

# Security Topics in Networking and Distributed Systems

## CS 590D

### **Lecture 1**

Department of Computer Sciences  
Purdue University

# Course Information

- Meetings
  - Tu&Th 1:30-2:45 PM
- Professor contact info:
  - Office: REC 217/CS174
  - Email: [crisn@cs.purdue.edu](mailto:crisn@cs.purdue.edu)
  - **Office hours: TuTh 2:45 – 4:30 PM in CS174**
- TA:
  - Chi-Bun Chan (Ben), [cbchan@cs.purdue.edu](mailto:cbchan@cs.purdue.edu)
  - Office hours to be announced

# Course Information (cont.)

- Class mailing list:  
590D@cs.purdue.edu
- Class webpage

<http://www.cs.purdue.edu/homes/crisn/courses/cs590D>

**IMPORTANT:** all messages to me about the class should contain in the subject 590D

# Grading Policy

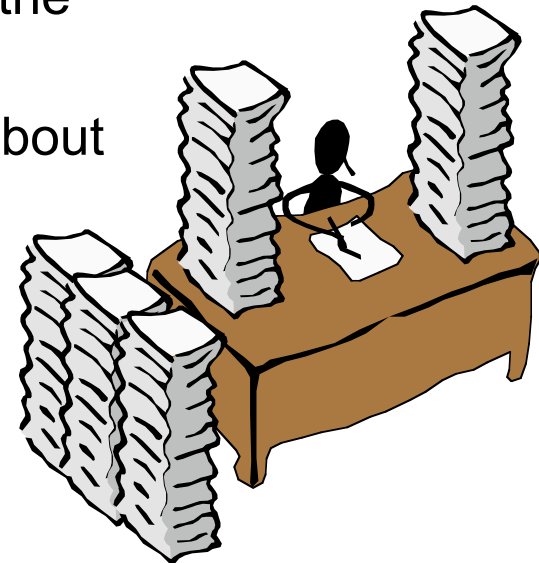
- Class presentation 20%
- Final project 50%
- Homework 15%
- Participation in class discussions and providing feedback on your colleagues presentations 15%

# Class Overview

- Set of topics provided
- Several lectures given by me providing overview on the topics with focus on one or two important papers
- Students give presentations of other significant papers on one of the topics. Each student should have a presentation (about 20 minutes).
- No books required, only research papers.
- ALL SUBMISSIONS are electronically **PDF**

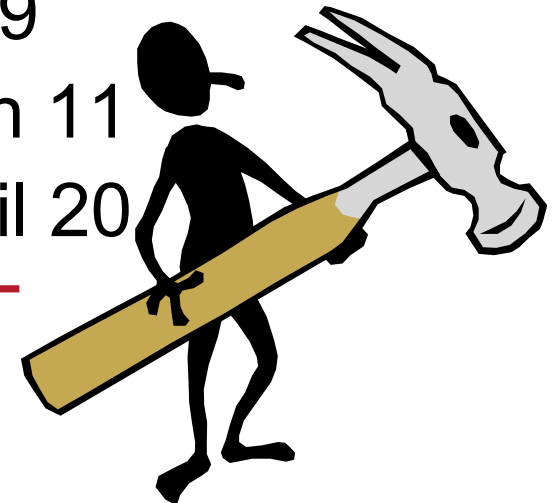
# Homework

- READ the assigned reading
- Before each class you will need to submit a 1 page report on one of the papers assigned to read, containing:
  - One paragraph summary of the paper
  - 3 strong points (what you liked about the paper)
  - 3 weak points (what you did not like about the paper)



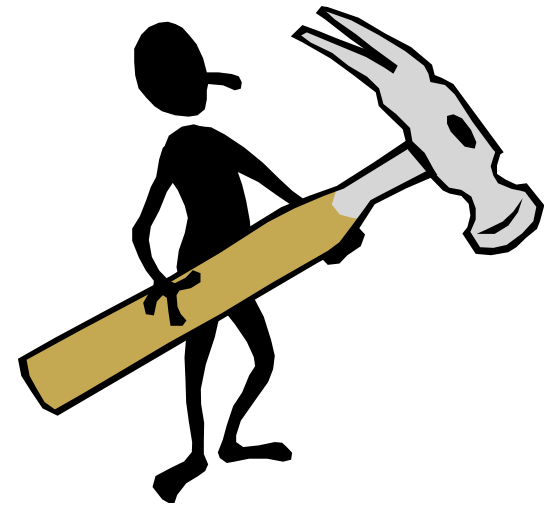
# Project

- It can be on one of the topics covered in the class, but this is not a requirement, as long as it is related to a security topic in networking and distributed systems
- Project proposal due by Jan.29
- Project progress due by March 11
- Project final report due by April 20
- **DEADLINES ARE STRICT**



# Project (cont.)

- Work in teams of 2-3 students, please form teams, otherwise I will assign you to a team.
- At the end of the course each team will give a brief presentation of what the project accomplished.
- Team will meet with me to demonstrate the project, discuss what was accomplished and assess the contribution of each member of the team.



# Course Topics (1)

- High-level protocols security (0.5 week)
- IP security and DDOS trace back (1 week)
- BGP, DNS, OSPF security (1 week)
- TCP security (0.5 week)
- Secure multicast (1 week)
- Intrusion detection (1 week)

# Course Topics (2)

- Group communication security (2 weeks)
- Byzantine security/fault tolerance  
(Intrusion fault-tolerance) (2 weeks)
- Security issues in wireless networks (3 weeks)
- Peer-to-peer systems security (2 weeks)
- Anonymity and privacy (2 weeks)

**ANYTHING ELSE YOU THINK IT'S INTERESTING  
and it's related to course topics**

# Possible projects (1)

- **Role-based access control for groups**: test-case group communication systems (will require working with Spread) and RT library.
- **Building intrusion fault-tolerance using threshold cryptography** (you can use Spread, it will require you to learn more about threshold crypto, and how it can help to design intrusion fault-tolerance systems).

# Possible projects (1)

- **Taxonomy of attacks on wireless routing networks:** identify, implement and test concrete attacks for AODV or DSR
- **Attacks on MAC protocols for wireless networks:** survey on possible attack, think/design possible solutions (ECE major preferred)
- **Key management for wireless systems:** survey, implementation, comparison, analysis of results (it can be focused on sensors only, etc)

# Possible projects (1)

- **SPAM:** investigate the current state of problems/losses caused by SPAM, think/implement a possible solution
- **Viruses/Worms:** identify why are they causing so much damage so quick and figure out if there any solutions to stop these type of attacks at the network level.
- **Metrics for risk assessment (in particular network security risks):** Are any of the methods applied to asses financial risk applicable to asses security risks ?Design a metric and try to apply it.

# Possible projects (4)

- **Use of smart-cards as way of enhancing health-care:** will involve designing a medical system where critical information is preserved on smartcards. Research challenges: preserving privacy, while allowing access to critical information. Smartcard readers(GemPlus) and cards available.

# Possible projects (5)

- **Secure DNS**: possible problems, focus on one of them, design solution; example: how is the data managed? Can availability be improved? What is the role/risk of caching?

# Next Lecture

- Topic: High-level protocols security
- Assigned reading:
  - V. Voydock and S. Kent. Security mechanisms in high-level network protocols
  - R. Needham and M. Schroeder. Using Encryption for authentication in large networks
  - K. Thompson. Reflections on Trusting Trust

