
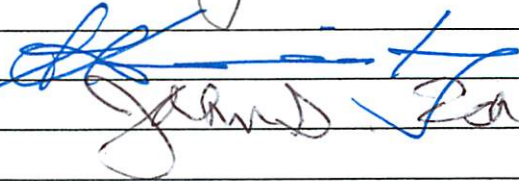
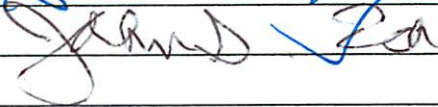


LSC Use Only No:	LSC Action-Date:	UWUCC USE Only No. 09-106 08-66	UWUCC Action-Date: App-10/27/09	Senate Action Date: App-12/1/09
------------------	------------------	---------------------------------------	------------------------------------	------------------------------------

**Curriculum Proposal Cover Sheet - University-Wide Undergraduate Curriculum Committee**

Contact Person <b>Waleed Farag</b>	Email Address <b>farag@iup.edu</b>
Proposing Department/Unit <b>COMPUTER SCIENCE</b>	Phone <b>7-7995</b>

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

<b>1. Course Proposals (check all that apply)</b> <input type="checkbox"/> New Course <input type="checkbox"/> Course Prefix Change <input type="checkbox"/> Course Deletion <input checked="" type="checkbox"/> Course Revision <input type="checkbox"/> Course Number and/or Title Change <input checked="" type="checkbox"/> Catalog Description Change		
<b>COSC 356 Network Security</b> <i>Current Course prefix, number and full title</i>		<b>COSC 356 Network Security</b> <i>Proposed course prefix, number and full title, if changing</i>
<b>2. Additional Course Designations: check if appropriate</b> <input type="checkbox"/> This course is also proposed as a Liberal Studies Course. <input type="checkbox"/> Other: (e.g., Women's Studies, Pan-African) <input type="checkbox"/> This course is also proposed as an Honors College Course.		
<b>3. Program Proposals</b> <input type="checkbox"/> New Degree Program <input type="checkbox"/> Program Title Change <input type="checkbox"/> Program Revision <input type="checkbox"/> New Minor Program <input type="checkbox"/> New Track <input type="checkbox"/> Other		
<i>Current program name</i>		<i>Proposed program name, if changing</i>
<b>4. Approvals</b>		
Department Curriculum Committee Chair(s)	waleed Farag	Date 11/10/2008
Department Chair(s)		11/10/08
College Curriculum Committee Chair		11/19/08
College Dean		
Director of Liberal Studies *		
Director of Honors College *		
Provost *		
<b>Additional signatures as appropriate:</b> (include title)		
UWUCC Co-Chairs	Gail Sedquist	11/6/09

\* where applicable

Received

FEB 13 2009

Liberal Studies

**Part-II Description of the Curriculum Change**

**1. Revision to Syllabus of Record**

See Attachment (next page) for the revised syllabus of record.

**2. Summary of the proposed revisions**

The course content was changed to address the problems listed below. A section reviewing basic networking concepts is introduced first. Course outlines were updated with new emerging technologies such as IDS, IPS, biometrics, etc. The bibliography has been completely updated with most recent published literature in the field. Finally, the course prerequisite has been modified to require both COSC 316 and COSC/IFMG 352.

**3. Justification/rationale for the revision**

After teaching the Information Assurance (IA) curriculum for a number of years, several issues have been raised by various faculty members teaching those courses and by some students too. The main source of these issues is the existence of some overlap among these courses. To respond to these issues and strengthen our IA track the contents of several courses ought to be modified simultaneously. Collaborative efforts have been undergoing to minimize that overlap and this proposal represents modifications to COSC 356, Network Security.

The change in the course prerequisite and the early coverage of a section reviewing networking basics were necessary to ensure that students have sufficient network background before taking the course.

Another important motivation behind these changes is that the department is preparing itself to be reaccredited by the National Security Agency (NSA) as a Center of Academic Excellence in Information Assurance Education. Therefore, our IA curriculum needs to be updated and changed in accordance with their recommendations presented in Committee on National Security Systems (CNSS) instructions 4011 and part of 4013.

**4. The old syllabus of record**

Attached.

**Part-III Letters of Support or Acknowledgement**

N/A

## **COSC 356 Network Security**

3 class hours  
0 lab hours  
3 credits  
(3c-01-3cr)

### **I. Catalog Description**

#### **COSC 356 Network Security**

3c-01-3cr

**Prerequisite:** COSC 316 and either COSC 345 or COSC/IFMG 352

Explores mechanisms for protecting networks against attacks. Emphasizes network security applications that are used on the Internet and for corporate networks. Investigates various networking security standards and studies methods for enforcing and enhancing those standards.

### **II. Course Outcomes**

Upon successful completion of this course, the student should be able to:

- A. Recognize the basic working principles of computer networks.
- B. Identify threats to network security.
- C. Distinguish between various protocols employed to secure networks.
- D. Utilize network security tools.
- E. Specify procedures for defending network systems.
- F. Develop network security policies.
- G. Specify procedures for recovery from attacks on networks.

### **III. Detailed Course Outline**

1. Review of Networking Fundamentals (3 hours)
  - Network reference models (OSI and TCP/IP)
  - Network protocols running at various layers (sliding window, PPP, CSMA/CD, IP, TCP, UDP, DNS, etc.)
  - Application layer issues
2. Network Security Concepts (3 hours)
  - Network security definition
  - Network protection mechanisms
  - Authentication techniques (CHAP, Kerberos, biometrics, etc.)
  - Intranets and Extranets

- Hardening software and hardware
  - Network address translation
3. Attacks to Networks and Countermeasures (10 hours)
    - Attackers categorization and motivations
    - Basic attacks (software exploits, Math attacks, password guessing, etc.)
    - Malicious software
    - Identity attacks (replay, session hijacking, etc.)
    - Distributed denial of service attacks
    - Network security countermeasures
  4. World Wide Web and Internet Security (6 hours)
    - Vulnerabilities in the WWW
    - Email and instant messenger security challenges
    - FTP and remote access security issues
  5. Encryption Mechanisms for Network Operations (4 hours)
    - Hashing algorithms and digital signature
    - Symmetric and asymmetric encryption algorithms
    - Public key infrastructure
    - Digital certificates and key management
    - Applications of cryptography in network security
  6. Security Protocols (6 hours)
    - Secure Socket Layer and Transport Layer Security (SSL/TLS)
    - Secure HTTP (HTTPS)
    - Virtual Private Networks (VPNs) and tunneling protocols (PPTP & L2TP)
    - Directory services (LDAP)
    - Wireless security protocols (WEP, WTLS, etc.)
  7. Intrusion Detection and Prevention Systems (4 hours)
    - Categories of IDS and IPS
    - Components and deployment of IDS
    - Maintenance and performance evaluation
  8. Organizational Security Issues (4 hours)
    - Risk analysis and network modeling
    - Assessing the security needs of an enterprise
    - Security policies for network operations
    - Disaster recovery and business continuity
  9. Two class tests (2 hours)

**Total = 42 hours**

Final Exam (during final exam week)

#### IV. Grading Scale

The standard grading scale will be used.

90%+=A; 80-89%=B; 70-79%=C; 60-69%=D; below 60%=F.

#### V. Evaluation Methods

20% Computer Lab assignments, attendance and participation.

50% Examinations. Two in-class exams and a final exam. Examinations can be given in various formats.

30% Projects. Selected projects covering various aspects of network security, especially those that cannot be covered exhaustively in class discussions. This can include research paper(s), case studies, etc.

#### VI. Textbook

Mark Ciampa, "Security+ Guide to Network Security Fundamentals", 2nd Edition Course Technology Incorporated, 2005, ISBN "0-619-21566-6".

#### VII. Attendance Policy

Class attendance is regarded as being very important. Individual faculty may establish penalties for excessive numbers of unexcused absences. Excused absences will be allowed for illness, family emergencies, and involvement in university activities, such as sports. The penalties specified will meet university guidelines and be distributed to students with the course syllabus on the first day of class.

#### VI. Special Resource Requirements

None

#### VII. Bibliography

1. Benton, C. (2002), *Mastering Network Security*, 2<sup>nd</sup> Ed., SYBEX, Inc., San Francisco.
2. Bishop, M. (2005), *Introduction to Computer Security*, Addison-Wesley, Reading, MA.
3. Brown, K. (2000), *Programming Windows Security*, Addison-Wesley, Reading, MA.
4. Ciampa, M. (2005), *Network Security Fundamentals*, 2<sup>nd</sup> Ed., Thomson Course Technology, Boston, MA.
5. Forouzan, B. (2008), *Cryptography and Network Security*, McGraw-Hill, Inc., New York, NY.
6. Frisch, A. (2002), *Essential System Administration*, 3<sup>rd</sup> Ed. O'Reilly & Associates, Inc., Sebastopol, CA.
7. Himma, K. (2007), *Internet Security*, Jones and Bartlett Publishers, Sudbury, MA.
8. Garfinkel, S., Spafford, G., and Schwartz, A. (2003), *Practical UNIX and Internet Security*, 2<sup>nd</sup> Ed. O'Reilly & Associates, Inc., Sebastopol, CA.
9. Hatch, B. and Lee, J. (2002), *Hacking Linux Exposed: Linux Security Secrets & Solutions*, 2<sup>nd</sup> Ed., Osborne/McGraw-Hill, Berkeley, CA.
10. Russell, R., Kaminsky, D., Puppy, R., and Grand, J. (2002), *Hack Proofing Your Network*, 2<sup>nd</sup> Ed., Syngress Publishing, Rockland, MA.
11. McClure, S., Scambray, J., and Kurtz, G. (2005), *Hacking Exposed*, 5<sup>th</sup> Ed., McGraw-Hill/Osborne Media, Berkeley, CA.

12. Schneier, B. (2004), *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, Somerset, NJ.
13. Stallings, W. (2006), *Network Security Essentials: Applications and Standards*, 3<sup>rd</sup> Ed., Prentice-Hall, Inc., Upper Saddle River, NJ.
14. Stallings, W. (2006), *Cryptography and Network Security: Principles and Practices*, 4<sup>th</sup> Ed., Prentice-Hall, Inc., Upper Saddle River, NJ.
15. Wadlow, Thomas A. (2000), *The Process of Network Security: Designing and Managing a Safe Network*, Addison Wesley Longman, Inc., Reading, MA.

## **COSC 356 - Network Security**

3 lecture hours  
0 lab hours  
3 credits  
(3c-0l-3sh)

### **I. Catalog Description**

COSC 356                      Network Security                      3c-0l-3sh

Prerequisite: COSC 316 or COSC/IFMG 352

Explores mechanisms for protecting networks against attacks. Emphasizes network security applications that are used on the Internet and for corporate networks. Investigates various networking security standards and explores methods for enforcing and enhancing those standards.

### **II. Course Objectives**

Upon successful completion of this course, the student should be able to:

- A. Utilize network security tools.
- B. Specify procedures for defending network systems.
- C. Develop network security policies.
- D. Recognize threats to network security.
- E. Deter attacks on network systems.
- F. Specify procedures for recovery from attacks on networks.

### **III. Detailed Course Outline**

- 1. Network Security Modeling (6 hours)  
A look at possible security violations and the concerns they raise for securing networks. Accessing the security needs of an establishment; evaluating and choosing various security products and policies. An overview of the common security services that is currently available.
- 2. Network Systems Communication (3 hours)

Overview computer network systems communication. An examination of the frames and packets of various protocols that travel the Internet. Analysis of data at the various layers on the Internet using the Open Systems Interconnection (OSI) Reference Model and comparing with the (Institute of Electrical and Electronic Engineers (IEEE) implementation. A study of different routing mechanisms and routing tables. Comparison and contrast of connectionless and connection-oriented communications.

3. Security Breaches of Interconnected Devices (6 hours)

A study of the communication properties of network transmissions; digital communications; electromagnetic interference, etc. A look at the various hardware devices on the network and their contribution to the security of the overall network.

4. Authentication and Encryption Control (3 hours)

Study of methods of ensuring that both ends of a communications connection are identifiable and verifiable. Examination of various cryptographic methods. Comparing and contrasting public key and private key cryptographic systems.

5. Access Control and Detection Systems (6 hours)

A look at systems for enforcing access control policies: firewalls and proxy servers. Analysis of packet filtering devices and their respective methods of approach to security enhancement. An examination of the strengths and weaknesses of intrusions detection systems.

6. Virtual Private Networks (6 hours)

An explanation of how encryption and authentication of a communication channel on a public network constitute a virtual private network. The process of ensuring the security of a virtual private network. Examination of some alternatives to virtual private networks.

7. Averting Intruders and Viruses (6 hours)

Establishing the meanings and differences between viruses, Trojans, and worms on the network. A look at various preventive measures used in combating such intrusive elements.

8. Security Design Issues (4 hours)

Analysis of the threats that the network system faces. A look at various principles that go into the design on security policies. Design of an authentic security policy.

9. Two class tests  
(2 hours)

---

Total = 42  
hours

#### IV. Evaluation Methods



- 20% Homework assignments and Research paper.
- 40% Examinations. Two in-class exams and a final exam all of which count equally toward the 40%. Examinations consist of short-answer, analysis, and what-if questions.
- 40% Project. Selected projects covering various aspects of network security, especially those that cannot be covered exhaustively in class discussions.

Grading Scale: The standard grading scale will be used.

90%+=A; 80-89%=B; 70-79%=C; 60-69%=D; below 60%=F.

## V. Required Textbook(s), Supplementary Books and Readings

Maiwald, Eric (2000), *Network Security: A Beginner's Guide*, Osborne/McGraw-Hill, Boston, MA.

Several handouts will be given to provide students with guidance with the projects. The professor has other related material that will be placed on reserve for students' use during the progress of the course.

## VI. Special Resource Requirements

None

## VII. Bibliography

1. Benton, Chris (1999), *Mastering Network Security*, SYBEX, Inc., San Francisco.
2. Brown, Keith (2000), *Programming Windows Security*, Addison-Wesley, Reading, MA.
3. Frisch, A. and Loukides (1995), *Essential System Administration*, 2<sup>nd</sup> Ed. O'Reilly & Associates, Inc., Sebastopol, CA.
4. Garfinkel, S., Spafford, G., and Russell D. (1995), *Practical UNIX and Internet Security*, 2<sup>nd</sup> Ed. O'Reilly & Associates, Inc., Sebastopol, CA.
5. Hatch, B., Lee, J., Kurtz, G. (2001), *Hacking Linux Exposed: Linux Security Secrets & Solutions*, Osborne/McGraw-Hill, Berkeley, CA.
6. Russell, R. and Cunningham S. (2000), *Hack Proofing Your Network: Internet Tradecraft*, Syngress Publishing, Rockland, MA.
7. Scambray, J. and McClure, S. (2000), *Network Security Secrets & Solutions*, McGraw-Hill, Boston, MA.
8. Schneier, B. (2000), *Digital Security in a Networked World*, John Wiley & Sons, Somerset, NJ.
9. Stallings, W. (2000), *Network Security Essentials: Applications and Standards*, Prentice-Hall, Inc., Upper Saddle River, NJ.
10. Wadlow, Thomas A. (2000), *The Process of Network Security: Designing and Managing a Safe Network*, Addison Wesley Longman, Inc., Reading, MA.