Advanced Computer and Network Security

Dr. Arjan Durresi
Louisiana State University
Baton Rouge, LA 70810
Durresi@Csc.LSU.Edu

These slides are available at:
http://www.csc.lsu.edu/~durresi/CSC7502_04/

Overview

- How
- What
- When
- Why
Overview

- How am I going to grade you?
- What are we going to cover?
- When are you going to do it?
- Why you should take this course?

Grading

- Learning-centered course:
  - The first priority: Maximize learning
  - Your grade will depend on how much you have learned
- Activity in the class (involvement in discussing the papers) (25%)
- Homework (15%)
- Quality of the project (60%).
Frequently Asked Questions

- Yes, I do use “curve”. Your grade depends upon the performance of the rest of the class.
- All homeworks are due at the beginning of the next class.
- All late submissions must be preapproved.
- Everyone including the graduating seniors are graded the same way.

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.
**Homework**

- Reading will be assigned for each lecture.
- Before lecture, every student must submit a one page report of one of the assigned papers (report should contain a one paragraph summary of the paper, description of three strong points of the paper and three weak points of the paper).
- The reports are due one hour before the class starts (DUE TIME: 12:30 PM), by email to durresi@byte.csc.lsu.edu, include 7502 - HW# in the subject.
- If more than one paper was assigned, you have to submit a report only on one of the papers. IMPORTANT: Submit your homework in PDF format.

**Project**

- Every student must complete a project on one of the topics discussed in the class.
- Students are required to work in teams of 2 or 3 on the project.
- In addition to the presentation given in the class every team will meet with me to discuss the accomplished results and assess the contribution of each team member.
- Every project must have a practical component that will require you to do an implementation and demonstration.
Project proposal (2-3 pages), due on September 14

- Should include:
  - Problem you address.
  - What is your approach.
  - Milestones (main steps and when and how you plan to address them)
  - References: additional reading that you intend to do
  - Tools: if you plan to use tools (software already available), specify if you already have experience with it or you will need first to get to know how to use it.
  - What will be the deliverables: implementation, simulation results, etc,
  - What are the points that if achieved, you will consider that the project was successful.

Project progress (1-2 pages), due October 28

- Should relate to the project proposal:
- What points from the milestones in project proposal were finished.
- What are the main challenges so far.
- Describe if you are stuck in solving a problem (technical or research).
- Sometimes things do not work the way you intended, specify all the modifications from the original proposal, and why were they necessary.
**Project final report (10-15 pages), due 1 day before your demonstration of the project**

- Should include:
  - Problem addressed
  - Proposed solution; In case of a system, describe and motivate the chosen architecture, design. If any new algorithm/protocol is designed, include description of the algorithm.
  - In case of comparison, simulations, include results.
  - What was your personal lessons learnt from the project

---

**What Is This Course About?**

- Overview of network security issues: what is the current status, what are the current interesting problems in point-to-point and multicast protocols.
- Security of the Internet infrastructure: DNS, BGP.
- Denial of service: intrusion detection systems, IP traceback, distributed denial of service tools, classifying denial of service.
- Key management: why is key management so important, what are the most successful proposed solutions, what are their limitations.
- Security in wireless communication: what are the main issues in security for distributed systems in a wireless environments, what are the particularities, solutions, and open problems.
- Peer-to-peer systems: after familiarizing with the main services that these systems provide, we will examine possible security problems and look at recent research papers focused on proposing solutions
Supplementary Text

- Books on Computer Networks, Distributed Systems and Information Security or Cryptography are highly recommended.

Course Outline

- Introduction to attacks on protocol
- Attacks on TCP
- DDoS attacks
- IP Traceback
- Proactive countermeasures against DDoS
- Intrusion detection
- Worms
- BGP security
- Security of WEP
Course Outline (Cont)

- 802.11 Denial of Service
- Security Issues in Routing protocols for Ad Hoc Wireless Network
- Sensor networks:
  - Key Management
  - Routing
- RFIDs and privacy
- Traffic analysis on anonymity providing systems

Prerequisites

- Networking, operating systems, discrete mathematics, and programming (C or C++, Java).
- Cryptography, network security
- The right motivations.
Possible Projects

- Building intrusion fault-tolerance using threshold cryptography.
- 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
- Key management for wireless systems:
  - survey, implementation, comparison, analysis of results (it can be focused on sensors only)

- 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

- **Use of smart-cards as way of enhancing healthcare:**
  - will involve designing a medical system where critical information is preserved on smartcards. Research challenges: preserving privacy, while allowing access to critical information.

- **Secure DNS:**
  - possible problems, focus on one of them, design solution; example: how is the data managed?

Office Hours

- Tuesday and Thursday: 3:00 to 4:00 PM and by appointments
- Office: 291 Coates Hall
- Telephone: (225)-578-3902
- Email: durresi@csc.lsu.edu
- Course web page:
  - [http://www.csc.lsu.edu/~durresi/CSC7502_04](http://www.csc.lsu.edu/~durresi/CSC7502_04)
- GTA:
Next Lecture

- Topic: High-level protocols security
- Assigned reading:
  - V. Voydock and S. Kent. Security mechanisms in high-level network protocols
  - K. Thompson. Reflections on Trusting Trust

Summary

- There will be a lot of self-reading
- Goal: To prepare you for a career in network security
- Get ready to work hard
- Next lecture papers are online
Thank You!