If you wish to enroll and do not have D clearance yet, send an email to CSci530@usc.edu with:
- Your name
- Which prerequisites you have completed
- A phone number
- Request to receive a D clearance
- I will contact and assess if space becomes available.

http://ccss.usc.edu/530
- Syllabus
- Assignments
- News
- Lecture notes (also on Blackboard)

http://ccss.usc.edu/530L
- 1 of the 4 units
- Instructor is David Morgan
- Instruction 4 - 4:50 Fridays in RTH105
  - WebCast via DEN
  - Hands on work in the lab – exercising the theoretical knowledge from class
  - Some labs will be done remotely using DETER testbed

Four reports, due as noted online
- Each discusses a paper of your choice from a few top security conferences/journals
  - Summary of the paper and its critique
  - Your ideas on the topic
  - 2-4 pages, submitted via Blackboard
  - You can submit reports early if you like
- One report from each student will be chosen for presentation in class
- Total 20% of your grade, 4% each
- Late policy: 48 h grace period divided over all 4 assignments - must email ahead of deadline
Administration

- Grading:
  - Paper reports/presentations: 20%
  - Lab: 20%
  - Quizzes: 5%
  - Participation: 5%
  - Midterm Exam: 20%
  - Final Exam: 30%
- Grades assigned using an absolute curve:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>93%</td>
</tr>
<tr>
<td>A-</td>
<td>90%</td>
</tr>
<tr>
<td>B+</td>
<td>86%</td>
</tr>
<tr>
<td>B</td>
<td>83%</td>
</tr>
<tr>
<td>C+</td>
<td>80%</td>
</tr>
<tr>
<td>C</td>
<td>76%</td>
</tr>
<tr>
<td>C-</td>
<td>73%</td>
</tr>
<tr>
<td>D+</td>
<td>70%</td>
</tr>
<tr>
<td>D</td>
<td>66%</td>
</tr>
<tr>
<td>D-</td>
<td>63%</td>
</tr>
<tr>
<td>F</td>
<td>60%</td>
</tr>
</tbody>
</table>

Blackboard

- DEN Blackboard system will host the class discussion board
- To gain access and log in:
  - [https://blackboard.usc.edu/](https://blackboard.usc.edu/)
- Contact webclass@usc.edu if you have difficulty gaining access to the system
- I will check the discussion board once daily but if you want a reliable response from me email me directly

Class Participation

- Class participation is important
- Ask and answer questions in class
- Ask, answer, participate on-line
- Class participation carries 5% of your grade
- If I don’t remember you from class, I look in the web discussion forum to check participation
  - Did you ask good questions
  - Did you provide good answers
  - Did you make good points in discussions

Academic Integrity

- What is and is not OK
  - I encourage you to work with others to learn the material but everyone must do their work ALONE
  - Do not turn in the work of others
  - Do not give others your work to use as their own
  - Do not plagiarize from others (published or not)
  - Do not try to deceive the instructors
- See section on web site and assignments
  - More guidelines on academic integrity
  - Links to university resources
  - Don’t just assume you know what is acceptable.

What Does Security Mean?

... In Real Life

- No one should be able to:
  - Break into my house
  - Attack me
  - Steal my TV
  - Use my house to throw water balloons on people
  - Damage my furniture
  - Pretend to be my friend Bob and fool me
  - Waste my time with irrelevant things
  - Prevent me from going to my favorite restaurant
What Does Security Mean? ... wrt Computers and Nets

- No one should be able to:
  - Break into my computer
  - Attack my computer
  - Steal my information
  - Use my computer to attack others
  - Damage my computer or data
  - Use my resources without my permission
  - I want to talk to Alice
    - Pretend to be Alice or myself or our computers
    - Prevent me from communicating with Alice

Computer vs. Network Security

- An isolated computer has a security risk?
  - Computer security aims to protect a single, connected, machine
- Networking = communication at all times and in all scenarios!!!
  - Network security aims to protect the communication and all its participants

- Security = robustness or fault tolerance?

What Are the Threats?

- Breaking into my computer
  - Hackers
    - Break a password or sniff it off the network
    - Exploit a vulnerability
    - A vulnerability is a bug in the software that creates unexpected computer behavior when exploited, such as enabling access without login, running unauthorized code or crashing the computer.
    - An exploit is an input to the buggy program that makes use of the existing vulnerability.
    - Use social engineering
      - Impersonate someone I trust
    - Viruses and worms

What Are the Threats?

- Attacking my computer
  - Denial-of-service attacks
    - A DOS attack aims to disrupt a service by either exploiting a vulnerability or by sending a lot of bogus messages to a computer offering a service
  - Viruses and some worms:
    - A virus is a self-replicating program that requires user action to activate such as clicking on E-mail, downloading an infected file or inserting an infected floppy, CD, etc...
    - A worm is a self-replicating program that does not require user action to activate. It propagates itself over the network, infects any vulnerable machine it finds and then spreads from it further.

What Are the Threats?

- Stealing my information
  - From my computer or from communication
    - I will use cryptography!
      - There are many ways to break ciphers
      - There are many ways to divulge partial information (e.g. who do you talk to)
      - I would also like to hide who I talk to and when
        - I will use anonymization techniques
        - Anonymization hinders other security approaches that build models of normal traffic patterns

What Are the Threats?

- Using my machine to attack others
  - E-mail viruses
  - Worms
  - Denial-of-service attacks (including reflector attacks)
  - Spam, phishing
What Are the Threats?

- Damaging my computer or data
  - I have to prevent break-ins
  - I will also use cryptography to detect tampering
  - I must replicate data to recover from tampering
  - Denial-of-service attacks and worms can sometimes damage computers

- Taking up my resources with irrelevant messages
  - Denial-of-service attacks
  - Spam mail (takes time to read and fills space)
  - Malicious mail (may contain a virus)
  - Viruses and worms

- Pretending to be Alice or myself or our computers
  - I want to be sure who I am talking to (authentication and digital signatures)
  - It is hard to impersonate a computer in two-way communication, such as TCP
    - But it has been done
  - Plain IP spoofing seems an extremely hard problem to solve
    - IP spoofing means putting a fake IP address in the sender field of IP packets.

- Preventing me from communicating with Alice
  - Alice could be attacked
  - Routers could be overloaded or tampered with
  - DNS servers could be attacked

The Three Aspects of Security

- Confidentiality (C)
  - Keep data secret from non-participants

- Integrity (I)
  - Aka “authenticity”
  - Keep data from being modified

- Availability (A)
  - Keep the system running and reachable
  - Keep it functioning properly

What Does Security Mean? ...

- ... wrt Computers and Nets

- No one should be able to:
  - Break into my computer – A, C, I
  - Attack my computer – A, C, I
  - Steal my information – C
  - Use my computer to attack others – I?
  - Damage my computer or data – I
  - Use my resources without my permission – A

- I want to talk to Alice
  - Pretend to be Alice or myself or our computers – C, I
  - Prevent me from communicating with Alice – A
Orthogonal Aspects

- **Policy**
  - Deciding what confidentiality, integrity and availability mean
- **Mechanism**
  - Implementing the policy