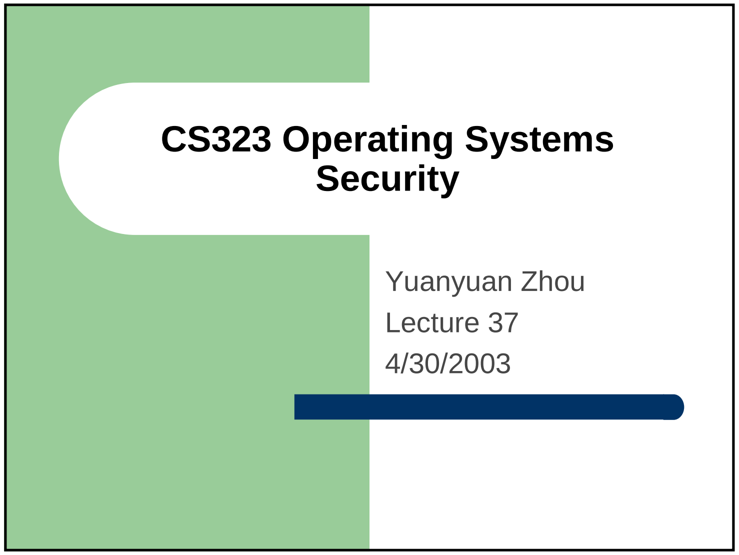
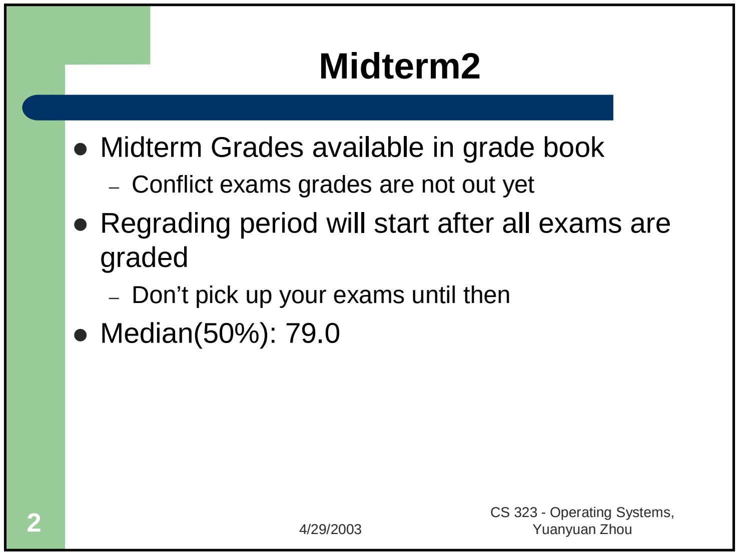


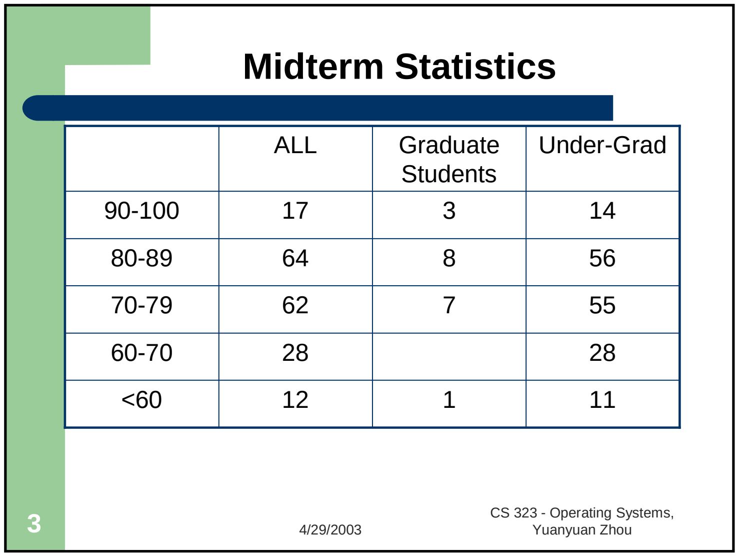
CS323 Operating Systems Security

Yuanyuan Zhou
Lecture 37
4/30/2003



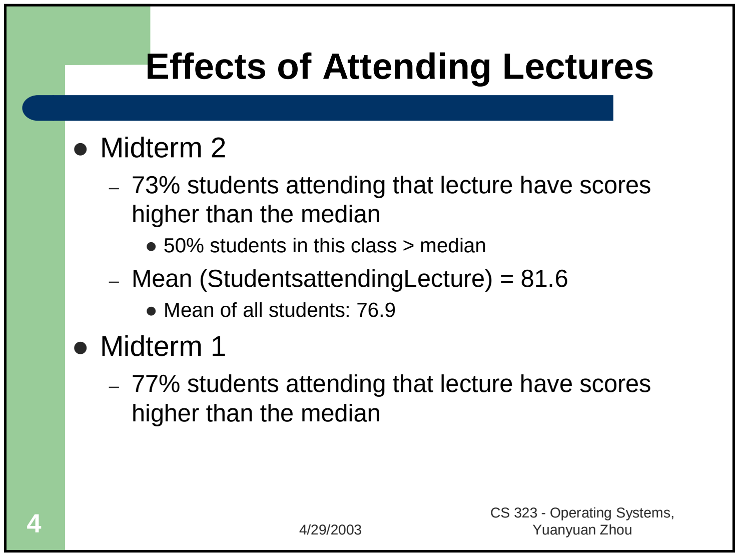
Midterm2

- Midterm Grades available in grade book
  - Conflict exams grades are not out yet
- Regrading period will start after all exams are graded
  - Don’t pick up your exams until then
- Median(50%): 79.0



Midterm Statistics

	ALL	Graduate Students	Under-Grad
90-100	17	3	14
80-89	64	8	56
70-79	62	7	55
60-70	28		28
<60	12	1	11



Effects of Attending Lectures

- Midterm 2
  - 73% students attending that lecture have scores higher than the median
    - 50% students in this class > median
  - Mean (StudentsattendingLecture) = 81.6
    - Mean of all students: 76.9
- Midterm 1
  - 77% students attending that lecture have scores higher than the median

User Authentication

- **User Attributes**: Something about the person -- e.g., fingerprints, voice-prints, photographs, signatures.
- **User Possession**: Something possessed by the person -- e.g., badges, id cards, keys.
- **User Knowledge**: Something known by the person -- e.g., passwords, lock combinations, mother-in-law's maiden name.

Passwords

- People tend to choose easy-to-remember passwords, which are also easy to guess.
- Short passwords can be guessed by repeated trials of all possibilities.
- Passwords that are too long prompt people to write them down, which risks compromise by loss or theft of the note.
- The best passwords are of length 6-10 chars.
- Avoid words that are in a dictionary.
- Passwords made up of nonsense syllables are almost as secure as those made up of randomly chosen characters, but are easier to remember.

How Crackers Break-in?

- Password guessing
  - crackers compile potential common words as passwords, and use them to login.
- War dialers
  - dial telephone numbers and detect if security is in place (some PC systems don't have passwords).
- Over Internet attack, using IP addresses (ping, telnet)
- Weak root password and installation of packet sniffer
- Script kiddies
  - scripts found on the Internet, use brute force attacks to exploit bugs in specific programs.

Protect Your Passwords

- One-way encrypt the password file
  - UNIX designers are so confident of their one-way encryption scheme that the UNIX password file is ``read permitted'' to all users.
- Encourage uses to change passwords often
- Limit the number of attempts to enter a password.
- The standard way to crack UNIX encryption
  - copy the password file to another machine
  - try encrypting the dictionary, permutations of common words, wife names, telephone numbers and comparing it against the password file contents.
- ``Salt'' technique (by Morris and Thompson):
  - associate an n-bit random number, called the **salt**, with each password. The random number is changed whenever the password is changed.

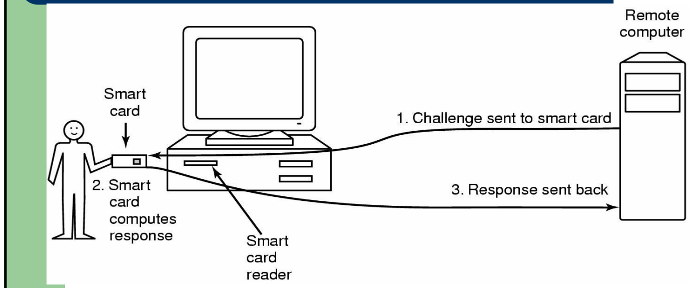
One-Time Password

- Extreme form of changing the passwords all the time
- When one-time passwords are used, the user gets a book containing a list of passwords. Each login uses the next password.
- More elegant scheme by Leslie Lamport: use one-way function which has property: given x it is easy to find y = f(x), but given y it is computationally infeasible to find x.
- Protocol:
  - User picks a secret password ``s'' that he memorizes.
  - User picks an integer ``n'', which is how many one-time passwords the algorithm is able to generate.
  - The first password is given by running the one-way function n times:
  - The second password is give by running the one-way function n-1 times:
- Note that given any password in the sequence, it is easy to compute previous password, but impossible the next one

Challenge-Response Authentication

- New user provides a long list of questions and answers which are securely stored.
- When the user logs in, randomly a question is asked and the server checks the answer.
- Another variation
  - user picks an algorithm when signing up as a user (e.g.,). When the user logs in, the server sends the user an argument (e.g., 7), and the user applies the agreed algorithms, and responses (e.g., 49). The server applies the algorithm as well as compares the answers.

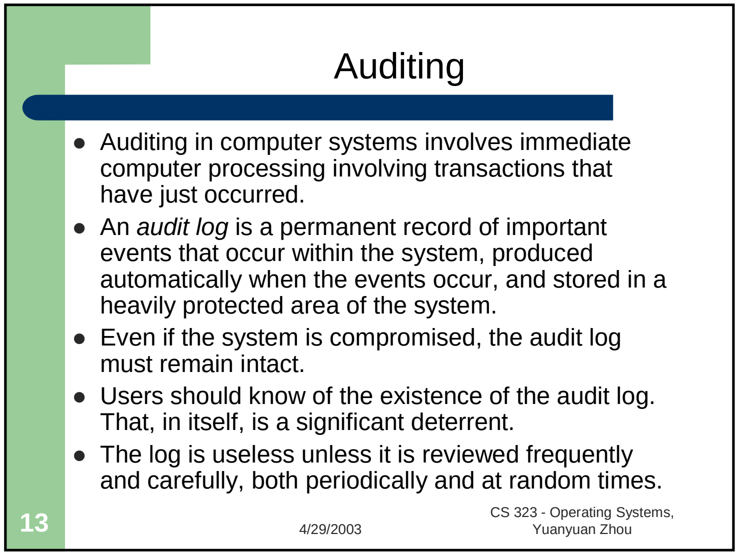
Authentication Using a Physical Object



- Magnetic cards
  - magnetic stripe cards
  - chip cards: stored value cards, smart cards

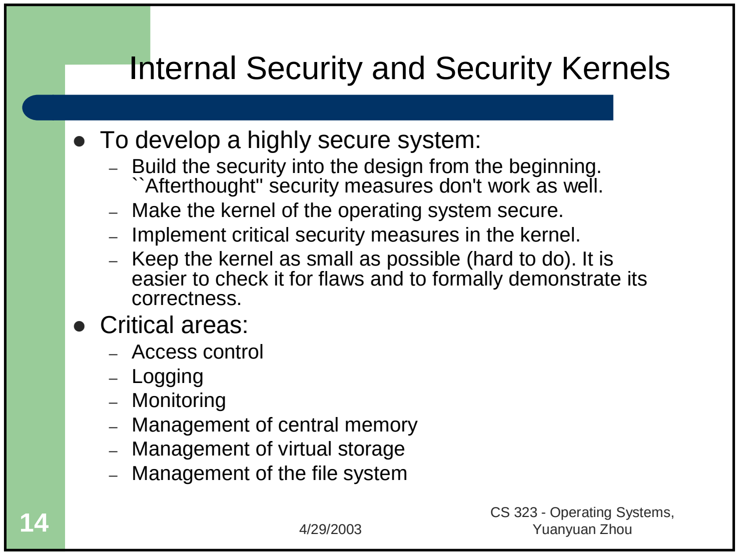
Authentication Using Biometrics

- Use physical characteristics of the users that are hard to forge for authentication, called biometrics.
- Biometrics systems have two parts: enrollment and identification.
- Finger length analysis is practical
- Retinal pattern analysis
- Signature analysis
- Voice biometrics



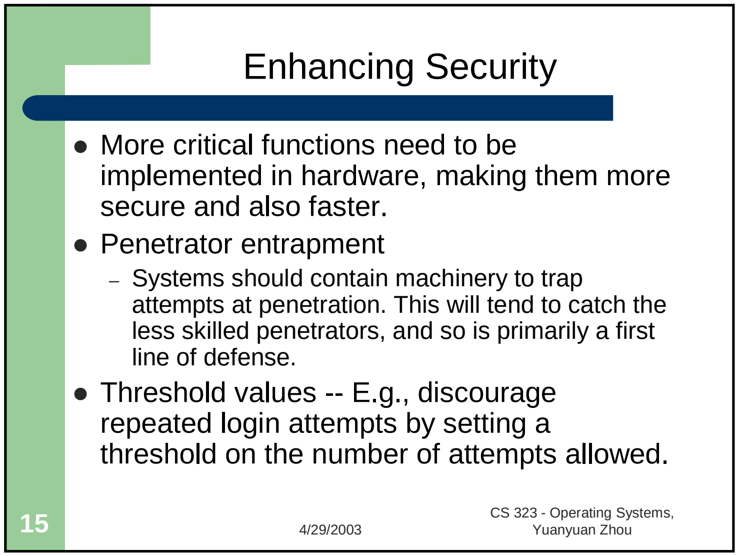
Auditing

- Auditing in computer systems involves immediate computer processing involving transactions that have just occurred.
- An *audit log* is a permanent record of important events that occur within the system, produced automatically when the events occur, and stored in a heavily protected area of the system.
- Even if the system is compromised, the audit log must remain intact.
- Users should know of the existence of the audit log. That, in itself, is a significant deterrent.
- The log is useless unless it is reviewed frequently and carefully, both periodically and at random times.



Internal Security and Security Kernels

- To develop a highly secure system:
  - Build the security into the design from the beginning. ``Afterthought'' security measures don't work as well.
  - Make the kernel of the operating system secure.
  - Implement critical security measures in the kernel.
  - Keep the kernel as small as possible (hard to do). It is easier to check it for flaws and to formally demonstrate its correctness.
- Critical areas:
  - Access control
  - Logging
  - Monitoring
  - Management of central memory
  - Management of virtual storage
  - Management of the file system



Enhancing Security

- More critical functions need to be implemented in hardware, making them more secure and also faster.
- Penetrator entrapment
  - Systems should contain machinery to trap attempts at penetration. This will tend to catch the less skilled penetrators, and so is primarily a first line of defense.
- Threshold values -- E.g., discourage repeated login attempts by setting a threshold on the number of attempts allowed.