CS458/CS558: Introduction to Computer Security

Course Info

- Class Time
  - Tue. & Thur. 4:25pm – 5:50pm
- Instructor: Ping Yang

  Office: T6 (3rd floor), engineering building

  Email: pyang@binghamton.edu

  Office Hours: Tue. Thur. 3:50pm – 4:20pm (start from Sept. 8)
- Teaching Assistant:

  Ruiqi Luo

  Office: N1 (3rd floor), engineering building

  Office Hours: Mon. Wed. Fri. 1pm – 2pm (start from Sept. 7)

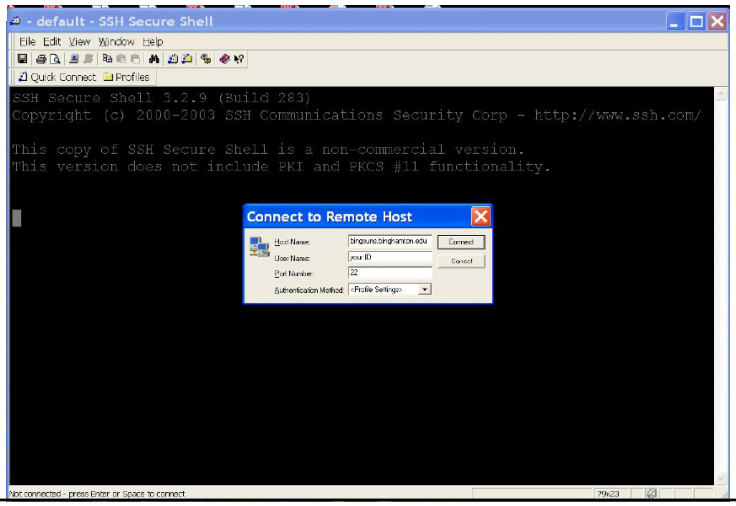
  Email: rluo1@binghamton.edu

Course Info (Cont.)

- Textbook:
  - William Stallings, *Cryptography and Network Security Principles and Practice*, Fourth/Fifth Edition, ISBN-10: 0-13-187316-2, ISBN-13: 978-0-13-187316-2
  - Electronic textbook: http://www.safarix.com
- Course website: http://www.cs.binghamton.edu/~pyang/cs558-F11.html contains links to some online resources.
- Course materials are available at the blackboard system. http://blackboard.binghamton.edu
  - Submitting assignments
  - Checking grades

Course Info (Cont.)

- Make sure that you have an account in bingsuns.binghamton.edu.
  - Download SSH secure shell client to access bingsuns

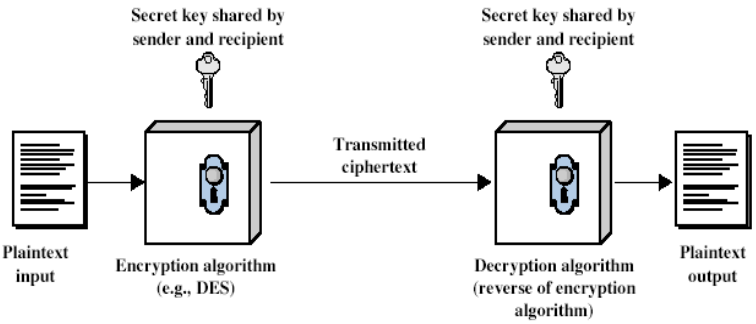


Prerequisites

- Proficient with programming in C or C++
- Comfortable working and programming in the Unix environment.

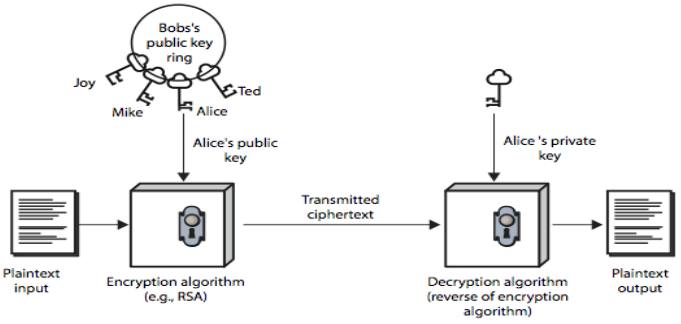
Topics

- A broad introduction to network, computer and information security.
- Topics may include:
  - Introduction to network and socket programming
  - Cryptography: encryption and decryption techniques
    - Symmetric encryption



Topics

- A broad introduction to network, computer and information security.
- Topics may include:
  - Introduction to network and socket programming
  - Cryptography: encryption and decryption techniques
    - Public-key encryption



(a) Encryption

7

Topics

- A broad introduction to network, computer and information security.
- Topics may include:
  - Introduction to network and socket programming
  - Cryptography: encryption and decryption techniques, key management, digital signature, authentication protocols
  - Network Security Applications: email/web security
  - System Security: intrusion detection, malicious software
  - Security Policies and Principles: confidentiality, integrity, availability, access control
  - Buffer overflow attack, SQL injection attack

Grading

- Assignments : 32%
  - Assignment 1 (programming, C/C++/Java): 9%
  - Assignment 2 (programming, C/C++/Java): 9%
  - Assignment 3 (programming, C/C++): 9%
  - Assignment 4 (written): 5%
- Exam1 (Oct.): 18%
- Exam2 (Dec. 8): 23%
- project: 18%
- Quizzes: 9%

Final grades will be curved over the entire class.

Grading

- If you have questions about the grading of assignments, quizzes and the programming project, please first contact the TA. This is used to ensure consistent grading.
- If the issue has not been resolved by the TA, then talk to the instructor, either during my office hours or after the class.
- Questions regarding the survey project, exams and final grades should be addressed to the instructor.

Assignment/Exam Policies

- Assignments
  - Start early, ask questions early, submit on time
  - No assignment will be accepted after 24 hours from the deadline.
  - Late penalty: 10 points off
  - All programming assignments should be done individually. The written assignment is done by a group of two. The project is done individually or by a group of two.
- Missed exam Policy
  - There will be NO makeup exams, except in medical emergencies, when accompanied with appropriate documentation from the doctor.

Asking Questions

- During the class
- During office hours
- Make google your friend
- Email me/TAs

Course Project

- Choose either a survey project or a programming project.
- You can also propose your own project: talk to me.

Course Project: Survey

- Survey
  - Present 1 paper (20-25min) : Oct. or Nov.
  - Read 2 more papers and write a survey
    - Should not copy any sentence from the papers
  - Submit the slides and survey report
    - Submission deadline: Dec. 1
- Grading
  - Presentation: 70%
  - Survey report: 30%
  - Bonus: <= 5 points

Course Project: Survey

- Topics
  - Cloud computing security
  - Malware defense
  - Trusted computing
  - Virtual machine security
  - Security vs usability
  - Firewalls
  - ……

Course Project: Programming

- Programming
  - Done by a group of 2
  - 5 points bonus if done individually
  - No presentation
  - Submit the code and a readme file
  - Submission deadline: Dec. 1
- Grading guideline
  - Implementation: 95%
  - Readme: 5%
  - Extra credits: 6

Course Project: Programming

- Topics (C, C++, or Java)
  - Virtual election booth
  - Secure banking

Course Project: Others

- Topics
  - Buffer overflow attack (language: C)
  - Rootkits
  - Virus

Course Project: Others

- Other projects:
  - Done by a group of 2
  - 5 points bonus if done individually
  - Present the design and implementation (20-25min) and show demo: Dec. 1
  - Submit the code and slides
    - Deadline: Dec. 1
- Grading guideline
  - Implementation: 80%
  - Presentation: 20%
  - Bonus

Academic Integrity

- All students should follow Student Academy Honesty Code(http://www.binghamton.edu/watson/Watson_Academic_Honesty_Policy.pdf).
- You may discuss the problems with other students, however, you must write your own codes and solutions. Discussing solutions to the problem is NOT acceptable.
- Copying an assignment from another student or allowing another student to copy your work.
  - **Report to the department and school**
  - **0 in the assignment/F in the course**

Academic Integrity

- Use chmod 700 <directoryname> command to change the permissions of your working directories before you start working on the assignments.
- We will use Moss, to detect plagiarism in assignments.
- If you have any questions about whether an act of collaboration may be treated as academic dishonesty, please consult me before you collaborate.

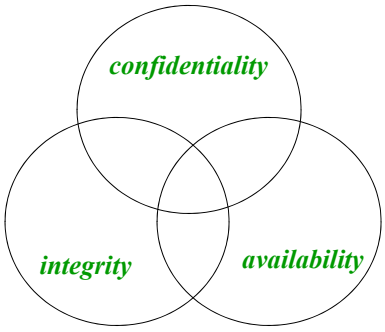
Flu, Fever Etc

- Please do not attend the lecture if you have flu or any infectious diseases
  - Inform me via email BEFORE the class

Introduction to Computer Security

What is Security

- Computer security rests on three basic components: confidentiality, integrity, and availability.



Confidentiality, Integrity and Availability

- Confidentiality: only authorized people or system can access the data or resource
- Integrity: assurance that the information is authentic and complete.
  - Data integrity: the assurance that data received is exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay)
  - Origin integrity: the source of data is trustworthy
- Availability: people has the ability to use the information or resource desired

Background

- Information Security requirements have changed in recent times

Background

- Information Security requirements have changed in recent times
- Traditionally provided by physical and administrative mechanisms
  - Physical: e.g. the use of rugged filing cabinets with a combination lock for storing sensitive documents
  - Administrative: e.g. personnel screening procedures used during the hiring process
- The use of computer: requires automated tools to protect files and other stored information
- The use of networks: requires measures to protect data during transmission

Examples: Security Violation

- User A transmits a file, which contains sensitive information to user B. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission
- A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

Aim of Course

- Consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information