CS458/CS558: Introduction to Computer Security

1

Course Info

- Class Time: Tue & Thur 4:25pm – 5:50pm
- Instructor: Ping Yang
  - Office: P11 (3rd floor), engineering building
  - Email: pyang@binghamton.edu
  - Office Hours: Wed. 10am - noon (start on Jan. 31)
- Teaching Assistant (0.5 TA): Di Mu
  - Office: TBA, engineering building
  - Office Hours: TBA (start on Jan. 29)
  - Email: dmu1@binghamton.edu

2

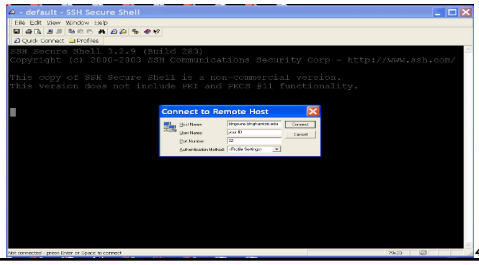
Course Materials

- 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
- Course website http://www.cs.binghamton.edu/~pyang/cs558S16.html contains links to some online resources.
- Course materials are available on blackboard system. http://blackboard.binghamton.edu
  - Submitting assignments
  - Checking grades

3

Course Info (Cont.)

- Make sure that you have an account in bingsuns.binghamton.edu.
  - Windows: Download SSH secure shell client to access bingsuns
  - https://cgi.math.princeton.edu/compudocwiki/index.php?title=HowTos:Connect_to_login_servers_via_ssh



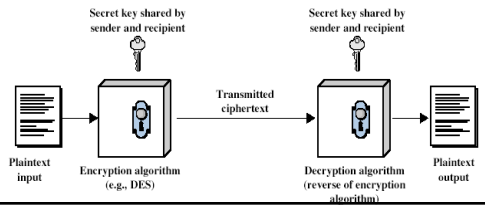
4

Prerequisites

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

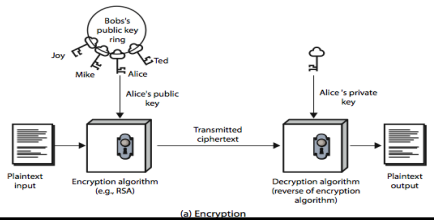
Topics

- 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

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
  - Systems Security: intrusion detection, malicious software
  - Security Policies and Principles: confidentiality, integrity, availability, access control
  - Buffer overflow attack, SQL injection attack, Heartbleed

8

Grading

- Assignments : 34%
  - Assignment 1: programming assignment (C/C++/Java): 14%
  - Assignment 2: Written assignment: 6%
  - Assignment 3: programming assignment (C/C++/Java): 8%
  - Assignment 4: rootkit/PGP: 6%
- Exam1 (March): 20%
- Exam2 (May): 20%
- Quizzes & attendence: 8%
- project: 18%

All assignments will be done by a group of two students.
Final grades will be curved over the entire class.

9

Grading

- If you have questions about the grading of assignments 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 presentation project, exams and final grades should be addressed to the instructor.

10

Assignment/Exam Policies

- Assignments
  - Start early, ask questions early, submit on time
  - No assignment will be accepted after 12 hours from the deadline.
  - Late penalty:
  - 0-6hrs: 2.5 6-12hrs: 5 points
- Missed exam Policy
  - There will be NO makeup exams, except in medical emergencies, when accompanied with appropriate documentation from the doctor.

11

Asking Questions

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

12

Course Project

- Choose either a presentation project a programming project, or a computer systems project.
- CS558 is considered a long programming course only if you choose to do a programming project.
- You can also propose your own project: talk to me.

13

Course Project: Presentation

- Presentation project
  - Done individually
  - Present 2 paper (each presentation takes about 25 min)
    - The presentation will be scheduled at the end of March or April.
    - You can choose to present the two papers on the same day or different days.
  - Submit the presentation slides
    - Submission deadline: May 3 (Thursday)
    - 1-5 points extra credits

14

Course Project: Presentation

- Topics
  - Blockchain
  - Securing code and data using Intel SGX
  - Web security

15

Course Project: Programming

- Programming project (C/C++/Java)
  - Done by a group of 2
  - 10 points extra credits if done individually
  - No presentation
  - Submit code & readme
    - Deadline: May 3 (Thursday)
- Grading guideline
  - Implementation: 97%
  - Readme: 3%

16

Course Project: Systems Projects

- Systems projects
  - Buffer overflow attack (language: C)
  - Virus
  - Rootkit
  - Secure checkout system
  - Blockchain

17

Course Project: Others

- Systems projects
  - Done by a group of 2
  - 10 points extra credits if done individually
  - In-class presentation and demo: May 3 (Thursday)
  - Submit codes and slides
    - Deadline: May 3 (Thursday)
- Grading guideline
  - Implementation/demo: 80%
  - Presentation: 20%

18

Academic Integrity

- All students should follow Student Academic Honesty Code(http://www2.binghamton.edu/watson/about/honesty-policy.pdf).
- You may discuss the problems with other students, however, you must write your own codes and solutions. Discussing algorithms and 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

19

Academic Integrity

- We will use Moss, to detect plagiarism.

http://lightningbirl.org/wp-content/uploads/2015/09/moss_sample-initial_result-masked-021.png

Academic Integrity

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

21

Flu/Fever/Weather

- Please do not attend the class if you have flu, fever, bad cough, or any infectious diseases
- If the weather is bad (e.g. heavy snow), please check your email before you attend the lecture.

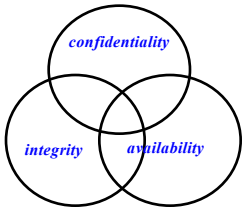
22

Introduction to Computer Security

23

What is Security

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



24

Confidentiality, Integrity and Availability

- Confidentiality: only authorized people or system can access the data or resource

25

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

26

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

27

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.

28

Background

- Information Security requirements have changed in recent times

29

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

30

Aim of Course

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

31

OSI Security Architecture

32

OSI Security Architecture

- ITU-T X.800: Security Architecture for OSI
  - ITU-T: International Telecommunication Union, Telecommunication standardization sector
  - OSI: Open Systems Interconnection - an effort to standardize networking
    - Started in 1982 by the Internationtional Organization for Standardization (ISO)
  - Systematic way of defining the requirements for security
- 3 aspects of information security:
  - Security attacks
  - Security mechanisms
  - Security services

33

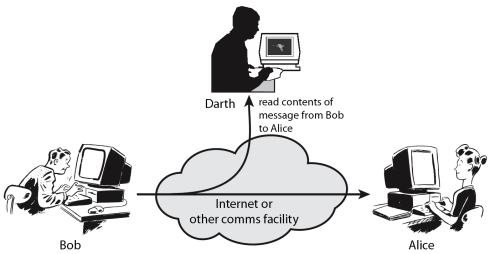
Security Attacks

- Any action that compromises the security of information owned by an organization
- Information security: how to prevent attacks and to detect attacks on information-based systems
- Can focus of generic types of attacks
  - Passive
  - Active

34

Passive Attacks

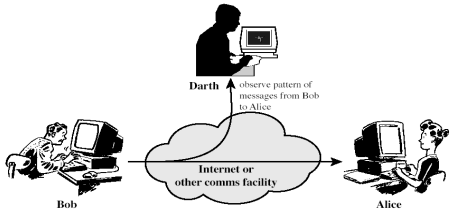
- Attempts to learn or make use of the information from the system but does not affect system resources
- The release of mesg. contents: eavesdropping on or monitoring of transmissions.



35

Passive Attacks

- Traffic analysis: may not be able to extract the information (encryption), but might still be able to observe the pattern of these massages
  - Observe the frequency and length of messages being exchanged.
  - Example: timing attack on the SSH protocol used timing information to deduce information about passwords



36

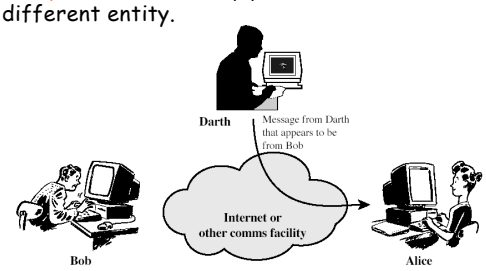
Passive Attacks

- Very difficult to detect because they do not involve any alteration of the data
- It is feasible to prevent the success of these attacks.
- The emphasis in dealing with passive attacks is on prevention rather than detection.

37

Active Attacks: Masquerade

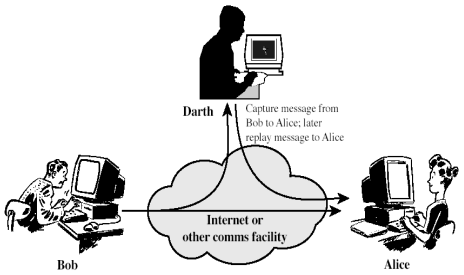
- Attempts to alter system resources or affect their operation.
  - Masquerade: one entity pretends to be a different entity.



38

Active Attacks: Replay

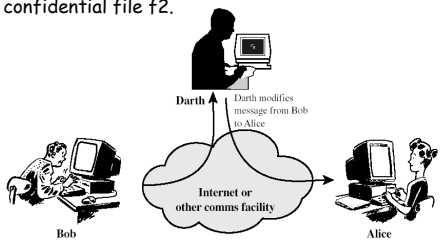
- Replay: capture the data unit and transmit to the receiver later to produce an unauthorized effect.



39

Active Attacks: Modification of Mesg.

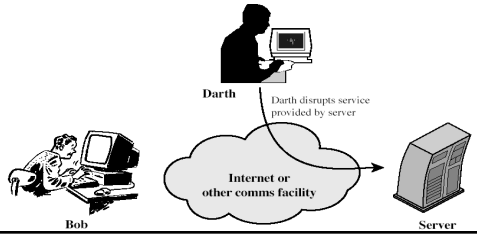
- Modification of messages: some portion of a legitimate message is altered, or messages are delayed or reordered
  - E.g. Allow a to read confidential file f1 → allow b to read confidential file f2.



40

Active Attacks: DOS

- Denial of service: prevents or inhibits the normal use or management of communications facilities
  - E.g. An entity may suppress all messages directed to a particular destination
  - E.g. disruption of an entire network by overloading it with messages so as to degrade performance



Security Services

- Provided by a system to give a specific kind of protection to system resources.
- Intended to counter security attacks
- Using one or more security mechanisms
- X800 divides these services into 5 categories and 14 specific services.

42

Security Services (X.800)

- Authentication: assurance that the communicating entity is the one claimed
- Access control: prevention of the unauthorized use of a resource
  - Controls who can have access to a resource.

43

Security Services (X.800)

- Data confidentiality: protection of data from unauthorized disclosure
  - Protection of transmitted data from passive attacks.
  - Broader service: protects all user data transmitted between two users over a period of time.
  - Narrower service: protection of a single message or specific fields within a message

44

Security Services (X.800)

- Data integrity: assurance that data received is as sent by an authorized entity
  - Integrity can apply to a stream of messages, a single message, or selected fields within a message.
  - Most useful: total stream protection
    - Connection-oriented integrity service: assures that messages are received as sent with no duplication, insertion, modification and denial of service

45

Security Services (X.800)

- Nonrepudiation: protection against denial by one of the parties in a communication
  - Proof that the message was sent by the specified party
  - Proof that the message was received by the specified party

46

Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- However one particular element underlies many of the security mechanisms in use:
  - cryptographic techniques

47

Security Mechanisms (X.800)

- Specific security mechanisms:
  - Encipherment: the use of mathematical algorithms to transform data into a form that is not readily intelligible
  - Digital signatures: data appended to a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery
  - Access control: enforce access rights to resources
  - Data integrity: assure the integrity of a data unit or stream of data units.

48

Security Mechanisms (X.800)

- Specific security mechanisms:
  - Authentication exchange: ensure the identity of an entity by means of information exchange.
  - Traffic padding: the insertion of bits into gaps in a data stream to frustrate traffic analysis
    - Make it difficult for an attacker to distinguish between true data flow and noise
    - Make it difficult to deduce the amount of traffic.

49

Relationship Between Security Services and Mechanisms

	Mechanism							
Service	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

50