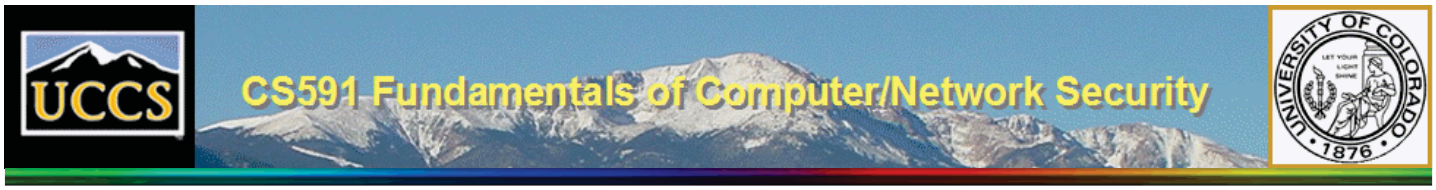

Course No.:	CS 591	Instructor:	C. Edward Chow
Class Time:	MW 5:50-7:05 pm	Office Address:	ENS 186
Class Room:	EN107	Office Hour:	**MW: 5:20-5:50pm; 7:05-7:35pm;** T:1-2pm
Office Phone:	255-3110	Email:	chow@cs.uccs.edu; cedwardchow (screenname) on MS Messenger or use my email address to establish contact.

4011 & 4013

CS5910 is one of core UCCS CS courses for the IA curriculum that was recognized by NSA and CNSS as meeting the CNSS 4011/4013 standards.

Course Objective:

> Introduction to the study of computer and network security from the view of information warfare. Topics include information system threats, vulnerabilities and defensive mechanisms, including cryptography, authentication, digital signatures, PKI, vulnerability analysis, IDS/firewall..

Course Outline (with links to presentation or related web pages):

- Introduction to Computer and Network Security
  - Secure Smart Grid
  - NERC CIP-005 as an Example of Security Policies and Security Standards.
- Basic Cryptography
  - Cryptography (Chapter 5).
  - Cryptoanalysis Exercise.
  - Tanenbaum Chapter 8.
  - Secure Web Access
- Network Attacks
  - Penetration Testing
  - Backtrack: Nessus/Metaspolit
  - Buffer Overflow Attack and Defense, related tools.
- Network Defense
  - Firewall
  - IDS
  - DDoS and Autonomous Anti-DDoS Defense.
  - Secure Collective Network Defense.

  Security Protocols
- Passwords
  - Security Engineering Chapter 3.
  - Linux Pluggable Authentication Modules (PAM).
- Access Control
  - MAC: SELinux
  - Secure Information Sharing.
- Multilevel Security

Grades:

> midterm(20%), final exam(20%), homework assignments(40%), web research/development project(20%)

Grade Query Web page

Class Info:

Class email list:You can send class related email to cs591-l@uccs.edu. Email to this mailing list will be forwarded to all cs591 class email accounts on uccs.edu. Use with caution.

Fall 2009 Class photo Album

Spring 2007 Class photo Album

F2005 Class photo Album

Please create a cs591 personal web page on walrus machines with your personal photo, basic vita, your interests in this class, and including later on the potential semester projects that you may work on . Note that in Unix system, your personal web site will be located in a subdirectory called public_html of your home directory. I have created a cs591 directory under public_html and a images subdirectory under cs591. Put your photo image file there with filename <login>.jpg, where <login> is your ufp account name. Reference it as <img src="images/*login*.jpg"> in your cs591 web page. This will allow your classmates to find common interests and know each other. I will use a Perl script to copy your photo images and create a class photo album. See http://cs.uccs.edu/~cs301/graphics/scanning.htm for scanning your personal photo. If you do not have recent photo, drop by my office. I can take it with my digital camera. You can also use my personal web page as a template. If you do not know how to setup your personal web page, drop by my office and I will help you get started. This is part of your hw#1.

If you use Windows system at home, try to use free SSH Secure Shelll software package with SSH Secure Shell Client,/Secure File Transfer Client, from http://www.ssh.org/support/downloads/secureshellwks/non-commercial.html, to login to CS Unix machines. It is secure since the password is not transmitted as clear text and all data are encrytped.
You can also setup xterm over ssh http://www.linuks.mine.nu/windows/sshx.html

Through Microsoft MSDN Academic Alliance program, our EAS system admin will setup an account for you on http://msdn07.e-academy.com/elms/Storefront/Home.aspx?campus=ucoloradohae_cs to download the software packages such as Vista, WinXP, Win2003/2008 Server, Visual Studio 2005/2008, SQL2005, visio2003 for the exercises/projects of this class.

We have set up a blade server system in SENG 212 server room with VMware vSphere software for creating/managing virtual machines in our homework exercises/semester projects and for iCTF competition preparation. In EN 138, 233, and SENG A208 lab, you can use vCenter client application on the desktop to access and configure these virtual machines. In SENG A210, we have one Dell Precision T3500 running Win2008, it contains special IDA pro/Hex-Rays Disassembler for reverse engineeing and scanning malicious software. You can install vCenter client on your own PC to access the vSphere blade server system. If you feel the response time of your Internet connection to these servers is too slow, you can download and install the vmware server software in you own PC to configure and run the virtual machines.

Disability Service:

If you have a disability for which you are requesting an accommodation, you are encouraged to contact the Disability Services Office within the first week of classes. The Disability Services Office is located in Main Hall #105. (Phone # is 262-3354.)

Text:

"Security Engineering " Ross Anderson. He just put this book online. You can purchase hard copy if you like

"Security Engineering," Ross Anderson. He just put this book online. You can purchase hard copy if you like from John Wiley & Sons, ISBN 0-471-38922-6.

References

- Glossary:
  - Internet Security Glossary: rfc2828 by Bob Shirey of GTE/BBN May 2000
  - National Informaiton Assurance (IA) Glossary by CNSS, revised May 2003.
- Related Textbooks:
  - Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing," 2003.
  - Matt Bishop, “Computer Security”
  - William Stallings. “Network Security Essentials: Applications and Standards.”
  - Kaufman, Perlman, Speciner. “Network Security: Private Communication in a Public World”.
  - Chapter 8 of Tanenbaum's Computer Networks.
- Interesting examples of exploit
- Os Hardening wiki.
- Cross Domain Solution wiki.
- UCCS iCTF 2006 wiki.
- Prof. Eugene H. Spafford's Keynote Speech, "What Comes Next in Infosec Research?", September 2003.
- Secure Programming for Linux and Unix HOWTO, by David Wheeler.
- Related Security Class Web Site:
  - Professor Vitaly Shmatikov's CS378: Network Security and Privacy
  - Stanford's CS155: Computer and Network Security
- SHA-1 is broken in Bruce Schneier’s Crypto-Gram Newsletter, 3/15/2005.
- Slammed! An inside view of the worm that crashed the Internet in 15 minutes, by Paul Boutin, July 11 2003 Wire magazine.
  - Nice diagram on BGP message volume during attack
  - Nice diagram on the number of jammed routes (cisco inferno), shows it took 24 hours to stamp out the worm.
  - Screendump of a more complete slammer code, including the whole UDP payload.
- The Spread of the Sapphire/Slammer Worm, by David Moore Vern Paxson Stefan Savage Colleen Shannon Stuart Staniford Nicholas Weaver.
  - Contains info about
    - original advisory from David L it chfield of NGSSoftware,
    - the disassembly code w it h annotation at eeye.com, it does not include buffer overflow part of the payload.
    - the binary and disassembly code (no annotation) at immun it ysec.om
- Reflections on Trusting Trust, by Ken Thompson’s 1983 Turing Award lecture.
  - It talks about self-reproducing program and Trojan horse.
  - Comment on moral and “whiz kid” hacker.
  - “You can't trust code that you did not totally create yourself.”
  - “No amount of source-level verification or scrutiny will protect you from using untrusted code.”
- W32/Mydoom@MM Virus info from McAfee Virtual Information library.
  - BBC new on mydoom.
  - **Method of Infection:**
    - Hosts Infected by executing the email attachment w it h virus.
    - Copy it self to %SysDir%\taskmon.exe
    - Create the following registry entry to hook Windows startup: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "TaskMon" = %SysDir%\taskmon.exe
    - Create %SysDir%\shimgapi.dll (4,096 bytes)
    - Inject shimgapi.dll into the EXPLORER.EXE upon reboot via this registry key: HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 "(Default)" = %SysDir%\shimgapi.dll
    - Harvest email addresses by searching for files w it h wab, adb, tbb, dbx, …, extension.
      - It avoids certain addresses including .gov, .mil, Berkeley , bsd,…!
    - Create new email addresses using harvested domain name w it h a set of common usernames.

        - Send emails via it s own SMTP engine.
        - When run after 2/1/2004 16:09:18 (UTC), it changes its behavior from mass mailing to initiating a denial of service attacks, 64 threads with HTTP GET requests to port 80 of www.sco.com.
    - **Peer to Peer Propagation**. Copies itself to KaZaa Shared directory
    - **Remote Access Component:** Open/listen TCP 3127 and 3198 ports
- IA Related Web Sites