Course Number: 3460:453/553
Course Name: Computer Security
Course Credits: 3
Schedule: intermittent (recent offerings – Fall 07)

Syllabus Date: 10/8/07
Prepared By: Dr. Kathy J. Liszka

Prerequisites: 3460:316 or equivalent or permission

Text: none

**Bulletin Description:** Principles of computer security — cryptography, authentications, secure network protocols, intrusion detection and countermeasures.

**Detailed Description:**
We will cover a wide range of topics including privacy, spam techniques, phishing, pharming, viruses, worms, network security, intrusion detection, web attacks and rootkits. There will be weekly papers to read and answer questions on and a lab accompanying each topic. This is not a hacking class, although some hacking techniques will be studied to understand how vulnerabilities are exposed and systems and software are exploited.

**Course Goals:**
The student will be aware of the variety of topics in computer security. Some hands on experience with tools in a computer lab that is isolated from the campus network and the Internet will give the students an opportunity to work with intrusion detection software, port scanning, packet sniffing, and other various network security tools. Cryptography and steganography tools will also be used.

**Topics:**
1. Privacy 7. Email forging
2. Identity theft 8. Phishing and pharming
3. Footprinting 9. Steganography
4. Scanning 10. Cryptography
5. Packet sniffing 11. Viruses, Worms and Rootkits
6. Firewalls

**Computer Usage:**
A special lab networked with a switch and/or a hub (depending on the week’s lab exercise) will be set up that is separated from the campus networks and the Internet.

**References:**