

Computer Science 223
Advanced Computer Security
Spring 2006

Martín Abadi

University of California, Santa Cruz

Introduction

Instructor information

Instructor: Martín Abadi

- Office: E2 347A
- Email: abadi@cs.ucsc.edu
- Web: www.soe.ucsc.edu/~abadi/home.html
- Phone: +1 831 459 1489 (but email is better)

Office hours:

- Tuesdays, noon to 2pm, and
- by appointment

Instructor information (cont.)

Research in:

- computer and network security,
- programming languages,
- specification and verification methods.

Web pages

Course web pages:

- www.soe.ucsc.edu/~abadi/CS223_S06/home.html
- www.soe.ucsc.edu/classes/cms223/Spring06/

(For the course slides, see the former.)

Prerequisites

Some familiarity with computer systems:

- operating systems,
- networks,
- programming languages.

Some mathematical sophistication:

- a little number theory,
- ability to follow and do proofs,
e.g., proofs by induction,
- acquaintance with mathematical logic,
- ease with formal notation and manipulation,
but no advanced mathematics required.

Please see me if:

- you are not sure that you meet the prerequisites, or
- you are an undergraduate or a graduate student from outside CS or CE.

More administratrivia

Please give me:

- name,
- email address,
- program (e.g., MS in CS),
- year of study.

Contents

A graduate-level course.

An introduction to basic concepts and techniques in computer and network security.

A look at some more advanced topics, in particular, topics related to mobile code and to security protocols.

Course topics, in more detail

- Basics and principles.
- Access control
(including ACLs, capabilities, mobile code).
- A little cryptography.
- User authentication.
- Security protocols (such as SSL).
- Protocol analysis.
- PKIs.
- And a little more.

Likely guests

Mike Schroeder (Microsoft)

Úlfar Erlingsson (Microsoft)

Ilya Mironov (Microsoft)

Bruno Blanchet (École Normale Supérieure)

Brian Hernacki (Symantec)

Monica Chew (Google)

The many facets of security

The study of security intersects with many domains:

- cryptography,
- mathematics,
- operating systems,
- networking,
- human-computer interaction,
- economics,
- policy and law.

We should at least touch on all of these, but will not even attempt to cover all aspects of security.

Contents (cont.)

Not a course on cryptography.

Not a complete course on security.

Reading

Required reading:

- No textbook!
- Many papers, indicated during the course.

Some recommended reading:

- Ross Anderson's book:

[Security engineering: A guide to building dependable distributed systems](#)

www.cl.cam.ac.uk/~rja14/book.html

- For background on cryptography,

[The handbook of applied cryptography](#)

www.cacr.math.uwaterloo.ca/hac/index.html

More books

- Schneier's "Applied cryptography" ,
 - Schneier's "Secrets and lies" ,
 - Mitnick's "The art of deception" ,
 - Bishop's "Computer Security: Art and Science" ,
 - Cheswick and Bellovin's "Firewalls and Internet security" ,
 - Milner's "Communicating and mobile systems: the π -calculus" ,
 - Rescorla's "SSL and TLS" ,
 - Gong's "Inside Java 2 platform security" .
 - NRC's "Trust in cyberspace" ,
- www.nap.edu/readingroom/books/trust/.

Other resources

Web sites and mailing lists with reports of incidents,
e.g., www.cert.org.

Course notes, e.g.:

- Fred Schneider's:
www.cs.cornell.edu/Courses/cs513/2005fa/,
- Peter Gutmann's:
www.cs.auckland.ac.nz/~pgut001/tutorial/index.html.

Course work

Reading.

Class participation.

Homework:

- announced and explained in class, (usually on Thursdays),
- posted as part of the slides or with the slides,
- usually due at the start of class one week later (strictly!),
- mostly but not always fairly easy.

A medium-size final project.

No exams.

Grades

Grades are determined as follows:

- project (including its presentation): 40 - 50 %
- homework: 40 - 50 %
- class participation: the rest

Regular class attendance is required.

Cheating

All work you turn in must be your own.

If you don't know whether something is allowed, please ask.

Any cheating will result in failure of the course and other standard measures.

Cheating (cont.)

You are encouraged to discuss the course material and assignments with others.

You are not allowed to do assignments with others (except projects, with permission).

You may use any conversations, texts, or other material, as long as you cite your sources.

The final project

Three kinds:

- survey of recent work on a relevant topic,
 - small research paper,
 - programming project,
- all with brief reports.

Surveys must be done by one person.

Other projects may be done by teams of appropriate size (up to 4).

Picking a project

You are encouraged to define your own project.

If you prefer it, I will be happy to assign you a project, but I can't guarantee that you will be happy with it.

Scale

I don't expect very fancy projects. 30–40 hours of work should suffice, unless you are very enthusiastic.

However, you are welcome to tackle much more ambitious projects.

You should structure such a project so that you can show partial results this quarter.

Collaboration

You can do the projects (except for surveys) in groups of 1–4.

If you have a great project idea, and it looks too big for one person, feel free to recruit help.

I think that it is easier to do the projects alone, but you are welcome to make your own choices.

Cheating (cont.)

Projects should be new and original:

- not a cut-and-paste of prior work, (particularly not prior surveys),
- not also fulfilling the requirements of another course (except by special arrangement),
- not something you have already finished.

But it is good if you care about the project beyond completion of this course.

In a group project, you are expected to do your share. You should notify me if others are not doing theirs.

Kinds of projects

There are three basic kinds of projects:

- Survey of work in some area of security.
- Implementation of some security mechanism.
- Research in security.

These kinds can be combined to some extent.

In all cases, you must write a short report and make a short presentation.

The survey project

Pick an area in which you are interested.

For example:

- proof-carrying code,
- information-flow control in languages,
- network intrusion detection,
- some particular kind of security protocols
(e.g., commerce, password-based authentication),
- model-checking of security protocols,
- security of some particular sort of systems
(e.g., storage systems, hospitals),
- block ciphers and their modes of operations.

For more ideas, see the proceedings of recent security conferences.

The survey project (cont.)

Read well 2–5 papers (or a monograph?).

Read at least superficially 2–5 extra papers.

Write a short report on what you have learned about the area.

- What are the basic problems in this area?
- What are the basic approaches to solving them?
- What are the main achievements to date?

Keep the project narrow enough that you can say something interesting!

The implementation project

Implement some (non-trivial) security mechanism.

For example:

- a little protocol,
- some static analysis related to security,
- an auditing tool.

This sort of project is most appropriate in the context of a larger system that you are developing.

Write a short report on your project (1–2 pages).

How much code? There is no firm limit.

100 lines is probably too small.

10,000 is probably too big.

The research project

There are many sorts of research projects:

- Develop new security policies, mechanisms, and assurance techniques.
- Try to apply existing ones in new settings.
- Evaluate defenses.
- Develop theories or apply them.
- Explore interesting vulnerabilities.

In all cases, write a report on this work, of whatever length is appropriate.

The writing need not be publication-quality, but I should be able to read it easily.

The research project (cont.)

Research projects are the hardest.

Starting on a survey project and turning it into a research project may be possible, and is recommended unless you have clear research ideas already.

Reports and presentations

Project reports are due on **June 8**.

We will have brief presentations in class at the end of the quarter. (Please stay tuned.)

Extra work afterwards will be considered only in truly exceptional circumstances.