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/CSC4601_07/

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 should you take this course?

Grading

- Learning-centered course:
  - The first priority: Maximize learning
  - Your grade will depend on how much you have learned
- Final Exam 40%
- Class participation 10%
  - Questions and discussions in class give you points and improve the quality of teaching
- Homework 25%
- Project or lab 25%
- Possibility of one extra-assignment to improve the final grade up to one point

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.
- All quizzes are open-book and extremely time limited.
- Exams consist of numerical as well as multiple-choice (true-false) questions.
- There is negative grading on incorrect multiple-choice questions.
- Everyone is graded the same way.

What Is This Course About?

- Understanding of basic issues, concepts, principles, and mechanisms in information security.
  - Security goals and threats to networking infrastructure and applications.
  - Introduction to cryptography.
  - Network security applications.
  - System security applications.
- Exposure to commercial as well as research security technologies.
Text Book

- Network security: PRIVATE communication in a PUBLIC world by Kaufman, Perlman, and Speciner.
  - This book is very comprehensive. I will follow it as much as possible.

Supplementary Text

  - Third Edition 2003
  - This book contains more recent technologies and will be used for the second half of the course.
- Internet Security: Cryptographic Principles, Algorithms and Protocols by Man Young Rhee
- Wireless Security Essentials: Defending Mobile Systems from Data Piracy by Russell Dean Vines

Course Outline

- Background:
  - Review of networking technologies
  - Network security threats and counter measures
- Cryptography:
  - Secret key cryptography
  - Hashes and message digests
  - Public key cryptography
  - Information hiding

Course Outline (Cont)

- Network and system security applications:
  - Authentication and security handshakes pitfalls
  - IP security
  - Web and E-commerce
  - Attacks to routing infrastructures and counter measures
  - DDoS and traceback
  - Virus/worm detection, firewalls, intrusion detection.
  - Hacking and forensics
  - Writing secure code

Prerequisites

- Networking, operating systems, discrete mathematics, and programming (C or C++, Java).
- The right motivations.

Office Hours

- Tuesday, Thursday 3-4 p.m.
- Telephone: (225)-578-3902
- Email: durresi@csc.lsu.edu
- Course web page:
  - http://www.csc.lsu.edu/~durresi/PUT/security-06
- TA:
  - Office, Tel.:
  - Email:
Summary

- There will be a lot of self-reading
- Goal: To prepare you for a career in network security
- Get ready to work hard

Quiz 0: Prerequisites

True or False?

- T  F
- Datalink refers to the 2nd layer in the ISO/OSI reference model
- T  F
- Category 5 unshielded twisted pair cable is better than category 3 cable.
- T  F
- Finding path from one node to another in a large network is a transport layer function.
- T  F
- It is impossible to send 3000 bits/second through a wire which has a bandwidth of 1000 Hz.
- T  F
- Bit stuffing is used so that characters used for framing do not occur in the data part of the frame.
- T  F
- For long delay paths, on-off flow control is better than window flow control.
- T  F
- Ethernet uses a CSMA/CD access method.
- T  F
- 10Base2 runs at 2 Mbps.
- T  F
- The packets sent in a connection-oriented network are called datagrams.
- T  F
- Spanning tree algorithm is used to find a loop free path in a network.

Marks = Correct Answers _____ - Incorrect Answers _____ = ______

Quiz 0: Solution

True or False?

- T  F
- √ T  F
- Datalink refers to the 2nd layer in the ISO/OSI reference model
- √ T  F
- Category 5 unshielded twisted pair cable is better than category 3 cable.
- √ T  F
- Finding path from one node to another in a large network is a transport layer function.
- √ T  F
- It is impossible to send 3000 bits/second through a wire which has a bandwidth of 1000 Hz.
- √ T  F
- Bit stuffing is used so that characters used for framing do not occur in the data part of the frame.
- √ T  F
- For long delay paths, on-off flow control is better than window flow control.
- √ T  F
- Ethernet uses a CSMA/CD access method.
- √ T  F
- 10Base2 runs at 2 Mbps.
- √ T  F
- The packets sent in a connection-oriented network are called datagrams.
- √ T  F
- Spanning tree algorithm is used to find a loop free path in a network.