

# COMS W4187: Security Architecture and Engineering

Prof. Steven M. Bellovin

<http://www.cs.columbia.edu/~smb>



## Introduction

What is this Course?

Security Primitives

Security

Architecture

Security Engineering

How to Think About

Security

How to Think About

Insecurity. . .

Administrivia

What is Security?

# Introduction

# What is this Course?

Introduction

**What is this Course?**

Security Primitives

Security  
Architecture

Security Engineering  
How to Think About  
Security

How to Think About  
Insecurity...

Administrivia

What is Security?

- Security primitives
- Security architecture
- Security engineering
- How to think about security
- ⇒ How to think about insecurity...
- *Not* 4180 — complementary to it

---

## Introduction

What is this Course?

## Security Primitives

Security

Architecture

Security Engineering

How to Think About  
Security

How to Think About  
Insecurity...

---

## Administrivia

---

What is Security?

- What are the basic mechanisms you can use to secure a system?
- What are the properties of these mechanisms?
- What is the *assurance* associated with them?

Introduction

What is this Course?

Security Primitives

Security  
Architecture

Security Engineering

How to Think About  
Security

How to Think About  
Insecurity...

Administrivia

What is Security?

- How to put the pieces together
- How to spot the risky parts
- How to evaluate an architecture

## Introduction

What is this Course?

Security Primitives

Security

Architecture

## **Security Engineering**

How to Think About Security

How to Think About Insecurity...

## Administrivia

What is Security?

- Putting the pieces together
- Tradeoffs
- Balancing cost, security, usability, acceptability, and more

# How to Think About Security

Introduction

What is this Course?

Security Primitives

Security

Architecture

Security Engineering

How to Think About  
Security

How to Think About  
Insecurity...

Administrivia

What is Security?

- Security is a property of the overall design
- You do *not* get security by sprinkling on crypto or by forcing people to change their passwords frequently
- Those can sometimes help — but bad guys go around strong security, not through it
- Security is a *systems property*

# How to Think About Insecurity...

## Introduction

What is this Course?

Security Primitives

Security

Architecture

Security Engineering

How to Think About

Security

How to Think About  
Insecurity...

## Administrivia

What is Security?

- The bad guys don't follow the rules
- To understand how to secure a system, you have to understand what sort of attacks are possible
- Note that that is *not* the same as actually launching them...



Introduction

**Administrivia**

Course Structure

Readings

Logistics

Programming

Assignments

Co-operation versus

Dishonesty

Using Open Source

Programs

The Ethics of

Security

Not How I Teach It!

Contacting Me

Talking to Me

Class Schedule

TAs

Lectures

Homeworks

The Homework

Project

The CLIC Lab

Responsibility

Practical Focus

What is Security?

# Administrivia

- Introduction
- Administrivia
- Course Structure**
- Readings
- Logistics
- Programming Assignments
- Co-operation versus Dishonesty
- Using Open Source Programs
- The Ethics of Security
- Not How I Teach It!
- Contacting Me
- Talking to Me
- Class Schedule
- TAs
- Lectures
- Homeworks
- The Homework Project
- The CLIC Lab
- Responsibility
- Practical Focus
- What is Security?

- Lecture format
- Syllabus subject to change to discuss current events
- Approximate grading percentages:

Homework	50%
Midterm	20%
Final	30%

The percentages will be adjusted slightly if there are only four homework assignments instead of five.
- Grades will be posted on Courseworks
- Yes, I curve

- [Introduction](#)
- [Administrivia](#)
- [Course Structure](#)
- [Readings](#)
- [Logistics](#)
- [Programming Assignments](#)
- [Co-operation versus Dishonesty](#)
- [Using Open Source Programs](#)
- [The Ethics of Security](#)
- [Not How I Teach It!](#)
- [Contacting Me](#)
- [Talking to Me](#)
- [Class Schedule](#)
- [TAs](#)
- [Lectures](#)
- [Homeworks](#)
- [The Homework Project](#)
- [The CLIC Lab](#)
- [Responsibility](#)
- [Practical Focus](#)
- [What is Security?](#)

- *The Craft of System Security*, Sean Smith and John Marchesini, Addison-Wesley, 2008, ISBN 0-321-43483-8.
- Some primary source material — I assume you all know how to use the library and/or electronic resources. (Hint: Google does not (yet?) have access to all of the world's knowledge.)
- Note: ACM and IEEE readings are often only easily available from the campus network.

Introduction

Administrivia

Course Structure

Readings

**Logistics**

Programming

Assignments

Co-operation versus  
Dishonesty

Using Open Source  
Programs

The Ethics of  
Security

Not How I Teach It!

Contacting Me

Talking to Me

Class Schedule

TAs

Lectures

Homeworks

The Homework  
Project

The CLIC Lab

Responsibility

Practical Focus

What is Security?

- For grading issues, approach the TA within two weeks; if you don't receive a satisfactory answer, contact me.
- For issues relating to *this class*, email `smb+4187@cs...`
- That lets me auto-sort class-related mail and keep better track of things

[Introduction](#)

[Administrivia](#)

[Course Structure](#)

[Readings](#)

[Logistics](#)

[Programming Assignments](#)

[Co-operation versus Dishonesty](#)

[Using Open Source Programs](#)

[The Ethics of Security](#)

[Not How I Teach It!](#)

[Contacting Me](#)

[Talking to Me](#)

[Class Schedule](#)

[TAs](#)

[Lectures](#)

[Homeworks](#)

[The Homework Project](#)

[The CLIC Lab](#)

[Responsibility](#)

[Practical Focus](#)

[What is Security?](#)

- All programming homework *must* be done in C or C++ unless otherwise instructed. Don't bother asking for exceptions.
- Turn in a single tar file, including a Makefile; if necessary, include test data and a README file with execution instructions
- All programs *must* compile and run on Linux on the CLIC machines; zero credit for programs that don't compile.
- Because most security problems are due to buggy code, there will be copious deductions for bugs or for inadequate documentation

# Co-operation versus Dishonesty

- Introduction
- Administrivia
- Course Structure
- Readings
- Logistics
- Programming Assignments
- Co-operation versus Dishonesty**
- Using Open Source Programs
- The Ethics of Security
- Not How I Teach It!
- Contacting Me
- Talking to Me
- Class Schedule
- TAs
- Lectures
- Homeworks
- The Homework Project
- The CLIC Lab
- Responsibility
- Practical Focus
- What is Security?

- Discussing homework with others is encouraged — but all programs and written material *must* be individual work unless otherwise instructed.
- Please use appropriate file permission mechanisms to protect your homework. (Looking at other people's work is forbidden.)
- Zero tolerance for cheating
- See the department's honesty policy:  
<http://www.cs.columbia.edu/education/honesty> | will assume that you have all read it; you are in any event responsible for its terms and provisions.

- Introduction
- Administrivia
- Course Structure
- Readings
- Logistics
- Programming
- Assignments
- Co-operation versus Dishonesty
- Using Open Source Programs**
- The Ethics of Security
- Not How I Teach It!
- Contacting Me
- Talking to Me
- Class Schedule
- TAs
- Lectures
- Homeworks
- The Homework Project
- The CLIC Lab
- Responsibility
- Practical Focus
- What is Security?

- Generally, you are free to use any binary software installed on the CLIC machines
- Generally, you are welcome to use any open source software if (a) all such files are in a separate subdirectory from anything you write; (b) you clearly identify the origin of all such code; and (c) it all compiles seamlessly if the grader just types 'make' in the parent directory.
- *Exception:* you may not use outside code that accomplishes the primary purpose of the assignment.
- If in doubt, ask me *first*.

- Introduction
- Administrivia
- Course Structure
- Readings
- Logistics
- Programming
- Assignments
- Co-operation versus Dishonesty
- Using Open Source Programs
- The Ethics of Security**
- Not How I Teach It!
- Contacting Me
- Talking to Me
- Class Schedule
- TAs
- Lectures
- Homeworks
- The Homework Project
- The CLIC Lab
- Responsibility
- Practical Focus
- What is Security?

- Taking a computer security class is *not* an excuse for hacking
- “Hacking” is any form of unauthorized access, including exceeding authorized permissions
- The fact that a file or computer is not properly protected is no excuse for unauthorized access
- *If* the owner of a resource invites you to attack it, such use is authorized
- For more details, see [http://www.columbia.edu/cu/policy/network\\_use.html](http://www.columbia.edu/cu/policy/network_use.html)
- *Absolutely no Trojan horses, back doors, or other malicious code in homework assignments*



- Introduction

---

- Administrivia

---

- Course Structure
- Readings
- Logistics
- Programming Assignments
- Co-operation versus Dishonesty
- Using Open Source Programs
- The Ethics of Security
- Not How I Teach It!**

---

- Contacting Me
- Talking to Me
- Class Schedule
- TAs
- Lectures
- Homeworks
- The Homework Project
- The CLIC Lab
- Responsibility
- Practical Focus

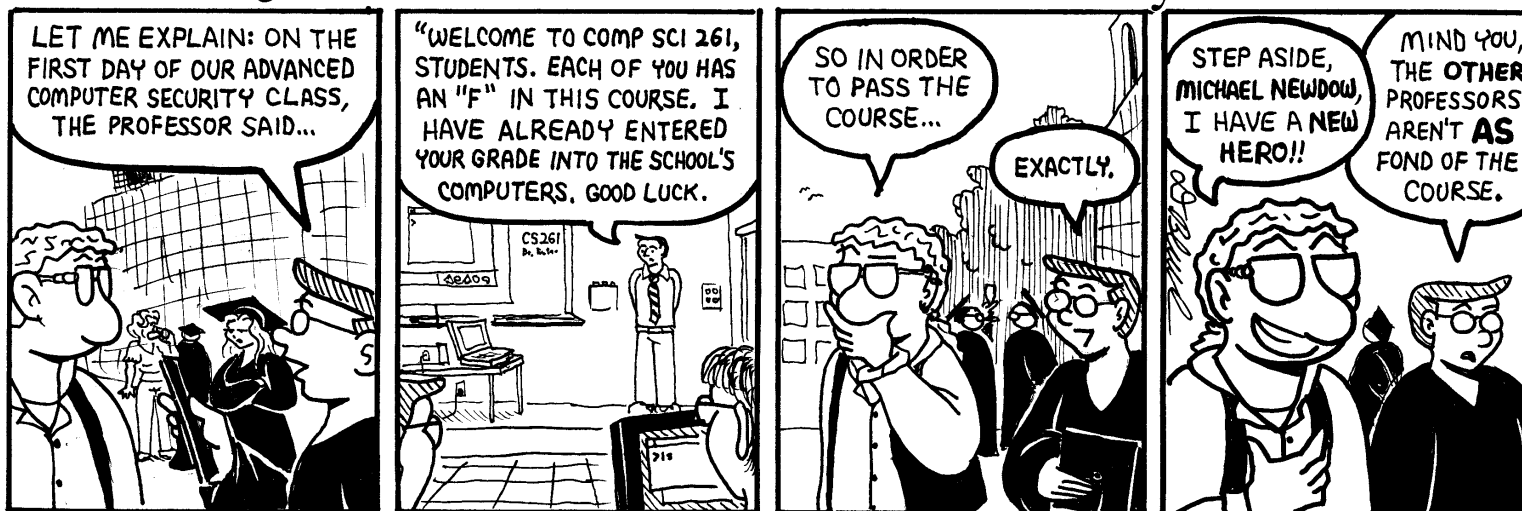
---

- What is Security?

---

## Nukees

by Darren Bleuel



<http://www.nukees.com>

Copyright 2007 Darren Bleuel. All rights reserved.

(Used with permission; see <http://www.nukees.com>)

[Introduction](#)

[Administrivia](#)

[Course Structure](#)

[Readings](#)

[Logistics](#)

[Programming](#)

[Assignments](#)

[Co-operation versus  
Dishonesty](#)

[Using Open Source  
Programs](#)

[The Ethics of  
Security](#)

[Not How I Teach It!](#)

[Contacting Me](#)

[Talking to Me](#)

[Class Schedule](#)

[TAs](#)

[Lectures](#)

[Homeworks](#)

[The Homework  
Project](#)

[The CLIC Lab](#)

[Responsibility](#)

[Practical Focus](#)

[What is Security?](#)

- Feel free to drop in during office hours.
- I'll announce changes on my home page
- I'm amenable to meeting other times, by appointment. You're welcome to drop in if my office door is open, but I reserve the right to ask you to come back later
- If you have any questions, please use email rather than telephone; I travel a lot and am not very reachable by phone

- Introduction
- Administrivia
- Course Structure
- Readings
- Logistics
- Programming
- Assignments
- Co-operation versus Dishonesty
- Using Open Source Programs
- The Ethics of Security
- Not How I Teach It!
- Contacting Me
- Talking to Me**
- Class Schedule
- TAs
- Lectures
- Homeworks
- The Homework Project
- The CLIC Lab
- Responsibility
- Practical Focus
- What is Security?

- Drop by, just to talk (a good idea if you think you'll want me to write a recommendation...)
- You don't need to be in trouble to talk with me...
- If my office door is open, just walk in
- But — I travel too much

Introduction

Administrivia

Course Structure

Readings

Logistics

Programming

Assignments

Co-operation versus

Dishonesty

Using Open Source

Programs

The Ethics of

Security

Not How I Teach It!

Contacting Me

Talking to Me

**Class Schedule**

TAs

Lectures

Homeworks

The Homework

Project

The CLIC Lab

Responsibility

Practical Focus

What is Security?

- The class may occasionally be rescheduled
- Some lectures may be available via CVN — feel free to watch it that way if they're available (but that's beyond my control)
- ⇒ This is best as a review; it's not a substitute for attending
- Tentative midterm date: October 20
- The final will be held on the date specified by the registrar

Introduction

Administrivia

Course Structure

Readings

Logistics

Programming

Assignments

Co-operation versus

Dishonesty

Using Open Source

Programs

The Ethics of

Security

Not How I Teach It!

Contacting Me

Talking to Me

Class Schedule

**TAs**

Lectures

Homeworks

The Homework

Project

The CLIC Lab

Responsibility

Practical Focus

What is Security?

## ■ TBA

Introduction

Administrivia

Course Structure

Readings

Logistics

Programming

Assignments

Co-operation versus

Dishonesty

Using Open Source

Programs

The Ethics of

Security

Not How I Teach It!

Contacting Me

Talking to Me

Class Schedule

TAs

**Lectures**

Homeworks

The Homework

Project

The CLIC Lab

Responsibility

Practical Focus

What is Security?

- I prepare slides for each class, and upload them shortly before class time
- Slides (and other information) are uploaded to my web page
- Well, occasionally they're uploaded shortly after class...

Introduction

Administrivia

Course Structure

Readings

Logistics

Programming

Assignments

Co-operation versus  
Dishonesty

Using Open Source  
Programs

The Ethics of  
Security

Not How I Teach It!

Contacting Me

Talking to Me

Class Schedule

TAs

Lectures

**Homeworks**

The Homework  
Project

The CLIC Lab

Responsibility

Practical Focus

What is Security?

- As noted, four or five homework assignments
- Homeworks are designed for practice, teaching, and evaluation
- Homeworks must be submitted electronically by the start of class
- Homeworks received later that day lose 5%, the next day 10%, two days late 20%, three days late 30%; after that, zero credit
- Exceptions granted only for *unforeseeable* events. Workload, day job, etc., are quite foreseeable.
- Problems? See me *before* the due date

# The Homework Project

[Introduction](#)

[Administrivia](#)

[Course Structure](#)

[Readings](#)

[Logistics](#)

[Programming](#)

[Assignments](#)

[Co-operation versus  
Dishonesty](#)

[Using Open Source  
Programs](#)

[The Ethics of  
Security](#)

[Not How I Teach It!](#)

[Contacting Me](#)

[Talking to Me](#)

[Class Schedule](#)

[TAs](#)

[Lectures](#)

[Homeworks](#)

[The Homework  
Project](#)

[The CLIC Lab](#)

[Responsibility](#)

[Practical Focus](#)

[What is Security?](#)

- 3 or 4 of the homeworks will be part of a single project — a “secure object store”
- As the semester goes on, more security features or requirements will be added: access control, encryption, authentication mechanisms, etc.
- You almost certainly *will* need to rearrange your code as the semester goes on
- Translation: modularity and clean design are very important



- All programs *must* run on the CLIC machines:  
<http://www.cs.columbia.edu/CLIC>)
- Programs that don't compile *on those machines* receive zero credit
- You need a CS account to use CLIC; see  
<https://www.cs.columbia.edu/~crf/accounts/>
- Some of the CLIC machines are for in-person use; others can only be accessed remotely

[Introduction](#)

[Administrivia](#)

[Course Structure](#)

[Readings](#)

[Logistics](#)

[Programming](#)

[Assignments](#)

[Co-operation versus](#)

[Dishonesty](#)

[Using Open Source](#)

[Programs](#)

[The Ethics of](#)

[Security](#)

[Not How I Teach It!](#)

[Contacting Me](#)

[Talking to Me](#)

[Class Schedule](#)

[TAs](#)

[Lectures](#)

[Homeworks](#)

[The Homework](#)

[Project](#)

[The CLIC Lab](#)

[Responsibility](#)

[Practical Focus](#)

[What is Security?](#)

- You're all adults
- You're all responsible for your own actions
- If there's something missing, you have to tell me

Introduction

Administrivia

Course Structure

Readings

Logistics

Programming

Assignments

Co-operation versus

Dishonesty

Using Open Source

Programs

The Ethics of

Security

Not How I Teach It!

Contacting Me

Talking to Me

Class Schedule

TAs

Lectures

Homeworks

The Homework

Project

The CLIC Lab

Responsibility

**Practical Focus**

What is Security?

- This is not a pure academic-style security course
- You'll be experimenting with real security holes
- A lot of (in)security is about doing the unexpected
- The ability to “think sideways” is a big advantage

Introduction

Administrivia

**What is Security?**

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is  
About

# What is Security?

# What is Security?

Introduction

Administrivia

What is Security?

**What is Security?**

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is  
About

*Security is keeping unauthorized entities from doing things you don't want them to do.*

This definition is too informal...

# What is Security?

Introduction

Administrivia

What is Security?

What is Security?

**What is Security?**

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is

About

- Confidentiality
- Integrity
- Availability

- Introduction
- Administrivia
- What is Security?
- What is Security?
- What is Security?
- Confidentiality**
- Integrity
- Availability
- They Interact
- More Definitions
- Vulnerabilities
- Threats
- The Human Element
- Engineering
- Designing Security
- What this Course is About

- “The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].” [definitions from RFC 4949]. Not the same as *privacy*.
- **Privacy:** “The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.” Privacy is a reason for confidentiality
- The traditional focus of computer security

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

**Integrity**

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is

About

- **data integrity:** “The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.”
- **system integrity:** “The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.”
- Often of more commercial interest than confidentiality



- “The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.”
- Turning off a computer provides confidentiality and integrity, but hurts availability. . .
- Denial of service attacks are direct assaults on availability

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

**They Interact**

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is  
About

- It's obvious that violations of integrity can be used to compromise confidentiality
- In some situations, violations of availability can be used that way as well

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is  
About

**vulnerability** An error or weakness in the design, implementation, or operation of a system

**attack** A means to exploit some vulnerability in a system

**threat** An adversary that is motivated and capable of exploiting a vulnerability

(Definitions from *Trust in Cyberspace*)

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is

About

- The technical failing in a system
- The primary focus of most computer security classes
- If you can close the vulnerabilities, the threats don't matter
- Or do they?

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

**Threats**

The Human Element

Engineering

Designing Security

What this Course is

About

- Different enemies have different abilities
- Teenage joy-hackers can't crack a modern cryptosystem
- Serious enemies can exploit the “three Bs”: burglary, bribery, and blackmail
- You can't design a security system unless you know who the enemy is

# The Human Element

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

**The Human Element**

Engineering

Designing Security

What this Course is

About

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations.”

*Network Security: Private Communication in a Public World,*  
Kaufman, Perlman, and Speciner

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

**Engineering**

Designing Security

What this Course is

About

- Sometimes, requirements are inconsistent and/or incomplete
- Conflicts:
  - ◆ Security versus cost
  - ◆ Security versus performance
  - ◆ Security versus acceptability and culture
  - ◆ Security versus usability
  - ◆ Security versus security!
- We'll discuss how to detect and analyze such conflicts

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is

About

- The problem is overconstrained
- Among the constraints are cost, human behavior, and ease of operation
- In the real world, realistic security is often far more important than theoretical security
- *What are you trying to protect against whom?*



# What this Course is About

Introduction

Administrivia

What is Security?

What is Security?

What is Security?

Confidentiality

Integrity

Availability

They Interact

More Definitions

Vulnerabilities

Threats

The Human Element

Engineering

Designing Security

What this Course is  
About

- Mechanisms
- Threat analysis
- Security architecture
- Assurance
- In short, *engineering* secure systems