LSC Use Only No:	LSC Action-Date:	UWUCC USE Only No.	UWUCC Action-Date:	Senate Action Date:
		~~08-65~~ 09-10a	AP-10/27/09	App-12/1/09

Curriculum Proposal Cover Sheet - University-Wide Undergraduate Curriculum Committee

Contact Person **Rose Shumba**	Email Address: **shumba@iup.edu**
Proposing Department/Unit **Computer Science**	Phone **7-3166**

Check all appropriate lines and complete information as requested. Use a separate cover sheet for each course proposal and for each program proposal.

1. Course Proposals (check all that apply)

_____New Course _____Course Prefix Change _____Course Deletion

__X__Course Revision _____Course Number and/or Title Change __X__Catalog Description Change

***Current* Course prefix, number and full title**	***Proposed* course prefix, number and full title, if changing**
COSC316: Host Computer Security	

2. Additional Course Designations: check if appropriate

_____ This course is also proposed as a Liberal Studies Course.

_____ This course is also proposed as an Honors College Course.

_____ Other: (e.g., Women's Studies, Pan-African)

3. Program Proposals

_____Catalog Description Change _____Program Revision

_____New Degree Program _____Program Title Change _____Other

_____New Minor Program _____New Track

***Current* program name**	***Proposed* program name, if changing**

4. Approvals		**Date**
Department Curriculum Committee Chair(s)	waleed Farag	11/01/2008
Department Chair(s)	Chris J Shelton	11/10/08
College Curriculum Committee Chair		11/19/08
College Dean	John D. Eck	
Director of Liberal Studies *		
Director of Honors College *		
Provost *		
Additional signatures as appropriate: (include title)		
UWUCC Co-Chairs	Gail S Sechrist	11/6/09

* where applicable

Received
NOV 06 2009
Liberal Studies

Received
FEB 13 2009
Liberal Studies

NEW Syllabus of Record

COSC 316 Host Computer Security

3 class hours
0 lab hours
3 credits
(3c-0l-3cr)

I. Course Description

COSC 316 Host Computer Security.

Prerequisites: COSC 110 or equivalent course, as approved by instructor

Provides an introduction to the theory and concepts of host computer security. Topics include security and policy guidelines, attack strategies and attacker profiles, users and groups security, file systems and security, integrity management, cryptography basics, back-up utilities, auditing and logging, and strategies for defending user accounts. Designed as a practical hands-on course.

II. Course Outcomes

Upon successful completion of this course, the students will:

1. Write a suitable set of security policies for different scenarios.
2. Apply various access control techniques.
3. Compare the basic tools and techniques used to attack systems.
4. Explain the different types of attacks.
5. Specify procedures for password/username management.
6. Explore the use of security tools in defending user/group accounts.
7. Explore techniques for integrity management.
8. Demonstrate the use of logging, auditing, and backup techniques for security.
9. Explain the basic cryptography concepts.

III. Course Outline

Academic hrs

1. Overview of computer security — **3**
   a. Definition and discussion of computer security.
   b. Security problems in computing.

2. Attacks to Host Computer Systems — **3**

   a. Attacker profiles (hackers, crackers, script kiddies, spies, employees)
   b. Attacking strategies (social engineering, spyware, software vulnerabilities, malware)

3. Introduction to an operating system — **3**

   a. The operating system overview and functionality.
   b. Operating system utilities.
   c. Operating system user and administrative commands.

4. Identification and Authentication **3**

   a. Managing username and passwords.
   b. Password management utilities
   c. Authentication techniques (biometrics, RFID devices, Smart cards, one time passwords)
   d. Use of password cracking tools.

5. File systems and access control **6**

   a. File ownership and user groups.
   b. Strategies for defending group accounts
   c. Working with Files/directories
   d. Using File Manager

6. Integrity Management **3**

   a. Immutable and append only files
   b. Read only files
   c. Checksum and signatures
   d. Use of integrity checking tools

7. File System and security **3**

   a. Access control through file permissions
   b. Setting up access control lists
   c. Other file protection schemes
   d. Basic computer forensics methods
   e. Electronic records management
   f. Electronic evidence

8. Auditing, logging, backup **4**

   a. Log file utilities
   b. Rotating and tracking log files
   c. Protecting and viewing log files
   d. Operating system specific tools for auditing and logging
   e. Backing up file systems
   f. Linux tools for backup

9. Encryption for Host System	4
a. Symmetric encryption i. Cryptography and cryptanalysis b. Asymmetric encryption i. Public vs private key encryption ii. Digital certificates iii. Encryption utilities	
10. Policies and guidelines	3
a. Policy development b. Planning for security needs c. Outsourcing policy development	
11. Overview of physical security	3
a. Physical controls vs technical controls b. Coping with natural and artificial disasters	
12. Student presentation on security tools	2
13. Two in class exams	2
Total	**42**

Final exam (during final exam week)

IV. Evaluation Methods

1. **Lab exercises: 25%.** Each student is expected to do the following hands on in-class exercises: user account security, user group account management, defending accounts, file security management, auditing and logging, cryptography, backup and recovery and integrity management. All exercises use free downloadable security tools.
2. **Tool Research project (15%)**: The objective of the project is to expose students to the array of other security tools available, not covered in the course. Students research on the tool, develop a tutorial for the tool, do a class presentation which includes a demonstration of how the tool works, and finally comment on their experience of using the tool.
3. **Assignments: 15%**: Students will have 3 assignments to complete, which are non-lab based.
4. **Exams 45%**: Students will be evaluated on their understanding of the concepts presented using short essay questions on the readings and class material. There will be three exams: first exam (15%), a mid-term exam (15%) and a final exam (15%).

V. Grading scale

Grading Scale. The standard grading scale will be used. 90%+ =A; 80-89%=B; 70-79%=C; 60-69%=D; <60%=F.

VI: Textbook

Garfinkel, S., Spafford, G., and Schwartz, A., Practical Unix and Internet Security", Third Edition, 2003, ISBN "0596-003234"

VII: Attendance Policy

The policy will follow the guidelines as in the IUP Handbook.

VIII: Special Resource Requirements

None

IX. References:

1. Barrett, D., Silverman R., and Byrnes, R., Linux Security CookBook, First Edition, O'Reilly, 2003
2. Davis, J. and Dark, M, Defining a curriculum framework in Information Assurance and Security, 2003 ASEE Annual Conference, Nashville, TN, June 2003.
3. Garfinkel, S., Spafford, G., and Schwartz, A., Practical Unix and Internet Security, Third Edition, 2003, ISBN "0596-003234"
4. Lockhart, A., Network Security Hacks, 100 Industrial-Strength Tips and Tools; O'Reilly; First Edition; 2004.
5. Hatch, B., Lee, J., Kurtz, G., Hacking Linux Exposed: Linux Security Secrets and Solutions, McGraw-Hill, 2001.
6. Whitman, M., Mattford, H., and Shackleford, D., Hands On Information Security Lab Manual, Thompson Technology, 2006.
7. Tomsho, G., Tittel, E., and Johnson, D., Guide to Networking Essentials, Thomson, Course Technology, 2007.

COSC 316 Host Computer Security

0 lab hours
3 lectures hours
3 credits
3c-0l-3sh

I. Course Description

COSC 316 Host Computer Security 3c-0l-3sh

Prerequisites: COSC 110 or equivalent programming course, junior standing or permission of instructor.

Provides an introduction to the theory and concepts of computer security in networked systems. The course will look at security issues and policies with regard to hardware, software development, databases, operating systems and networks as well as the use of encryption. The more common attacks on systems will be covered. Vulnerability assessment tools and techniques for defending systems will be explored in various projects.

II. Course Objectives

Upon successful completion of this course, the students will:
1. model the security risks in a network.
2. write a suitable set of security policies for different scenarios.
3. apply various access control techniques.
4. become familiar with the basic tools and techniques used by hackers to attack systems.
5. assess network and system vulnerabilities to these attacks and learn countermeasures.
6. log data on simulated attacks and analyze the logs and other audit controls.
7. gain skill in cyberforensics.
8. be familiar with existing and proposed legislation related to all types of cybercrime.
9. be aware of the importance of ethical conduct.

III. Course Outline

A. Major categories of threats (Attack) 2 weeks
- Wiretapping
- Impersonation/social engineering
- Foot printing
- Packet Sniffing

B. Network attacks/access controls 1 week
- Access controls
- Denial of service
- Email/web hacks
- Other forms of attack
- Risk analysis

C. Security goals/policies. 1 week

D. Security in networks and distributed systems (Defend) 2 weeks
- Network overview: Traffic control
- Firewalls/proxy servers
- Protection schemes.
- Vulnerability assessment tools

E. Audit controls, Logging and log analysis (Convict) 1 week

F. Basic Encryption and Decryption /Protocols and Practices. 2 weeks

G. Program security. • Viruses and other malicious code • Controls against program threats	1 week
H. Protection in General Purpose Operating Systems	1 week
I. Database/web security	1 week
J. Legal Issues in Computer Security	1 week
K. Ethical Issues in Computer Security	1 week
Total=	**14 weeks (including two class tests)**

IV. Evaluation Methods

1. Classroom activities and exercises: 30%. There will be graded assignments involving hands-on exercises or problem solving in the classroom. Outside class readings are required in association with these activities.

2. Assignments: 30%. Students will have 3 research papers to complete outside of class time.

3. Exams and quizzes. 40%. Students will be evaluated on their understanding of the concepts presented using short essay questions on the readings and class material. There will be several quizzes (collectively counting 10%), a mid-term exam (15%) and a final exam (15%).

4. Grading Scale. The standard grading scale will be used. 90%+ =A; 80-89%=B; 70-79%=C; 60-69%=D; <60%=F.

V. Required Textbook:

Garfinkel, Simson CISSP, Gene Spafford (1998), Practical UNIX & Internet Security, O'Reilly & Associates, ISBN: 1565921488
Supplemented by:
Hatch, Brian, James Lee, and George Kurtz (2001), Hacking Linux Exposed: Network Security Secrets and Solutions, Osborne/McGraw Hill, ISBN 0-07-212127-0

VI. Special Resource Requirements

None.

VII. Bibliography

1. Brenton, Chris (1999), Mastering Network Security. Network Press, (SYBEX)
ISBN 0-7821-2343-0

2. Denning, Dorothy E. (1999), Information Warfare and Security. Addison-Wesley, ISBN 0-2014-3303-6

3. Krause, Micki, Harold F. Tipton, Editors (2000), Handbook of Information Security Management. Auerbach, ISBN 0-8493-9829-0

4. Krist, Martin A. (1999), Standard for Auditing Computer Applications. Auerbach, ISBN 0-8493-9983-1

5. McClure, Stuart, Joel Scambray, and George Kurtz (1999), Hacking Exposed: Network Security Secrets and Solutions, Osborne/McGraw Hill, ISBN 0-07-212127-0

6. Nichols, Randall K.,Daniel J. Ryan, and Julie J.C.H. Ryan,(2000), Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves. McGraw Hill, ISBN 0-07-212285-4

7. Schwartau, Winn (1999), Time-Based Security, Practical and Provable Methods to Protect Enterprise and Infrastructure Networks and Nation. Interpact Press, ISBN 0-9628700-4-8

8. Schneier, Bruce (1996), Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley and Sons, ISBN 0-471-11709-9

9. Scott, Charlie, Paul Wolfe, and Mike Erwin (1999), Virtual Private Networks. 2nd Edition O'Reilly and Associates, ISBN 1-56592-529-7

10. Tiwana , Amrit (1999), Web Security. Butterworth-Heinemann, ISBN 1-55558-210-9 2nd Edition

11. Class web site: http://penguin.nsm.iup.edu/security/bibliography.htm