytics from a variety of domains, such as healthcare, finance, e-commerce, social media, etc. Learning objectives for students are broadly understand the widely used machine learning algorithms and hands-on experience with data preprocessing, feature extraction, and information visualization, when applying the learned algorithms to solving practical problems. A basic understanding engineering and technology principles is strongly encouraged, including basic programming skills; as is sufficient mathematical background in probability, statistics, and linear algebra.

Specific topic coverage includes:

- Clustering
- Classification
- Statistical Inference
- Network Analysis

Prerequisites

Student are expected to have taken the following classes:

AMAT 108	Introduction to Statistics
BFOR 206	Programming for Data Analytics

Textbook & Readings

N/A

Website and Course Materials

This course material is available at UAlbany Blackboard. It contains class notes, PowerPoint slides, class announcements, course syllabus, and other information for the course.

Instructor Contact
Please set up an appointment to discuss any class related material by phone or email.

Type	Information	Availability
Email	goel@albany.edu	I will try to answer your questions within 24 hours. In case you feel that your email gets buried in my mailbox feel free to send a reminder.
Phone	(518) 956-8323 (Office) (518) 387-9090 (Mobile)	
Virtual Chat	Skype (goelsahib) Google Hangout/Chat (goelsa@gmail.com)	Times can be scheduled by phone or email for individuals or groups.

TECHNICAL RESOURCES
If you experience technical problems that interrupt your ability to complete class work, it's important that you know where to seek help immediately. Here is a simple guide for where you should direct questions and calls for help.

Problems with…	You should contact…
Logging into your ISP (Internet Service Provider); connecting to websites; launching web browser (e.g. Internet Explorer, Firefox)	Your ISP. The following links are provided to a couple of local ISP providers contact pages. If yours is not on this list, look up your ISP in a search engine and find a "Contact Us" page: Time Warner (Road Runner) & Verizon (FIOS)
Connecting & logging into to the UAlbany BLS website; accessing your course(s); interacting or participating in course activities, submission of assignment or file attachments in course.	The ITS Help Desk by using the ITS Help Request Form (http://www.albany.edu/its/help) or call (518) 442-4000. Press "1" for students. Then, press "2" for help with Blackboard.
Forgotten PIN when trying to get forgotten password.	The ITS HelpDesk at (518) 442-3700 or go to Lecture Center (LC) 27 at the UAlbany main campus with your SUNYCard and another form of identification. Press "1" for assistance when calling.

Please note that your instructor is not on this list. If you send inquiries about these technical problems, you will be referred to the resources listed above.

COURSE ACTIVITIES
Lectures & Readings: The course will feature assigned chapters, articles, or other PowerPoint readings as well as presentations.

Assignments: There will be several assignments in this class and you are expected to work alone or in teams as suggested in the assignment.

Hands-On Laboratory Exercises:
Project:

GRADING AND ASSESSMENT

The instructor will try to grade discussions, assignments, and labs fairly and return them within a reasonable time period with relevant comments and be available to discuss questions. Students are expected to set up an appointment to talk with the grader within a week of receiving a grade. Please let us know if there is a mistake in calculation – mistakes happen!

Late assignments, labs, or papers will receive 15% off per day late from the final possible grade for the exercise unless there is a legitimate excuse. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. Please also send any documentation to the instructor(s) as early as possible if you want to request any reasonable accommodations based on a disability.

Final grades will be graded on a curve using the following weightages. Based on the natural distribution of grades, students will be assigned final letter grades. Grading on a curve generally gives the person who performs the best in the class an "A" and other grades are decided based on their relative closeness to the score of the top performer and other students in the class.

Activity	Portion of Grade
Participation	10%
Assignments	30%
Hands-On Laboratories	20%
Project	40

The instructor is expected to get approval of the entire class prior to making any changes regarding the grading rubric.

COURSE SCHEDULE

Unit	Course Activities
Week 1	**Introduction to the Course** - Datasets for the course - Problem of Large datasets - Cleaning and organizing data **Lab:** Sorting and Searching Problems using Unix/Shell commands
Week 2	**Unsupervised Learning: Partitional Clustering Algorithms** - Problem Definition - Types of Clustering Algorithms - Distance Measures - K-Means Clustering Algorithm - Optimizing Clusters - Mean Shift Clustering - Gaussian Clustering Algorithm **Lab:** Develop and Implement a K-Means Algorithm
Week 3	**Unsupervised Learning: Hierarchical Clustering Algorithms** - Agglomerative Clustering Algorithm - Divisive Clustering - Visualizing Clusters (Dendograms and Heatmaps) - Applications of Clustering **Lab:** Data Analysis using Clustering Algorithm
Week 4	**Classification: Decision Trees** - Representation of Decision Trees - Metrics (Entropy and Information Gain) - Overfitting Problem - Using Continuous Variables - Developing Attack Trees **Lab:** Develop Security Decision Trees
Week 5	**Classification: Support Vector Machines** - Linear Classifiers (Logistic Regression, Naïve Bayes Classifier) - Support Vector Machines - Random Forest **Lab:** Use Software to classify data using support vector machines
Week 6	**Classification: Neural Networks** - Back Propagation Algorithm - Deep Neural Networks **Lab:** Use Deep Neural Network for Linguistics Analysis
Week 7	**Exam**
Week 8	**Statistical Inference: Frequentist Inference** - Frequentist Probability - Significance Testing - Confidence Intervals

	- Distributions **Lab:** German Tank Problem
Week 9	**Statistical Inference: Bayesian Inference** - Intro to Bayesian Theory - Maximum Likelihood Equation - Markov chain Monte Carlo - Nested Sampling **Lab:** Bayesian vs Frequentist Approach
Week 10	**Statistical Inference: Akaike information criterion** - Information Theory - Building Models - Fit **Lab:** Model Testing in MatLab
Week 11	**Network Analysis: Graphs and Trees** - Types of Graphs - Properties of Graphs - Graph Metrics - Representation of Graphs - Graphs in Real Life - Power Law and Heavy Tail Distribution **Lab:** Given a graph write program for computing graph metrics
Week 12	**Network Analysis: Link Analysis** - Web Search Ranking o PageRank o HITS o CHEI Rank - Network Robustness **Lab:** Rank your favorite website
Week 13	**Network Analysis: Social Network Analysis** - Introduction to Social Networks - Metrics for Social Networks - Visualizations **Lab:** Build your own social network
Week 14	**Advanced Topics /Snow Day Spillover**
Week 15	**Exam**

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

“GREAT” EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.
- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

School of Business
University at Albany State University of New York

BFOR 418

Malware Reverse Engineering

Syllabus

BFOR 418 Malware Reverse Engineering 3 credits
Instructor: Sanjay Goel
Class Time and Location: This class has yet to be scheduled. As a 3 credit course, it will meet either 3 times per week for one hour or two times per week for 90 minutes.

COURSE DESCRIPTION

Reverse engineering of malware is the process of examining the disassembled code of malware via a disassembler or hex editor to better understand how the code logic. The analysis helps understand the behavior of the malware by executing it in a quarantined environment to prevent contamination of the rest of the environment. The behavior could include files accessed, network communication, and processes launch etc. The class also covers fundaments of assembly language and hex editing which are useful for the code analysis. Students will also be able to use code disassemblers to generate assembly language code from machine-executable code. Students will also learn about different types of malware and how to finger print malware.

LEARNING OBJECTIVES

Overarching Goal: Understand the process of malware reverse engineering

Sub-Objectives: Student will learn to:
1. Read assembly language code
2. Use hex editors for code analysis
3. Run malware in sandbox environments
4. Disassemble machine executable code generate assembly level code
5. Analyze malware to identify its behavior
6. Use debuggers to analyze code
7. Fingerprint malware

TEXTBOOKS AND READINGS

Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software 1st Edition
by Michael Sikorski

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation 1st Edition by Bruce Dang

The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler 2nd Edition
by Chris Eagle

INSTRUCTOR CONTACT

Type	Information	Availability
Email	goel@albany.edu	I will try to answer your questions within 24 hours. In case you feel that your email gets buried in my mailbox feel free to send a reminder.
Phone	(518) 956-8323 (Office) (518) 956-8333 (Lab) (518) 387-9090 (Goel Mobile)	Typically, I am in the office / lab from 8:30am (08:30) to 4:30 (16:30) EDT Mondays – Fridays when not in class or meetings. If unavailable I can generally be reached via mobile, but only in cases of dire emergency.
Secretary	Set up an appointment by phone or email.	Please stop by Jennifer North, in the Dean's Suite to set up an appointment in case you can't reach me.
Virtual Chat	Skype (goelsahib) Google Hangout/Chat (goelsa@gmail.com)	Times can be scheduled by phone or email for individuals or groups.

TECHNICAL RESOURCES

If you experience technical problems that interrupt your ability to complete class work, it's important that you know where to seek help immediately. Here is a simple guide for where you should direct questions and calls for help.

Problems with…	You should contact…
Logging into your ISP (Internet Service Provider); connecting to websites; launching web browser (e.g. Internet Explorer, Firefox)	Your ISP. The following links are provided to a couple of local ISP providers contact pages. If yours is not on this list, look up your ISP in a search engine and find a "Contact Us" page: Time Warner (Road Runner) & Verizon (FIOS)
Connecting & logging into to the UAlbany BLS website; accessing your course(s); interacting or participating in course activities, submission of assignment or file attachments in course.	The ITS Help Desk by using the ITS Help Request Form (http://www.albany.edu/its/help) or call (518) 442-4000. Press "1" for students. Then, press "2" for help with Blackboard.
Forgotten PIN when trying to get forgotten password.	The ITS HelpDesk at (518) 442-3700 or go to Lecture Center (LC) 27 at the UAlbany main campus with your SUNYCard and another form of identification. Press "1" for assistance when calling.

Please note that your instructor is not on this list. If you send inquiries about these technical problems, you will be referred to the resources listed above.

COURSE ACTIVITIES

Lectures / Readings: The course will feature assigned chapters, articles, or other PowerPoint readings as well as presentations.

Cases: Case studies using actual examples to provide real-world relevance to class topics.

Assignments: There will be several assignments in this class and you are expected to work alone or in teams as suggested in the assignment.

Hands-On Laboratory Exercises: Laboratory exercises will be offered where students get hands-on experience using tools and techniques in the field. Laboratory associated exercises take around 1 – 1 ½ hour to complete and will have associated questions for which your answers will be graded. Lab exercises will often require installation of software on computers and completing the corresponding exercises. At the end of the exercise, you should delete the software installed on the machines.

GRADING AND ASSESSMENT

The instructor will try to grade discussions, assignments, and exams fairly and return them within a reasonable time period with relevant comments and be available to discuss questions. Students are expected to set up an appointment to talk with the grader within a week of receiving a grade. Please let us know if there is a mistake in calculation – mistakes happen!

Late assignments, labs, or papers will receive 15% off per day late from the final possible grade for the exercise unless there is a legitimate excuse. Missing any assessment without a verifiable legitimate excuse will result in a grade of zero. Please also send any documentation to the instructor(s) as early as possible if you want to request any reasonable accommodations based on a disability.

Final grades will be graded on a curve using the following weightages. Based on the natural distribution of grades, students will be assigned final letter grades. Grading on a curve generally gives the person who performs the best in the class an "A" and other grades are decided based on their relative closeness to the score of the top performer and other students in the class.

Activity	Portion of Grade
Exam 1	25%
Exam 2:	25%
Assignments & Hands-On Laboratories	50%

The instructor is expected to get approval of the entire class prior to making any changes regarding the grading rubric.

COURSE SCHEDULE	
Unit	Course Activities
Class 1	**Introduction to Malware and Malware Analysis** - Syllabus - Types of Malware - Basics of Malware Analysis **Lab: Malware Lab**
Class 2	**Understanding Assembly Language I** - Fundamentals of Assembly Language - Interpreting Assembly Code **Lab: Assembly Language Programming Lab I**
Class 3	**Understanding Assembly Language II** - Programming in Assembly Language **Lab: Assembly Language Programming Lab II**
Class 4	**HEX Editors I** - Understanding HEX Code - Different HEX Editors **Lab: HEX Programming Lab I**
Class 5	**HEX Editors II** - Using a HEX Editor **Lab: HEX Programming Lab I**
Class 6	**Malware Writing** - Writing simple malware - Polymorphic malware - Compression and Obfuscation techniques **Lab: Malware Writing Lab**
Class 7	**EXAM**
Class 8	**Sandboxing and Executing Malware** - Type of Sandboxes - Using a Sandbox - Interpreting results from Sandbox - Open Source Intel in identifying malware **Lab: Malware Analysis Lab I**
Class 9	**Disassembling Code** I - Use IDA Pro **Lab: Code Disassembly Lab I**
Class 10	**Disassembling Code** II - Other Disassembly tools **Lab: Code Disassembly Lab II**

Class 11	**Software Debuggers for Malware Analysis** - Exploring Software Debuggers - Using Software Debugger **Lab Exercise: Malware Analysis Lab II**
Class 12	**Analyzing Malicious Documents** **Lab Exercise: Document Analysis Lab**
Class 13	**Project Presentations** **Lab Exercise: None**
Class 14	**EXAM**

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

"GREAT" EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.

- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.
- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

Syllabus

BFOR 419
System Administration and Operating System Concepts (3 credits)

A practical study of the secure management of multiple internet connected server and workstation computers. System setup and periodic maintenance (with topics such as OS installation, filesystems, application server software builds, patching, performance monitoring) combined with issues of availability (including networking and remote access, backup and restores, user accounts) and interoperability issues.

Class Time and Location: This class has yet to be scheduled. As a 3 credit course, it will meet either 3 times per week for one hour or two times per week for 90 minutes.

Instructor: William Augustine
Office Hours: TBD

Website: Blackboard will be used to provide essential course materials, the most current syllabus, and assignments. No separate course website will be maintained.

Prerequisites: BFOR 100, BFOR 206
The course will build on concepts from that course and add several more.

Course Goals

By the end of the semester, you should be able to

1. set up and maintain multiple, well behaved, interdependent, secure Unix workstations and servers;
2. understand networked systems that provide the Internet's structure and the threats to which they might be exposed;
3. operate comfortably and proficiently at the UNIX shell level.

Required Textbook:
Linux Operations and Administration, 1st Edition
Copyright 2013
Alfred Basta | Dustin A. Finamore | Nadine Basta | Serge Palladino
ISBN-10: 111103530X
ISBN-13: 9781111035303

Supplemental readings will be distributed via Blackboard and/or in class.

Computer Access:
In order to complete assignments, you will need access to a modern computer on which you can run virtual machine hosting software (specifically, Oracle's VirtualBox) and where you will have the appropriate permissions to install and execute open source, security related software; such as but not limited to Nmap, Wireshark, and Metasploit.

Attendance

Attendance is mandatory for every class. Your in-class performance is key to your success in this course. Attendance, itself, is not graded. Instead, graded in-class activities and assignments constitute an important part of the course grade. It is unlikely you can maintain a passing average without consistent attendance. Missing class means the student earns an automatic zero for the activities or assignments missed. Because of the nature of the assignments, no make-up opportunities will be available.

Tardiness

Missing an assignment or activity that happened before a student arrives or after a student leaves also earns a zero. No make-up opportunities will be available.

If you know that it will be difficult for you to consistently get to class on time and stay for the entire period, you should take this course at a time that better fits your schedule. Being late frequently will likely negatively impact your grade for the course.

Withdrawal from the course

The drop date for the **????** semester is **????** for undergraduate students. That is the last date you can drop a semester length course and receive a 'W'. It is your responsibility to take action by this date if you wish to drop the course. In particular, grades of "incomplete" will not be awarded to students because they missed the drop deadline.

All important dates can be found in the University academic calendar, which is available online : http://www.albany.edu/registrar/????-academic-calendar.php

Academic Integrity

It is every student's responsibility to become familiar with the standards of academic integrity at the University. Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity. See http://www.albany.edu/undergraduate_bulletin/regulations.html

Course work and examinations are considered individual exercises. Copying the work of others is a violation of university rules on academic integrity. Individual course work is also key to your being prepared and performing well on tests and exams. Forming study groups and discussing assignments and techniques in general terms is encouraged, but the final work must be your own work. For example, two or more people may not create an assignment together and submit it for credit. If you have specific questions about this or any other policy, please ask.

The following is a list of the types of behaviors that are defined as examples of academic dishonesty and are therefore unacceptable. Attempts to commit such acts also fall under the term academic dishonesty and are subject to penalty. No set of guidelines can, of course, define all possible types or degrees of academic dishonesty; thus, the following descriptions should be understood as examples of infractions rather than an exhaustive list.

Syllabus

- Plagiarism
- Allowing other students to see or copy your assignments or exams
- Examining or copying another student's assignments or exams
- Lying to the professor about issues of academic integrity
- Submitting the same work for multiple assignments/classes without prior consent from the instructor(s)
- Getting answers or help from people, or other sources (e.g. research papers, web sites) without acknowledging them.
- Forgery
- Sabotage
- Unauthorized Collaboration (just check first!)
- Falsification
- Bribery
- Theft, Damage, or Misuse of Library or Computer Resources

Any incident of academic dishonesty in this course, no matter how "minor" will result in:
1. No credit for the affected assignment.
2. A written report will be sent to the appropriate University authorities (e.g. the Dean of Undergraduate Studies)
And may result in:
3. One of –

- A final mark reduction by at least one-half letter grade (e.g. B →B-, C- →D+),
- A Failing mark in the course, and referral of the matter to the University Judicial System for disposition.

Policies from Undergraduate Bulletin:
http://www.albany.edu/undergraduate_bulletin/regulations.html

Responsible Use of Information Technology
Students are required to read the University at Albany Policy for the Responsible Use of Information Technology available at the ITS Web Site:
https://wiki.albany.edu/display/public/askit/Responsible+Use+of+Information+Technology+Policy

Available Support Services - Reasonable accommodation
Reasonable accommodation will be provided for students with documented physical, sensory, cognitive, learning and psychiatric disorders. If you believe you have a disability requiring accommodation in this class, please notify the Disability Resource Center (CC130, 442-5490). That office will provide the course instructor with verification of your disability, and will recommend appropriate accommodations. In general, it is the student's responsibility to contact the instructor at least one week before the relevant assignment to make arrangements.

Missing Deadlines Due to Illness
Please be familiar with the University rules regarding missing deadlines due to health:
http://www.albany.edu/health_center/medicalexcuse.shtml

Assessment: By default, this is an A-E graded course.
Your achievement of these objectives will be assessed through in-class activities, assignments and exams. Material submitted late without prior approval will be penalized 20% for every day or part thereof.

COURSE SCHEDULE

Date	Topics	Readings	Assignments	
			Given	Due
Week 1	Introduction to Systems Administration OS Installation	Chapters 1,2		
Week 2	Secondary Storage Management Filesystems; Backup and Restore	Chapters 3,6	HW1	
Week 3	Commands and Scripts CLI	Chapters 4,5		
Week 4	Users Accounts Passwords; Authentication; Access Controls	Chapter 7	HW2	HW1
Week 5	Networking Configuration and defense	Chapters 8,11		
Week 6	Software Building; Configuring; Updates and Patches	Chapter 9		HW2
Week 7	***First Exam***			
Week 8	OS Installation and Operation Revisited Virtualization	Chapters 14	HW3	
Week 9	Internet Services HTTP; SMTP	Chapters 10,12		
Week 10	Enterprise Management Configuration Management; Policies	Chapter 13,15	HW4	HW3
Week 11	Resource and Performance Management	Chapter 16,22		
Week 12	Auditing Logging; Intrusion Detection	Chapters 19,21	HW5	HW4
Week 13	Interoperability	Chapter 17,18		
Week 14	The Kernel OS Concepts; Memory; Processes	Chapter 20		HW5
Finals Week	***Second Exam***			

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, either announced in-class or through email.

HW Project #1: The students will demonstrate their ability to create and subsequently back up a Unix system and user/application data. The more important task of restoring an archive is also involved.

HW Project #2: For this assignment the students will automate the creation and subsequent retirement of user accounts. A thorough understanding of authentication and permissions best practices will be required.

HW Project #3: Virtualization, emulation and simulation are powerful tools. Knowledge of their values and the ability to construct systems that employ these environments is exposed.

HW Project #4: Hosting user applications and their supporting system software is what servers do. This assignment requires the student to build a complex piece of open source software.

HW Project #5: In this final assignment, the student will evaluate the operation of a host-based intrusion detection system in coordination with a network security sensor.

GRADING RUBRIC		
Type	**% of Grade**	**Description**
2 Exams	40%	Two exams worth 20% each.
Homework Assignments	40%	There will be five assignments. The lowest grade will be dropped leaving four submissions (worth 10% of the total grade each). Late submissions will be penalized 20% of the assignment grade per day or part thereof.
Miscellaneous Assessments	20%	Various assessments that may include short (unannounced) quizzes based on the text and/or additional readings or directed in-class activities.

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY State University of New York

BFOR 420

National Cyber Security Challenge Problems

Syllabus

BFOR 420 National Cyber Security Challenge Problems 3 credits
Class Time and Location: This class has yet to be scheduled. As a 3 credit course, it will meet either 3 times per week for one hour or two times per week for 90 minutes.
Instructor: Sanjay Goel

COURSE DESCRIPTION

This course exposes students to national cyber security challenge problems that our National Labs are currently dealing with and is suitable for seniors who are majors in Digital Forensics, Computer Science, Mathematics, and Cyber Security. This is an experiential learning course where student teams will work closely with the faculty instructor and scientists in a National Lab or a Government Agency dealing with cyber security or intelligence problems. UAlbany has been invited to join a network of about 20 Universities under the INSURE program that facilities such experiential learning. The role of the scientists/directors at the national lab is to define the challenge problem along with a recorded overview of each problem; they will also provide another 15-18 hours of their time over the course of the semester supporting and interacting with the team. Students will work in teams on the project and will have weekly sessions with the faculty instructor who will review their work.

NATIONAL LABS/FEDERAL AGENCIES PARTICIPATING IN INSURE:

1. Argonne National Laboratory
2. Idaho National Laboratory
3. Indiana Office of Technology
4. Johns Hopkins University Applied Physics Laboratory
5. MITRE
6. National Institute of Standards and Technology
7. National Security Agency
8. Naval Surface Warfare Center Crane Division
9. New Jersey Office of Homeland Security and Preparedness
10. Oak Ridge National Laboratory
11. Pacific Northwest National Laboratory
12. Sandia National Laboratories

LEARNING OBJECTIVES

Overarching Goal: Learn to solve national challenge security problems

Sub-Objectives: Student will learn to:

1. Domain knowledge in a specialized area of cyber security and forensics
2. Solve abstract problems
3. Conduct independent research
4. Project Management
5. Think critically

TEXTBOOKS AND READINGS

Will vary depending on the problem set being investigated.

INSTRUCTOR CONTACT

Type	Information	Availability
Email	goel@albany.edu	I will try to answer your questions within 24 hours. In case you feel that your email gets buried in my mailbox feel free to send a reminder.
Phone	(518) 956-8323 (Office) (518) 956-8333 (Lab) (518) 387-9090 (Goel Mobile)	Typically, I am in the office / lab from 8:30am (08:30) to 4:30 (16:30) EDT Mondays – Fridays when not in class or meetings. If unavailable I can generally be reached via mobile, but only in cases of dire emergency.
Secretary	Set up an appointment by phone or email.	Please stop by Jennifer North, in the Dean's Suite to set up an appointment in case you can't reach me.
Virtual Chat	Skype (goelsahib) Google Hangout/Chat (goelsa@gmail.com)	Times can be scheduled by phone or email for individuals or groups.

TECHNICAL RESOURCES

If you experience technical problems that interrupt your ability to complete your work, it's important that you know where to seek help immediately. Here is a simple guide for where you should direct questions and calls for help.

Problems with…	You should contact…
Logging into your ISP (Internet Service Provider); connecting to websites; launching web browser (e.g. Internet Explorer, Firefox)	Your ISP. The following links are provided to a couple of local ISP providers contact pages. If yours is not on this list, look up your ISP in a search engine and find a "Contact Us" page: Time Warner (Road Runner) & Verizon (FIOS)
Connecting & logging into to the UAlbany BLS website; accessing your course(s); interacting or participating in course activities, submission of assignment or file attachments in course.	The ITS Help Desk by using the ITS Help Request Form (http://www.albany.edu/its/help) or call (518) 442-4000. Press "1" for students. Then, press "2" for help with Blackboard.
Forgotten PIN when trying to get forgotten password.	The ITS HelpDesk at (518) 442-3700 or go to Lecture Center (LC) 27 at the UAlbany main campus with your SUNYCard and another form of identification. Press "1" for assistance when calling.

Please note that your instructor is not on this list. If you send inquiries about these technical problems, you will be referred to the resources listed above.

COURSE ACTIVITIES

Lectures / Readings: Assigned based on the context of the problem being investigated

Cases: Case studies using actual examples to provide real-world relevance to class topics.

Assignments: Students will work on weekly deliverables, including, research, project work, and report writing.

GRADING AND ASSESSMENT

The grading for the class will be based on the work delivered, peer assessment, mentor assessment, and faculty assessment. The grading scheme may change based on the type of project being designed.

Activity	Portion of Grade
Instructor Assessment	40%
Mentor Assessment	20%
Peer Assessment	20%
Final Presentation	20%

Grading rubric can change based on the requirement of the sponsor organization and the type of project

COURSE SCHEDULE

Unit	Course Activities
Week 1	**Introduction to the class, Bidding for the Proposal, and Team Building** - Define the skill set required for the class and make compatible teams that have complementary skills to complete the project
Week 2-4	**Project Planning** - Students will work with the faculty and sponsor to develop a detailed project plan Interpreting Assembly Code - Students will have assigned weekly readings that they will present to the faculty instructor
Week 5-8	**Phase I** - Students work on project activities as laid out in the project plan - Students engage in research to investigate the problem at hand - Students present their research and progress in a weekly meeting with the faculty instructor - Challenges and issues are discussed with the sponsor as necessary - Students complete their Phase I deliverables including an intermediate report and plan their phase I presentation
Week 9	**Phase I presentation** - Students present their work via Video conferencing to the sponsoring organization - Students are evaluated on the presentation and provided feedback - Students provide peer feedback on their team members
Week 10-14	**Phase II** - Students take feedback from the Phase I presentation and make any changes necessary

Week 15	- Students have weekly meetings with the instructor to discuss progress on the project - Challenges and issues are discussed with the sponsor as necessary - Students complete their Phase II deliverables including an intermediate report and plan their phase II presentation
	Final Presentation - Students present their work either in-person or via video conferencing to the sponsoring organization - Students are evaluated and provided feedback - Students provide peer feedback on their team members

This schedule is subject to change and students are expected to be aware of any modifications to including, but not limited to: due dates, readings, exam dates, and project guidelines, announced via email, Blackboard announcements or during class hangouts.

ACADEMIC INTEGRITY & HONESTY

Students MUST comply with all University at Albany's standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** Non-compliance with academic integrity standards, will result in the student being reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Violations include: Giving or receiving unauthorized help on an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (e.g., words, ideas, information, code, data, evidence, organizing principles, or presentation style of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, purchase of prepared research, papers or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations. **If you have questions about academic integrity - ASK!**

"GREAT" EXPECTATIONS

- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.
- Students are expected to respectfully participate in the course and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material.
- If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible.
- Students are expected to provide reliable contact information and inform the instructor of any updates.
- Students are expected to contact the instructor via email, phone, or in person for reliable response.

- Students are expected to complete all assignments and readings as well as set up meeting times with the instructor as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of the course.