What is this course about?

**Comprehensive introduction** to network security
- learn **principles** of network security
- learn **practice** of network security
- Internet security architecture/protocols as case study

**Goals:**
- learn a lot (not just factoids, but principles and practice)
- have fun (well, it should be interesting, at least)
Course Information

- **Who is this course for?**
  - MS/PhD students, undergrads - juniors/seniors

- **Prerequisites:**
  - Computer networks class, and/or good practical experience with networking
    - Socket programming required, some understanding of TCP/IP (protocol functions, header structure)

Course Materials


- **Secondary texts:**
  - Security in Computing, Pfleeger, Pfleeger, & Margulies, Pearson

- **Other sources**
  - Internet Denial-of-service by Mirkovic et al
  - SSL by Rescorla
  - IEEE Security and Privacy Magazine
  - ...

- **Class notes (no slides, most of the time)**
Course Information (more)

- Class WWW site (same for cs5490 and cs6490):
  
  www.eng.utah.edu/~cs6490

- everything will be posted on this site!
  - topics and schedule
  - assignments
    nothing will be handed out in class :-)

- working on having this class on canvas

Course Information (more)

- Mailing Lists: cs6490@list.eng.utah.edu, teach-cs6490@list.eng.utah.edu
  - announcements, discussions, questions
  - join by going to https://sympa.eng.utah.edu/sympa

- Workload:

<table>
<thead>
<tr>
<th>Coursework</th>
<th>approx</th>
<th>approx %</th>
</tr>
</thead>
<tbody>
<tr>
<td>written HW</td>
<td>5</td>
<td>25%</td>
</tr>
<tr>
<td>programming assigns.</td>
<td>2</td>
<td>15%</td>
</tr>
<tr>
<td>programming questions (in written HW)</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>midterm exams</td>
<td>2</td>
<td>35%</td>
</tr>
<tr>
<td>course project</td>
<td></td>
<td>20%</td>
</tr>
</tbody>
</table>

- Cheating policy:
  http://www.cs.utah.edu/graduate/cheating_policy.pdf
  Please read, sign academic misconduct acknowledgment form
Course Information (more)

- **cs5490 vs cs6490**
  - same lectures
  - cs6490 - more questions in HW & Exams, extra credit for cs5490

- **TA:** Shishir Bhargav, Office hour: TBA

- **Professor's meeting hour:** Tuesday 10-11 AM

- **could also ask questions by sending email to the class mailing list, meet (briefly) after class**

---

Course Information (more)

- **Grading guidelines:**
  - 90-100 A
  - 80-89 A-
  - 70-79 B-, B, B+
  - 60-69 C-, C, C+
  - 50-59 D-, D, D+
  - < 50 (or caught cheating) E

  The ranges as well as the thresholds could be shifted/changed depending on the overall performance of the class in the midterm exams, home works, programming assignments, and final project

- **in-class style:** interaction, questions *(please!)*

- please read Chapter 8 from Kurose and Ross \( \geq 4^\text{th} \) edition
Course Overview:

Part 1: Cryptography

- Introduction
- Secret key crypto
  - permutations & substitutions, block ciphers
  - stream ciphers, one time pads
- Modes of operation
  - encrypting large messages (CBC), multiple enc/dec (3DES)
Course Overview:

Part 1: Cryptography

- Hashes and message digests
  - birthday paradox, Unix password hash, MD*, SHA, HMAC
- Public key crypto
  - elementary number theory, RSA, Euclid’s theorem, Chinese remainder theorem
  - Diffie Hellman key exchange
  - zero knowledge proof systems
  - finite fields, elliptic curves

Course Overview:

Part 2: Authentication

- Overview
- Authentication of people
  - reliably verifying identity of someone (or something)
- Security handshake pitfalls
  - minor variants of authentication protocols can have security holes, e.g., timer-based & reflection attacks
  - mediated authentication
**Course Overview:**

**Part 2: Authentication**
- Strong password protocols
  - Lamport's hash
  - Secure even when password broken by offline dictionary attacks

**Course Overview:**

**Part 3: Standards**
- Kerberos, PKI (Certificates)
- SSL - handshake, data exchange, export rules
- IPsec
  - AH, ESP
  - IKE
  - IPsec over NAT
  - Firewall friendliness
- Wireless security - 2G/3G/4G, WiFi, M2M

Mary had a little key
(It's all she could export)
And all the email that she sent
Was opened at the Fort.
Course Overview:

Part 4: Topics in Security

- Denial-of-service
  - general concepts, formulations
  - Pushback
  - IP traceback – find attacker locations
  - KillBots – distinguish flash crowds from DDoS, Bloom filters
  - new Internet architectures

- Anonymity, End-point hiding

Midterm Exam II

- Digital Pests: Viruses, Buffer overflow, worms
- Software Defined Networks
- Firewalls, Intrusion detection (if time permits)

No Final Exam
- looked at several courses offered elsewhere
  - Radia Perlman's course at Harvard
  - security courses offered at U. Delaware, Virginia, Columbia U., Purdue U.
- those with security experiences - please provide your input to the class
- very hot, constantly evolving field - will need everybody's help

Questions, comments, ... ??