CSc 466/566

Computer Security

0 : Administrivia

Version: 2012/02/19 10:49:51

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

Outline

Contact Information

Class:	466/566 — Computer Security
Instructor:	Christian Collberg
WWW:	http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012
Office:	Gould-Simpson 758
Office Hours:	Tuesday 09:00-10:00
Phone:	621-6612
Lectures:	MW 16:30-17:45, PSYCH 306

Course Communication

Here are ways to communicate with me and the rest of the class:

Email: collberg@gmail.com.

Sign up for the class on: d2l.arizona.edu.

Teaching Assistants

TAs: Nitin Shinde

Email: nitinshinde@email.arizona.edu

Office: GS 721

Office hours: Wed 11:00 – 13:00

Prerequisites

- You should be a proficient C programmer. Some knowledge of Java may also be necessary.
- You should have some background in an assembly language. It doesn't matter which one.
- You should have a functional understanding of Unix, i.e. shell commands, editing (`emacs`, `vi`), compiling (`gcc`), makefiles, etc.

Syllabus

You are responsible for reading
and understanding this syllabus.
If you have any concerns or issues
about the information in this document
you should bring them up during the
first week of class.

Exam-schedule

Midterm: The midterm exam is scheduled for Mon Mar 19. This may change, so pay attention in class and check the web site.

Final: The final exam is scheduled for Wed May 11, 13:00-15:00.

Office hours

- Office hours: Tuesday 09:00-10:00
- I use an open door policy:

Collberg's Café

- Please come and see me to chat, ask questions, or snack:

Outline

Course Description

Course Description

This is an introductory course covering the fundamentals of computer security. In particular, the course will cover basic concepts of computer security such as threat models and security policies, and will show how these concepts apply to specific areas such as communication security, software security, operating system security, network security, web security, and hardware-based security.

Course Objectives and Expected Learning Outcomes

Expected Learning Outcomes

At the end of the course you should be able to recognize potential threats to confidentiality, integrity, and availability, and have a basic understanding of the tools and techniques available to adversaries to violate the security of a system as well as the tools and techniques available to defend against such attacks.

Topics I

Communication security: cryptography and cryptographic protocols, including encryption, message authentication codes, hash functions, one-way functions, public-key cryptography, digital signatures, cryptographic protocols.

Topics II

Operating system security: memory protection, access control, authorization, authenticating users (something you know, something you have, something you are, password cracking.

Topics III

Intellectual property protection: digital rights management, copy protection, software tamper-resistance.

Outline

Textbooks

- *Introduction to Computer Security*, by Goodrich and Tamassia.
- http://www.securitybook.net

Handouts & Other Material

1. Various web resources.
2. I always make copies of my transparencies available to students on the class website. Note that
   - I do this to relieve you of having to take notes during class,
   - they are not a substitute for reading the textbook,
   - their primary purpose is to remind you of what you need to study for the exam.
3. Various manuals and papers may be handed out during class.

Outline

Undergraduate Student News Stories Presentations

- At the beginning of every class 1-2 students will present a security-related story they've found in the news.
- Each undergraduate student has to present one story during the course of the semester.
- I will pass around a signup sheet at the beginning of the semester.

Topics

- Ideally, you should find a story that you can relate to what we're talking about in class, but it's not absolutely necessary.
- Stories about computer security are preferred, of course, but stories about failed physical security are fine too (TSA security, nuclear power station security, military security,...).
- You don't necessarily have to talk about something technical — security is as much about politics as anything else.
- Try to find a topic that engages you, and is likely to engage the class.
- Register the story you're going to talk about on `d2l.arizona.edu` to make sure that no one else will talk about the same topic!

Structure of the Presentation

- Each presentation should be no longer than 5 minutes. I will cut you off mercilessly of you go over time.
- Since you only have 5 minutes, it's important that you think through what you are going to say, and plan out your presentation in some detail.
- Try to engage the class by asking them questions during the presentation.

Presentation Slides

- Use LaTeX/Beamer to put together a few slides to help structure the presentation:

Presentation Slides

- Use LaTeX/Beamer to put together a few slides to help structure the presentation:
  1. a slide with a title, your name, and where you picked up the news story;

Presentation Slides

- Use LaTeX/Beamer to put together a few slides to help structure the presentation:
  1. a slide with a title, your name, and where you picked up the news story;
  2. an introductory slide giving a brief overview of what you are going to talk about;

Presentation Slides

- Use LaTeX/Beamer to put together a few slides to help structure the presentation:
  1. a slide with a title, your name, and where you picked up the news story;
  2. an introductory slide giving a brief overview of what you are going to talk about;
  3. 1-3 slides with the meat of the presentation;

Presentation Slides

- Use LaTeX/Beamer to put together a few slides to help structure the presentation:
  1. a slide with a title, your name, and where you picked up the news story;
  2. an introductory slide giving a brief overview of what you are going to talk about;
  3. 1-3 slides with the meat of the presentation;
  4. a slide discussing/summarizing the story, asking a few poignant questions.

Presentation Slides

- Use LaTeX/Beamer to put together a few slides to help structure the presentation:
  1. a slide with a title, your name, and where you picked up the news story;
  2. an introductory slide giving a brief overview of what you are going to talk about;
  3. 1-3 slides with the meat of the presentation;
  4. a slide discussing/summarizing the story, asking a few poignant questions.
- To make sure we're not wasting any time, please put your slides on the web so that we can quickly fire them up at the beginning of class.

Presentation Slides

- Use LaTeX/Beamer to put together a few slides to help structure the presentation:
  1. a slide with a title, your name, and where you picked up the news story;
  2. an introductory slide giving a brief overview of what you are going to talk about;
  3. 1-3 slides with the meat of the presentation;
  4. a slide discussing/summarizing the story, asking a few poignant questions.
- To make sure we're not wasting any time, please put your slides on the web so that we can quickly fire them up at the beginning of class.
- Also submit the LaTeX/Beamer slides to `d2l`.

Assessment

You will be assessed on

1. the relevance of your story to the class;

Assessment

You will be assessed on

1. the relevance of your story to the class;
2. the depth of thinking you've done on your chosen story;

Assessment

You will be assessed on

1. the relevance of your story to the class;
2. the depth of thinking you've done on your chosen story;
3. how well you've prepared and rehearsed your presentation;

Assessment

You will be assessed on

1. the relevance of your story to the class;
2. the depth of thinking you've done on your chosen story;
3. how well you've prepared and rehearsed your presentation;
4. your use of slides, blackboard, computer, etc. during the presentation;

Assessment

You will be assessed on

1. the relevance of your story to the class;
2. the depth of thinking you've done on your chosen story;
3. how well you've prepared and rehearsed your presentation;
4. your use of slides, blackboard, computer, etc. during the presentation;
5. the quality of your slides (use of illustrations, language, structure, etc.);

Assessment

You will be assessed on

1. the relevance of your story to the class;
2. the depth of thinking you've done on your chosen story;
3. how well you've prepared and rehearsed your presentation;
4. your use of slides, blackboard, computer, etc. during the presentation;
5. the quality of your slides (use of illustrations, language, structure, etc.);
6. how well organized your presentation was;

Assessment

You will be assessed on

1. the relevance of your story to the class;
2. the depth of thinking you've done on your chosen story;
3. how well you've prepared and rehearsed your presentation;
4. your use of slides, blackboard, computer, etc. during the presentation;
5. the quality of your slides (use of illustrations, language, structure, etc.);
6. how well organized your presentation was;
7. if you timed your presentation well;

Assessment

You will be assessed on

1. the relevance of your story to the class;
2. the depth of thinking you've done on your chosen story;
3. how well you've prepared and rehearsed your presentation;
4. your use of slides, blackboard, computer, etc. during the presentation;
5. the quality of your slides (use of illustrations, language, structure, etc.);
6. how well organized your presentation was;
7. if you timed your presentation well;
8. if you spoke clearly and at the right pace.

Resources

Here are some web sites you can check for newsworthy stories:

- http://seclists.org
- http://www.schneier.com
- http://computersecuritynews.us
- http://www.securityfocus.com
- http://www.securityweek.com
- http://news.yahoo.com/security
- http://www.sciencedaily.com/news/computers_math/encryption
- http://news.cnet.com/defense-in-depth

Feel free to check with me if a particular story is suitable for presentation.

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?
3. talk about this really cool security problem we had at work?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?
3. talk about this really cool security problem we had at work?
4. copy pictures/illustrations from the news source I read rather than make my own?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?
3. talk about this really cool security problem we had at work?
4. copy pictures/illustrations from the news source I read rather than make my own?
5. not rehearse my presentation?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?
3. talk about this really cool security problem we had at work?
4. copy pictures/illustrations from the news source I read rather than make my own?
5. not rehearse my presentation?
6. make really boring slides with lists-of-lists-of-lists-. . . ?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?
3. talk about this really cool security problem we had at work?
4. copy pictures/illustrations from the news source I read rather than make my own?
5. not rehearse my presentation?
6. make really boring slides with lists-of-lists-of-lists-. . . ?
7. forget I had to do a presentation and then sign up for another slot later?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?
3. talk about this really cool security problem we had at work?
4. copy pictures/illustrations from the news source I read rather than make my own?
5. not rehearse my presentation?
6. make really boring slides with lists-of-lists-of-lists-. . . ?
7. forget I had to do a presentation and then sign up for another slot later?
8. go over time, just a little, I only have a few more slides, and there's so much more to say, and. . . ?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/Beamer?
2. work with someone rather than present alone?
3. talk about this really cool security problem we had at work?
4. copy pictures/illustrations from the news source I read rather than make my own?
5. not rehearse my presentation?
6. make really boring slides with lists-of-lists-of-lists-. . . ?
7. forget I had to do a presentation and then sign up for another slot later?
8. go over time, just a little, I only have a few more slides, and there's so much more to say, and. . . ?

No.

Outline

Graduate Student Lectures

- Masters and PhD students enrolled in the class will pair up to research a topic and present it to the class.
- This is not the normal "read a paper and present it in class" type of assignment. Rather, you will be given a fairly broad topic that you will research thoroughly throughout the semester. At the end of the semester you will have

- Thus, the last 5 lectures will be given by graduate students.

Graduate Student Lectures

- Masters and PhD students enrolled in the class will pair up to research a topic and present it to the class.
- This is not the normal "read a paper and present it in class" type of assignment. Rather, you will be given a fairly broad topic that you will research thoroughly throughout the semester. At the end of the semester you will have
  1. collected a comprehensive set of resources (books, papers, tools, etc.) relevant to the topic;

- Thus, the last 5 lectures will be given by graduate students.

Graduate Student Lectures

- Masters and PhD students enrolled in the class will pair up to research a topic and present it to the class.
- This is not the normal "read a paper and present it in class" type of assignment. Rather, you will be given a fairly broad topic that you will research thoroughly throughout the semester. At the end of the semester you will have
  1. collected a comprehensive set of resources (books, papers, tools, etc.) relevant to the topic;
  2. become an expert on your chosen topic,

- Thus, the last 5 lectures will be given by graduate students.

Graduate Student Lectures

- Masters and PhD students enrolled in the class will pair up to research a topic and present it to the class.
- This is not the normal "read a paper and present it in class" type of assignment. Rather, you will be given a fairly broad topic that you will research thoroughly throughout the semester. At the end of the semester you will have
  1. collected a comprehensive set of resources (books, papers, tools, etc.) relevant to the topic;
  2. become an expert on your chosen topic,
  3. written a 10-page paper summarizing the topic,

- Thus, the last 5 lectures will be given by graduate students.

Graduate Student Lectures

- Masters and PhD students enrolled in the class will pair up to research a topic and present it to the class.
- This is not the normal "read a paper and present it in class" type of assignment. Rather, you will be given a fairly broad topic that you will research thoroughly throughout the semester. At the end of the semester you will have
  1. collected a comprehensive set of resources (books, papers, tools, etc.) relevant to the topic;
  2. become an expert on your chosen topic,
  3. written a 10-page paper summarizing the topic,
  4. created a 30-slide presentation on the topic,

- Thus, the last 5 lectures will be given by graduate students.

Graduate Student Lectures

- Masters and PhD students enrolled in the class will pair up to research a topic and present it to the class.
- This is not the normal "read a paper and present it in class" type of assignment. Rather, you will be given a fairly broad topic that you will research thoroughly throughout the semester. At the end of the semester you will have
  1. collected a comprehensive set of resources (books, papers, tools, etc.) relevant to the topic;
  2. become an expert on your chosen topic,
  3. written a 10-page paper summarizing the topic,
  4. created a 30-slide presentation on the topic,
  5. delivered a 30 minute long (+ 5 minutes for questions) presentation on the topic.
- Thus, the last 5 lectures will be given by graduate students.

Due dates

Topic selection: 21:59, Jan 30

Resources: 23:59, Feb 15

First draft: 23:59, Mar 21

Second draft: 23:59, Apr 4

Final submission: 23:59, Apr 11

Presentations: Apr 16, 18, 23, 25, 30

The paper

- The paper should give a thorough introduction to your chosen topic, suitable for someone with no previous background (such as your classmates).
- It should not be be organized as a survey paper ("and in this paper they said the following..."), but rather as a chapter in a textbook, say.
- Obviously, you still need to references relevant works. This can be done in a separate section at the end, or throughout the report.
- Illustrations and examples are very important, and should help the reader grasp the subject.

Topic Selection

- Select your preferred presentation topics.
- Send email to `nitinshinde@email.arizona.edu` immediately after 21:59, Jan 30 (emails received before will be ignored) consisting of
  1. the subject line 566 presentation topic;
  2. GROUP: `student1, student2`;
  3. RANKING: `topic preference` (most desired topic first).
- For example, an email 5,4,1,6 indicates to me that you most prefer topic 5, then 4, then 1, then 6, and after that, you don't care.
- Topics will be assigned on a first-come-first-served basis.

Resources I

- Start your research on your assigned topic by collecting a list of references that you plan to use in the presentation. This can include books, papers, web sites, tools, etc.
- Upload to d2l a zip-file named `topic⟨topic-number⟩-resources.zip`;
- The zip-file should consist of a directory named topic⟨topic-number⟩-resources containing (at least) the following files:
  1. A BibTeX file `references.bib` with all the resources, each resource annotated with a paragraph, describing the contents.
  2. A LaTeX file `report.tex` that produces an annotated bibliography.
  3. A `makefile` that builds `report.pdf`. The `makefile` should work (at least) on the department's `lectura` system.
  4. A text file `README` that lists the names of the group members.

Resources II

5. Any other files (such as `annotate.bst`) that are necessary to build your presentations.
6. A subdirectory resources containing the `pdf` files of all the papers you've used.

- You may, of course, add additional resources during the semester, as your research progresses.
- Make an appointment with me to discuss your progress so far. Together we will go over the resources you've collected, the direction in which your research is taking you, and possibly steer you in a different direction.

First Draft I

- At this stage, you should have produced
  1. 15 LaTeX/Beamer slides, at least 7 slides with illustrations;
  2. A 5-page LaTeX paper, with at least 3 drawings/illustrations, 11pt, 1in margins, single column.
     Don't include the bibliography annotations!
- The first draft should take into account previous feedback from the instructor.
- Don't plagiarize text/images/drawings from any resource!
- A `README` file that should now also include
  1. an outline of how you intend to run/organize your presentation;
  2. some ideas of in-class exercises you intend to run, tools you intend to demonstrate, etc.
- Upload to d2l a zip-file named `topic⟨topic-number⟩-first-draft.zip`;

First Draft II

- The zip-file should consist of a directory named `topic⟨topic-number⟩-first-draft` containing the same files as before, plus
  1. A Beamer file `slides.tex` consisting of the presentation slides;
  2. A `makefile` that now also builds `slides.pdf`.
- Make an appointment with me to discuss your progress so far.

Second Draft I

- At this stage, you should have produced
  1. 30 LaTeX/Beamer slides, at least 20 slides with illustrations;
  2. A 10-page LaTeX paper, with at least 5 drawings/illustrations, 11pt, 1in margins, single column.
     Don't include the bibliography annotations!
- The second draft should take into account feedback from the instructor on the first draft.
- A `README` file that should now also include
  1. detailed, step-by-step, instructions for how you intend to run/organize your presentation;
  2. detailed, step-by-step, instructions for the 1-2 in-class exercises you intend to run.
- Upload to d2l a zip-file named `topic⟨topic-number⟩-second-draft.zip`;

Second Draft II

- The zip-file should consist of a directory named `topic⟨topic-number⟩-second-draft` containing the same files as before, plus
  1. A LaTeX file `eval.tex` consisting of end-of-class evaluation (I will provide a template);
  2. A `makefile` that now also builds `eval.pdf`.
- Make an appointment with me to discuss your progress so far.

Final Version

- Submit final presentation, slides, exercises, etc.
  1. Upload to d2l a zip-file named `topic⟨topic-number⟩-final.zip`;
  2. make the zip-file consist of a directory named `topic⟨topic-number⟩-final` containing all the documents.
- Note that this is a hard deadline. I won't accept any late submissions.
- Make sure to adjust your paper and slides based on any feedback you have received from the instructor.
- You can't make any changes to the presentation slides after the submission. (This is so that every group has the same amount of time to prepare their presentation.)

Presentations

- Presentations, 1/2 lecture each;
- 2 minutes setup time;
- 30 minutes presentation (you are expected to not exceed this, and not not be any shorter than 28 minutes);
- 5 minutes questions.

Topics I

1. Hardware game console hacking

   Starting point: *Hacking the XBOX*, hackingthexbox.com/

2. Tempest

   Starting point: www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf; en.wikipedia.org/wiki/TEMPEST

3. Hardware hacking

   Starting point: www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf

4. Hacking networked games

   Starting point: Greg Hoglund, Gary McGraw, *Exploiting Online Games: Cheating Massively Distributed Systems*

Topics II

5. Phishing

   Starting point: Markus Jakobsson, Steven Myers, *Phishing and Countermeasures: Understanding the Increasing Problem...*

6. Electronic voting

   Subtopics: Computer voting techniques, electronic voting machines vulnerabilities.

   Starting point: avirubin.com/vote.pdf

7. Password cracking

   Subtopics: Cracking, rainbow tables, alternatives (graphical passwords, etc.)

Topics III

Starting point: Simon Marechal, *Advances in password cracking, Journal in Computer Virology, 2008*, dx.doi.org/10.1007/s11416-007-0064-y; en.wikipedia.org/wiki/Rainbow_table

8. **Two-party computation**

   Starting point: www.pinkas.net/PAPERS/MNPS.pdf; en.wikipedia.org/wiki/Secure_multi-party_computation

   Software: See me for a copy of the `fairplay` system.

9. **Stuxnet**

   Subtopics: Who-dunnit?, techniques used

   Starting point: en.wikipedia.org/wiki/Stuxnet; http://youtu.be/fVNHX1Hrr6w

10. **Insider attacks**

Topics IV

Starting point: Angelos Keromytis, Salvatore J. Stolfo, Sara Sinclair, Sean W. Smith, Shlomo Hershkop, Steven M. Bellovin, *Insider Attack and Cyber Security. Beyond the Hacker*

Topics V

11. **Botnets**

    Starting point: Evan Cooke, Farnam Jahanian, Danny McPherson, *The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets*, USENIX SRUTI '05

12. **Honeypots**

    Starting point: Niels Provos, *A virtual honeypot framework*;

    en.wikipedia.org/wiki/Honeypot_(computing)

13. **Network security visualization**

    Starting point: Greg Conti, *Security Data Visualization: Graphical Techniques for Network Analysis*

Topics VI

14. Critical infrastructure security (SCADA)

Starting point: *Sandia Report: Advanced Metering Infrastructure Security Considerations*, www.oe.energy.gov/DocumentsandMedia/20-AMI_Security_Considerations.pdf; F. M. Cleveland, *Cyber security issues for Advanced Metering Infrasttructure*, www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf; Ross Anderson and Shailendra Fuloria, *Who controls the off switch?*

15. Security of Electronic Medical Records (EMR)

Starting point: Kai Wang and yan Sui and Xukai Zou and Arjan Durresi and Shiaofen Fang, *Pervasive and Trustworthy Healthcare*; Vince Stanford, *Pervasive Health Care Applications Face Tough Security Challenges*;

Topics VII

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;
3. your use of slides, blackboard, computer, etc. during the presentation;

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;
3. your use of slides, blackboard, computer, etc. during the presentation;
4. the quality of your slides (use of illustrations, language, structure, etc.);

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;
3. your use of slides, blackboard, computer, etc. during the presentation;
4. the quality of your slides (use of illustrations, language, structure, etc.);
5. how well organized your presentation was;

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;
3. your use of slides, blackboard, computer, etc. during the presentation;
4. the quality of your slides (use of illustrations, language, structure, etc.);
5. how well organized your presentation was;
6. if your presentation had the right level of technical detail;

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;
3. your use of slides, blackboard, computer, etc. during the presentation;
4. the quality of your slides (use of illustrations, language, structure, etc.);
5. how well organized your presentation was;
6. if your presentation had the right level of technical detail;
7. if you timed your presentation well;

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;
3. your use of slides, blackboard, computer, etc. during the presentation;
4. the quality of your slides (use of illustrations, language, structure, etc.);
5. how well organized your presentation was;
6. if your presentation had the right level of technical detail;
7. if you timed your presentation well;
8. if you spoke clearly and at the right pace;

Assessment

You will be assessed on

1. the depth of the research you've done on your chosen topic;
2. how well you've prepared and rehearsed your presentation;
3. your use of slides, blackboard, computer, etc. during the presentation;
4. the quality of your slides (use of illustrations, language, structure, etc.);
5. how well organized your presentation was;
6. if your presentation had the right level of technical detail;
7. if you timed your presentation well;
8. if you spoke clearly and at the right pace;
9. the quality (structure, language, organization) of your report.

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?
4. copy pictures/illustrations from papers I read rather than make my own?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?
4. copy pictures/illustrations from papers I read rather than make my own?
5. hand in the final version of the slide-set the day before my presentation?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?
4. copy pictures/illustrations from papers I read rather than make my own?
5. hand in the final version of the slide-set the day before my presentation?
6. make really boring slides with lists-of-lists-of-lists-. . . ?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?
4. copy pictures/illustrations from papers I read rather than make my own?
5. hand in the final version of the slide-set the day before my presentation?
6. make really boring slides with lists-of-lists-of-lists-. . . ?
7. not rehearse my presentation?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/. . . instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?
4. copy pictures/illustrations from papers I read rather than make my own?
5. hand in the final version of the slide-set the day before my presentation?
6. make really boring slides with lists-of-lists-of-lists-. . . ?
7. not rehearse my presentation?
8. improve the presentation slides after the final submission?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/... instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?
4. copy pictures/illustrations from papers I read rather than make my own?
5. hand in the final version of the slide-set the day before my presentation?
6. make really boring slides with lists-of-lists-of-lists-...?
7. not rehearse my presentation?
8. improve the presentation slides after the final submission?
9. go over time, just a little, I only have a few more slides, and there's so much more to say, and...?

FAQ

Can I

1. use Word/Pages/Powerpoint/Keynote/... instead of LaTeX/BibTeX/Beamer?
2. work alone/with 3 people rather than in a pair?
3. pick my own topic?
4. copy pictures/illustrations from papers I read rather than make my own?
5. hand in the final version of the slide-set the day before my presentation?
6. make really boring slides with lists-of-lists-of-lists-...?
7. not rehearse my presentation?
8. improve the presentation slides after the final submission?
9. go over time, just a little, I only have a few more slides, and there's so much more to say, and...?

No.

Outline

Course Work and Assessment

- There will be 4 take-home assignments.
- The assignments will be done in teams of 2 students.
- Masters and PhD students will research and present a topic of their choice.
- Undergraduate students will each give a 5-minute presentation on a security-related news story.
- Assessment for undergraduate students: Assignments 30%, news story presentation 10%, Midterm 20%, Final 40%.
- Assessment for Masters and PhD students: Assignments 20%, Topic presentation 20%, Midterm 20%, Final 40%.

Curving

- All grades (for exams, quizzes, assignments, etc) will be curved up by throwing away the highest grade in the class and scaling up such that the second highest grade is 100.
- The curving is done to adjust for particularly difficult tests/assignments, and to prevent an outlier from skewing the grade distribution.
- You cannot, after scaling, receive more than 100 on any exam, quiz, assignment, etc.

Grade Assignment

- You will fail the class if you get less than 50 (after curving) on the final exam.
- Otherwise, a curved total grade of [90,100] gives you an A, [80,89] a B, [70,79] a C, [60,69] a D, and 59 and below an E.

Detailed Grading Scheme

- To avoid any ambiguities, I have formalized the informal rules given above.
- The rules below should be considered *minimum* requirements to achieve a particular grade. The instructor reserves the right to do additional adjustments, as necessary.
- Any contradictions, omissions, errors, or ambiguities in the grading scheme will be resolved by the instructor.
- Any issues or concerns regarding the grading scheme should be brought to the attention of the instructor within the first week of class.

Curving I

- All raw scores range from 0 to 100.
- Each individual score (final, midterm, quizzes, assignments) will be curved using the function

$$\mathrm{curve}(\bar{x}, s) = \min(100, (100.0/\max(\bar{x} - \max(\bar{x})))\bar{x}_s)$$

  where $\bar{x}$ is a set of scores (for an assignment, a test, etc.) and s is a student.
- Note: $-$ is set subtraction.
- $\mathrm{curve}(\bar{x}, s)$ returns s's score, curved up by $100.0/\mathit{2nd\_highest\_class\_score}$.

Curving II

- For example, assume the following final exam scores:

  34 45 66 88 98

  After the curve has been applied, the scores will be

  38.6 51.1 75 100 100

Details — Exams

final exam:

- Let $\bar{f}$ be the set of final exam scores.
- Let $\bar{f}^s$ be the final exam score for student s.
- Let $\mathcal{W}^f$ be the weight of the final exam (40% (ugrad)/40% (grad)).
- $\bar{t}^s_f = \mathrm{curve}(\bar{f}, s)\mathcal{W}^f$ is the curved final score for s.

midterm exam:

- Let $\bar{m}$ be the set of midterm exam scores.
- Let $\bar{m}^s$ be the midterm exam score for student s.
- Let $\mathcal{W}^m$ be the weight of the midterm exam (20% (ugrad)/20% (grad)).
- $\bar{t}^s_m = \mathrm{curve}(\bar{m}, s)\mathcal{W}^m$ is the curved midterm score for s.

Details — Presentation

- Let $\bar{p}$ be the set of presentation scores.
- Let $\bar{p}^s$ be the presentation score for student s.
- Let $\mathcal{W}^p$ be the weight of the presentation (10% (ugrad)/20% (grad)).
- $\bar{t}_p^s = \mathrm{curve}(\bar{p}, s)\mathcal{W}^p$ is the curved presentation score for s.

Details — Assignments

- Let $\bar{a}_i$ be the set of scores for the i:th assignment.
- Let $\bar{a}_i^s$ be the score for student s on the i:th assignment.
- Let $\mathcal{W}_i^a$ be the weight of the i:th assignment ($\sum_i \mathcal{W}_i^a = 30\%\ (\mathrm{ugrad})/20\%\ (\mathrm{grad})$).
- Let $\bar{\alpha}_i^s$ be the assignment score after late penalties have been applied:

$$\bar{\alpha}_i^s = \begin{cases} \bar{a}_i^s & \text{if the assignment is handed in on time} \\ 0.9\bar{a}_i^s & \text{if the assignment is } > 0 \text{ and } \leq 24 \text{ hours late} \\ 0.8\bar{a}_i^s & \text{if the assignment is } > 24 \text{ and } \leq 48 \text{ hours late} \\ 0 & \text{if the assignment is } > 48 \text{ hours late} \end{cases}$$

Details — Assignments. . .

- $\bar{t}_a^s = \sum_i (\mathrm{curve}(\bar{\alpha}_i, s)\mathcal{W}_i^a)$ is the total curved assignment score for student s.
- If, for whatever reason, the actual number of assignments is less than the planned number, the $\mathcal{W}_i^a$'s will be scaled up uniformly.

Details — Total Scores

- The raw total score for student s is

$$\bar{t}_s = \bar{t}_f^s + \bar{t}_m^s + \bar{t}_p^s + \bar{t}_a^s$$

- We round up to the nearest integer:

$$\text{total}_s = \lceil \bar{t}_s \rceil$$

Details — Grade Assignment

- The final grade assignment for student s is

$$\text{grade}_s = \begin{cases} E & \text{if } t_f^s < 50 \\ \begin{cases} A & \text{if } \text{total}_s \in [90, 100] \\ B & \text{if } \text{total}_s \in [80, 89] \\ C & \text{if } \text{total}_s \in [70, 79] \\ D & \text{if } \text{total}_s \in [60, 69] \\ E & \text{if } \text{total}_s < 60 \end{cases} & \text{otherwise} \end{cases}$$

- In other words, a student with a curved final exam score $t_f^s < 50$ will fail the class, regardless of their results on the other assessment categories.

Outline

Attendance Policy

- My goal is to keep class attendance high so that we can get good discussions going in the class.
- You are not required to attend lectures, but...

  you cut class at your own risk.

  Anything covered in class or in any of the required readings is fair game on tests and exams.
- All holidays or special events observed by organized religions will be honored for those students who show affiliation with that particular religion. Absences pre-approved by the UA Dean of Students (or Dean's designee) will be honored.

Subject to Change Policy

- The information contained in this course syllabus, other than the grade and absence policies, may be subject to change with reasonable advance notice, as deemed appropriate by the instructor.
- The instructor reserves the right to
  1. add, drop, or change topics;
  2. change exam or homework dates, etc.
- Changes will be announced in class and on the class web site and/or on d2l.arizona.edu!
  You are responsible for checking these sites regularly.

Notification of Objectionable Materials

- There is no objectionable material in this class.

Students with Disabilities

- If you anticipate barriers related to the format or requirements of this course, please meet with me so that we can discuss ways to ensure your full participation in the course.
- If you determine that disability-related accommodations are necessary, please register with Disability Resources (621-3268; drc.arizona.edu) and notify me of your eligibility for reasonable accommodations. We can then plan how best to coordinate your accommodations.

Student Code of Academic Integrity I

- Assignments in this course require individual attention and effort to be of any benefit. All work is expected to be that of each student alone. You may not consult with others, except in ways specifically authorized by the course instructor. You also may not plagiarize another person's work or copy another person's code.
- Students are responsible for understanding and complying with the University's Code of Academic Integrity. A synopsis of the Code is attached; the full text is available from the Office of the Dean of Students in Room 203 Old Main. Among other provisions, the Code demands that the work you submit is your own, and that graded papers and exams will not subsequently be tampered with. Copying of another student's programs or data, or writings is prohibited when they are part

Student Code of Academic Integrity II

of a published class assignment; it is immaterial whether the copying is by computer, xerox, pen or other means. Witting collaboration in allowing such copying is also a Code violation.

- Assignments in this course require individual attention and effort
- Violations of the Code will, at minimum, result in loss of credit for a graded item. An egregious first violation or any second violation will minimally result in failure of the entire course.
- See also http://studpubs.web.arizona.edu/policies/cacaint.htm the University of Arizona Code of Academic Integrity.

I take academic integrity seriously! I will report *every* violation!

Expected classroom behavior

- Be courteous and treat others in the class with respect.
- Please be courteous to other students by refraining from talking, playing loud music in your headphones, etc.
- Silence cell phones, pagers, etc.
- We come to class to learn: don't read the newspaper, solve cross-word puzzles, etc.
- Treat the TAs with respect: they do their best to grade your assignments on time, help you with software installation problems, help you with assignments, etc. But they have their own class work to attend to, too.

Policies against threatening behavior

- Read and abide by the following link:

  http://policy.web.arizona.edu/~policy/threaten.shtml.

Assignment grade complaints/regrades

- You have 72 hours from when the assignment/quiz/midterm/exam/... grades have been returned to you to register a complaint with the TAs or me.
- First approach the TAs with your complaint. If the complaint was not resolved to your satisfaction, please contact me.
- I will not consider any regrade for any assessment if you have failed to register a complaint within the allowed time period.

Late turnins

- Course-work handed in no more than 24 hours late will incur a 10% penalty.
- Course-work handed in more than 24 but no more than 48 hours late will incur a 20% penalty.
- Course-work handed more than 48 hours after the deadline will receive a grade of 0.
- Course-work that has been marked as having a hard deadline will receive a grade of 0 if handed in late.

Making up Tests

You cannot make up tests/exams unless

1. you have notified the instructor in writing (email is fine) or by phone prior to the test that you will be absent, and
2. you receive permission from the instructor to take the test at a later date.

Incomplete work policy

- I will not assign incomplete grades except under exceptional circumstances .
- I decide what is an exceptional circumstance.

FAQ

1. I overslept and missed the midterm, can I take it later today?

FAQ

1. I overslept and missed the midterm, can I take it later today?
2. I just need a few more points to pass this class, can you regrade assignment 1 from back in September?

FAQ

1. I overslept and missed the midterm, can I take it later today?
2. I just need a few more points to pass this class, can you regrade assignment 1 from back in September?
3. Can I play *words with friends* in class?

FAQ

1. I overslept and missed the midterm, can I take it later today?
2. I just need a few more points to pass this class, can you regrade assignment 1 from back in September?
3. Can I play *words with friends* in class?
4. What if I sit way in the back of class and don't bother anyone?

FAQ

1. I overslept and missed the midterm, can I take it later today?
2. I just need a few more points to pass this class, can you regrade assignment 1 from back in September?
3. Can I play *words with friends* in class?
4. What if I sit way in the back of class and don't bother anyone?

No.

Outline

References

- LaTeX: http://www.latex-project.org/ftp.html
- Beamer: http://www.ctan.org/tex-archive/macros/latex/contrib/beamer/
- You can download the templates below from here:

  http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resourcesl

Article style

```
\documentclass[11pt]{article}
\usepackage[margin=1in]{geometry}

\title{My Title Here}
\author{This is me!}

\begin{document}
\maketitle
\bibliographystyle{annotate}
```

Article style

```
\section{Section 1 Title Here!}
\begin{itemize}
   \item One
   \item Two
   \item Three
\end{itemize}

In reference~\cite{shang10malicious} Shang et al.
claim\ldots
```

Article style

```
\section{Section 2 Title Here!}
\begin{enumerate}
   \item One
   \item Two
   \item Three
\end{enumerate}

\subsection{Section 2 Subtitle Here!}
\begin{center}
   \scalebox{0.6}{\includegraphics{cafe.eps}}
\end{center}
```

Article style

```
\begin{center}
\begin{minipage}{5cm}
\begin{lstlisting}
if blah then
   boo
else
   blurp
endif
\end{lstlisting}
\end{minipage}
\end{center}
```

Article style

```
\begin{figure}
\begin{center}
\begin{minipage}{5cm}
\begin{lstlisting}
Here's some text in a
floating figure!
\end{lstlisting}
\end{minipage}
\end{center}
\caption{This is the caption of the floating figure!}
\label{floating:figure:label}
\end{figure}

In Figure~\ref{floating:figure:label} we show a floating
figure. You may have to re-run \LaTeX\ several times to
get the figure number right.
```

Article style

```
\section{Let's look at some tables!}
\begin{center}
\begin{tabular}{|l|p{3cm}|c|}\hline
boo & yo dude, sweet, no, really & duh \\\hline
boo & yo dude, sweet, no, really & duh \\\hline
boo & yo dude, sweet, no, really & duh \\\hline
\end{tabular}
\end{center}

In Figure~\ref{floating:table:label} we show a floating
table.
```

Article style

```
\section{Let's include a url!}
\begin{center}
\url{http://www.ctan.org/tex-archive/macros/latex/...}
\end{center}
\end{document}
```

BibTeX Bibliographies

```
@INPROCEEDINGS{shang10malicious,
    author    = {Shanhu Shang and Ning Zheng and Jian Xu
                 and Ming Xu and Haiping Zhang},
    booktitle = "{MALWARE}",
    title     = {Detecting malware variants via
                 function-call graph similarity},
    year      = 2010,
    month     = oct,
    pages     = {113 -120},
    annotate  = {This is an annotation},
}
```

Annotated bibliographies with BibTeX

- Use this BibTeX style:

  www.tex.ac.uk/tex-archive/biblio/bibtex/contrib/misc/annotate.bst.

- Add annotations to the BibTeX file:

```
annotate = {This is an annotation},
```

- Add the \nocite{*} command to include all your resources, to produce an annotated bibliography:

```
\documentclass{article}
\begin{document}
\bibliographystyle{annotate}
\nocite{*}
\bibliography{references.bib}
\end{document}
```

Beamer Slides

```
\documentclass[presentation,dvips]{beamer}
\title{My Title Here}
\author{This is me!}

\begin{document}
\maketitle

\begin{frame}[plain]
\begin{center}
   {\Huge Plain slide}
\end{center}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Itemized slide}
\begin{itemize}
   \item One
   \item Two
   \item Three
\end{itemize}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Enumerated slide}
\begin{enumerate}
   \item One
   \item Two
   \item Three
\end{enumerate}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Incrementally revealed}
\begin{enumerate}
   \item<1-> One
   \item<2-> Two
   \item<3-> Three
\end{enumerate}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Include postscript}
\begin{center}
   \scalebox{0.6}{\includegraphics{cafe.eps}}
\end{center}
\end{frame}
```

Beamer Slides

```
\begin{frame}[containsverbatim]\frametitle{Include code}
\begin{center}
\begin{minipage}{5cm}
\begin{lstlisting}
if blah then
   boo
else
   blurp
endif
\end{lstlisting}
\end{minipage}
\end{center}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Include table}
\begin{center}
\begin{tabular}{|l|p{3cm}|c|}\hline
boo & yo dude, sweet, no, really & duh \\\hline
boo & yo dude, sweet, no, really & duh \\\hline
boo & yo dude, sweet, no, really & duh \\\hline
\end{tabular}
\end{center}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Include URLs}
Lear more about the Beamer class here:
\begin{center}
\url{http://www.ctan.org/tex-archive/macros/latex/...}
\end{center}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Include theorem}
    \framesubtitle{\textit{reductio ad absurdum}.}
    \begin{theorem}There is no largest prime number.
    \end{theorem}
    \begin{proof}
      \begin{enumerate}
         \item<1-| alert@1> Suppose $p$ ....
         \item<2-> Let $q$ be the product ....
         \item<3-> Then $q+1$ is ....
         \item<1-> Thus $q+1$ is ... $p$.\qedhere
      \end{enumerate}
   \end{proof}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Include theorem}
\begin{center}
\setbeamercolor{postit}{fg=black,bg=yellow}
\begin{beamercolorbox}[sep=1em,wd=5cm]{postit}
I am curious, yellow.
\end{beamercolorbox}
\end{center}
\end{frame}
```

Beamer Slides

```
\begin{frame}\frametitle{Split into columns}
\begin{center}
\begin{columns}[t]
    \column{5cm}
     One fish \\
     Two fish
    \column[T]{5cm}
     Red fish \\
     Blue fish
\end{columns}
\end{center}
\end{frame}

\end{document}
```

Outline

Round up the usual suspects. . .

Alice

Bob

Eve

Carol

Dave