As: CS490s Companion to CS422 (Networks)

**Intended Audience**
- This version of the class is addressed to advanced undergraduate students who have a special interest in networking, as CS422 is an optional course in the CS curriculum. In order to provide value to CS422 students who have already taken CS390s, this class does not discuss buffer overflows, but focuses on networking vulnerabilities in drives, protocols and applications.

**Format**
- One hour weekly lectures, two in-class quizzes, and 3 lab assignments.

**Focus: Secure Network Programming**
- Shell and shell scripting
- Concepts in secure network protocols: Nonces, randomness, authentication, encryption
- Common network protocols (TCP, UDP, FTP, SMTP, HTTP, Telnet, POP, IMAP, DNS)
- Filesystem utilities and shell built-ins
- Programmers' tricks (e.g., environment variables, command injection)
- Introduction to network intrusion detection
- Resource exhaustion vulnerabilities
- Race conditions (including symlinks)
- Robust programming and error handling
- Block and file systems management
- Introduction to IPS/IDS

**External References and Source Material**

- No single reference covered every aspect of the class as discussed in lectures. Material covered was based on the contents of lectures, and the following sources:
  2. Secure Programming for Linux and Unix HOWTO by David A. Wheeler
  3. KARUS Guide to Building Secure Web Applications and Web Services (Free)

**Class Evaluation**

**Overall class rating:** 4.4/5 (HIB)

**Overall instructor (P. Meunier) rating:** 4.5/5 (HIB)

**Worthwhile learning experience:** 4.5/5 (HIB)

**Improved my skills and understanding:** 4.4/5 (HIB)

**Increased my interest in computer science substantially:** 3.8/5 (HIB)

**Work requirements were too much:** 2.0/5 (LIB)

**Concepts were too difficult:** 1.8/5 (LIB)

**Anonymous comments:**

- "Wow, this was the first CS class that seemed relevant to the real world! Should be a requirement for all CS majors. Dr. Meunier was an excellent instructor & adapted his style to student needs as class progressed. This class, though, might be over the heads of some people who lack experience."
- "I especially like this class because of its practical application -- what we learn is useful. I hope it will be offered again, eventually as a 3 credit course."
- "Show more examples."
- "Much of this course seemed focused, especially towards the end, on web security issues, which are obviously valid, but many of us, such as myself, have never seen these technologies, so it is much more difficult to understand what is being said."

**As: Independent Short Course**

**Intended Audience**
- Programmers who want to learn about the most common vulnerabilities introduced during software implementation, and how to avoid them: this includes programmers using web scripting languages such as PHP, ASP, Python, etc.

**Format**
- A 2-day seminar, at 8 hours/day, packed with the contents of all the lectures, separated with exercises that approximately recreate the pedagogical value of the missing assignments.

**Offered in Spring 2003, exact date to be announced.**

**Topics Covered:**
- Dekimione of Vulnerabilities, exploits, exposures. Policies, Web resources. Consequences of exploits. Unix permissions and related commands, chmod, chgrp, chown, umask
- Buffer overflows
- Kernel validation and File system management
- Race conditions (including symlinks)
- String format vulnerabilities
- Cross-site scripting vulnerabilities
- RCE, code injection vulnerabilities
- XSS and ClickJacking vulnerabilities
- CSRF and DOM XSS (see other page)