CS 166: *Information Security*

Introduction to Security

Prof. Tom Austin

San José State University

Why should we learn about information security?

Computer Security in the News

Computer Crime for Fun & Profit

Computer virus attacks restaurant's credit card system

Tuesday, January 31, 2012 | Devin Monk | 3

Photo by Devin Monk

Flores Mexican Restaurant of Lakeway manager Isaias Figueroa, left, and co-owner Jose Flores say the restaurant has lost about 15 percent of its business as false rumors circulated after a computer virus recently hacked its credit card system.

Flores Mexican Restaurant of Lakeway is one of the latest institutions attempting to rebuild its reputation after falling victim to a computer virus that attacked its credit card system.

Lakeway police said a few accounts started to trickle in Dec. 5, 2011, from local residents reporting they were the victims of credit card fraud. Within a week, at least 50 individuals filed complaints with the department.

Man nabbed for 'revenge' virus attack

The Yomiuri Shimbun

UTSUNOMIYA--A 44-year-old man from Okayama Prefecture has been arrested on suspicion of sending a computer virus to a server hosting a Web site he had been partially restricted from using, causing the site to crash, police said Wednesday.

It was the first time an arrest has been made for the creation and transmission of a computer virus since the Penal Code was beefed up in July.

Takashi Tomiyama apparently sent a computer virus he created on his home PC to a server hosting a Web site owned and operated by a 38-year-old man in Tochigi Prefecture on Aug. 26, rendering the site's online chat service unusable, they said.

When users attempted to access the chat service screen on the site, the virus caused browser windows to rapidly pop up one after another, potentially causing the browser to crash and overwhelming the PC.

Attackers have gone from pranksters, to professional criminals.

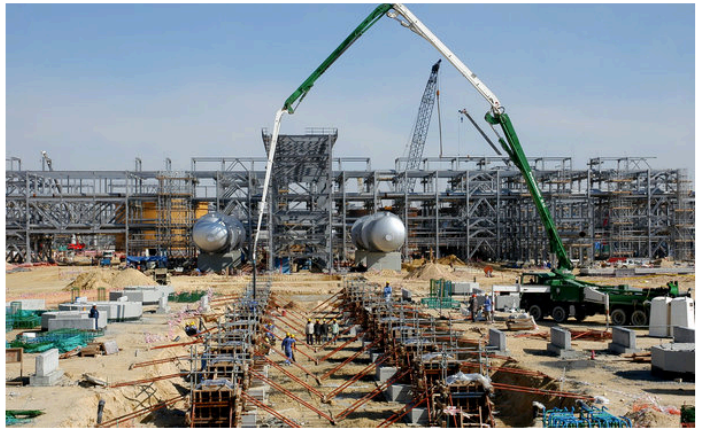
Now Part of Warfare

Iranian President Mahmoud Ahmadinejad, center, visits the Natanz Uranium Enrichment Facility in this file photo. Photograph: Iranian President's Office via AP Images

Bloomberg News

Iran Nuclear Plants Hit By Virus Playing AC/DC, Website Says

In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back



Agence France-Presse/Getty Images

Saudi Aramco's Khurais plant. A cyberattack wiped out data on three-quarters of Aramco's PCs.

By NICOLE PERLROTH
Published: October 23, 2012 | 105 Comments

The hackers picked the one day of the year they knew they could inflict the most damage on the world's most valuable company, Saudi Aramco.

FACEBOOK
TWITTER
GOOGLE+

Nation-states now use cyber-attacks against one another.

The Defenders Are Falling Behind

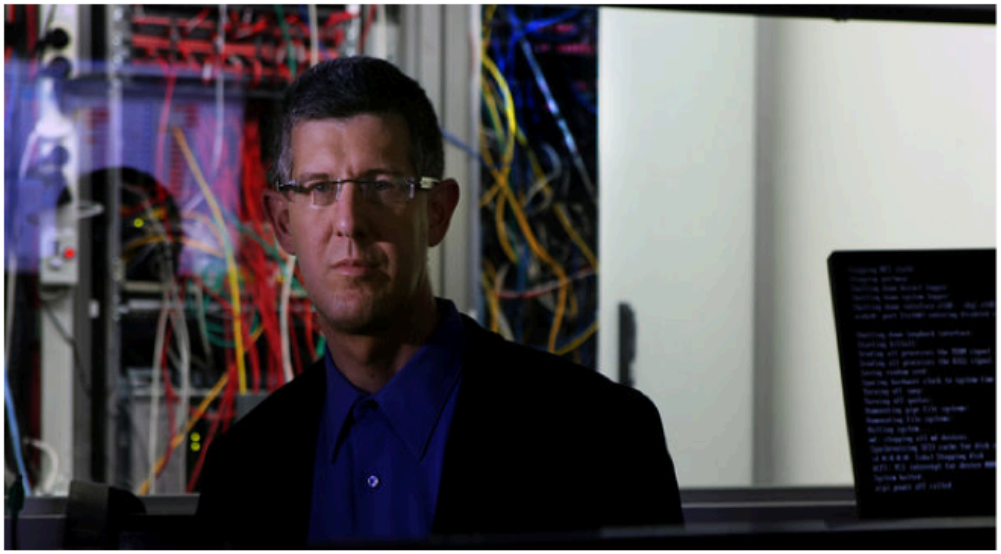
Creating undetectable computer virus 'surprisingly simple'

By Andre Mayer, CBC News Posted: May 30, 2012 3:39 PM ET | Last Updated: May 30, 2012 6:59 PM ET 135

The Flame virus that reportedly hit computers in at least seven Middle Eastern countries has been touted for its s and ability to hide from anti-virus software. (iStock)

Stay Connected with CBC News

Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt



Rina Castelnuovo for The New York Times

Amichai Shulman, the chief technology officer at Imperva. The data security firm recently found that antivirus software programs perform poorly against new viruses.

By NICOLE PERLROTH
Published: December 31, 2012

SAN FRANCISCO — The antivirus industry has a dirty little secret: its products are often not very good at stopping viruses.

FACEBOOK
TWITTER

Administrative Details

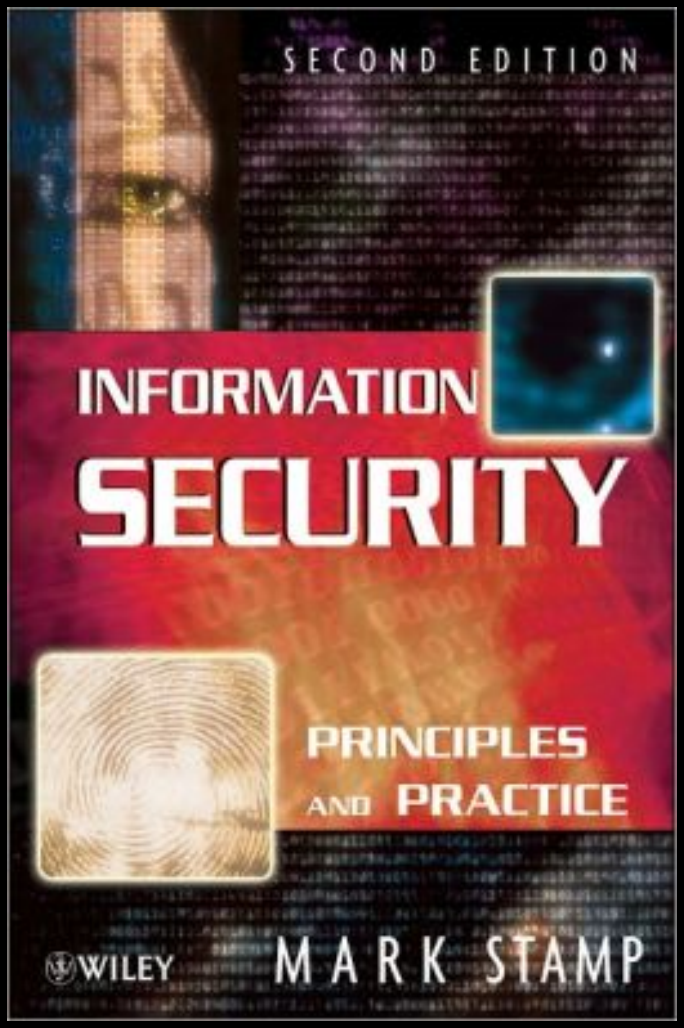
- Green sheet available at http://www.cs.sjsu.edu/~austin/cs166-spring17/greensheet.html
- Homework assignments will be submitted through Canvas (https://sjsu.instructure.com/)
- Academic integrity policy: http://info.sjsu.edu/static/catalog/integrity.html

Homework Schedule

- The homework schedule is available through Canvas
- Late homeworks will not be accepted
- Check the schedule before every class
- Check the schedule before every class
- And finally, CHECK THE SCHEDULE BEFORE EVERY CLASS.

Textbook

Information Security: Principles and Practice, 2nd edition, Mark Stamp, (Wiley, May 2011, ISBN-10: 0470626399, ISBN-13: 978-0470626399).



Grading

- 30%: Homework
- 20%: Test 1
- 20%: Test 2
- 20%: Final exam
  http://info.sjsu.edu/static/policies/final-exam-schedule-fall.html
- 10%: Participation (in-class labs)

Do the homework! If you don't, you won't pass the exams.

Participation: Labs & Drills

- No feedback given (usually)
- I will look at them
- If you have questions, ask me

Homework

- Done *individually*.
- You may *discuss* the assignment with others.
- **Do your own work!**

How to fail yourself and your friend

If two of you turn in similar assignments:

you both get a 0

Office hours

- MacQuarrie Hall room 216.
- Monday/Thursday
  12:00 – 1:00 pm.
- If you need to meet with me another time, email me.

Prerequisites (all with "C-" or better)

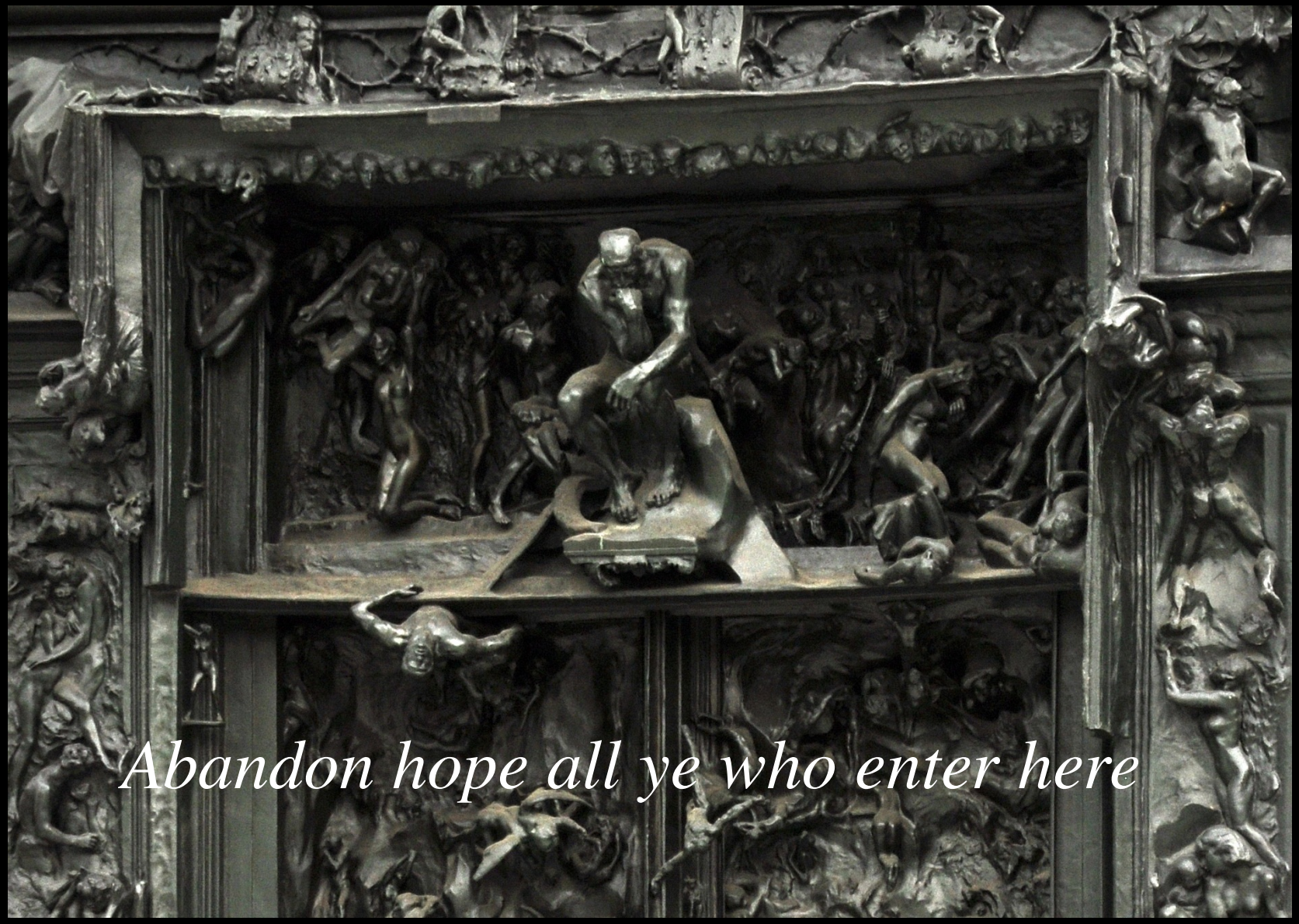
- CS 146: Data Structures & Algorithms
- One of
  - CS 47: Introduction to Computer Organization
  - CMPE 102: Fundamentals of Embedded Software
  - CMPE 120: Computer Organization and Architecture
- **I need to see proof of your prerequisites.**

WARNING!!!!

This class is a lot of work. You will have:

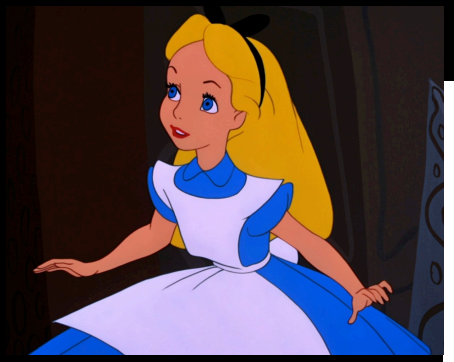
- 3 exams
- Almost weekly homework assignments
- Programming assignments in Java **AND** C
- A moderate of math

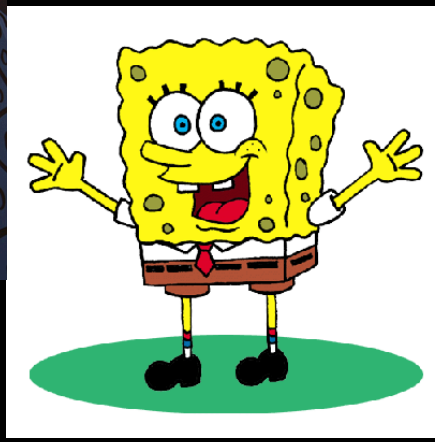
But have fun!



The Cast of Characters

Alice and **Bob:** the traditional "good guys".





The "bad guys" are often Eve and Trudy – the textbook uses **Trudy**.

I get bored with Alice and Bob, so I may use others

Example: Alice's Online Bank

- Alice opens *Alice's Online Bank*
- What are Alice's security concerns?
- What about her customer Bob? What are his security concerns?
- How are these concerns similar? How are they different?
- How does Trudy view the situation?

CIA

The Central Intelligence Agency?

No, though we might mention it from time to time.

CIA

- *Confidentiality*
- *Integrity*
- *Availability*

CIA: Confidentiality

- keeping information secret
- preventing unauthorized "reads"

CIA: Integrity

- defending data from being corrupted
- preventing (or detecting) unauthorized writes

CIA: Availability

- Ensuring that authorized users can use resources
- Preventing denial-of-service (DoS) attacks

Overview of This Course

1. Cryptography
2. Access Control
3. Security Protocols
4. Software
5. Web Security (interwoven)

Cryptography

- The making of "secret codes".
- An important tool in security.
- Just part of the story.

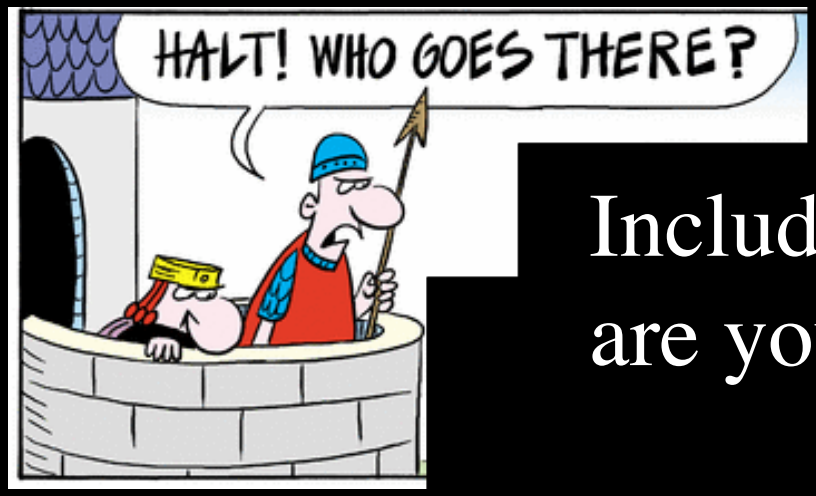
Quote

If you think that cryptography is the answer to your problem then you don't understand cryptography and you don't understand your problem.

--attributed to R. Needham.

Access Control

Umbrella term for security issues related to access of system resources.

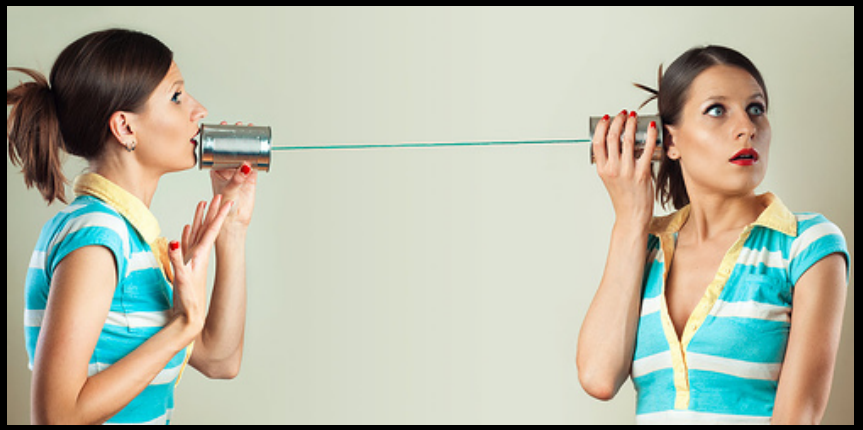


Includes *authentication:*
are you who you say you are?

And *authorization:*
are you allowed to do that?

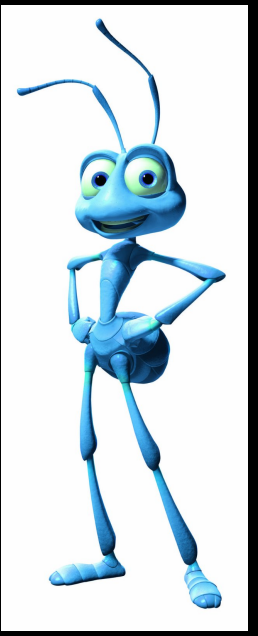
Security Protocols

Communication rules involved in some particular interaction.



Rules must be designed with care, or an attacker might be able to exploit them.

Software



Any large software project has a number of bugs, several of them critical.

To an attacker, bugs are opportunities.

The Weakest Link

A system is only as strong as its weakest point.

Often, the weak point is the user…

The Dancing Pigs Problem

"Given a choice between dancing pigs and security, users will pick dancing pigs every time."

--Edward Felten & Gary McGraw

"While amusing, this is unfair: users are never offered security"

--Mark Pothier

Usable Security

- We can't get rid of the users.
- Security tools can't be overly restrictive.
- Some compromises in security may be required.

Quote

"The only secure computer is one that's unplugged, locked in a safe, and buried 20 feet under the ground in a secret location... and I'm not even too sure about that one"

-- Dennis Huges, FBI.

Passwords

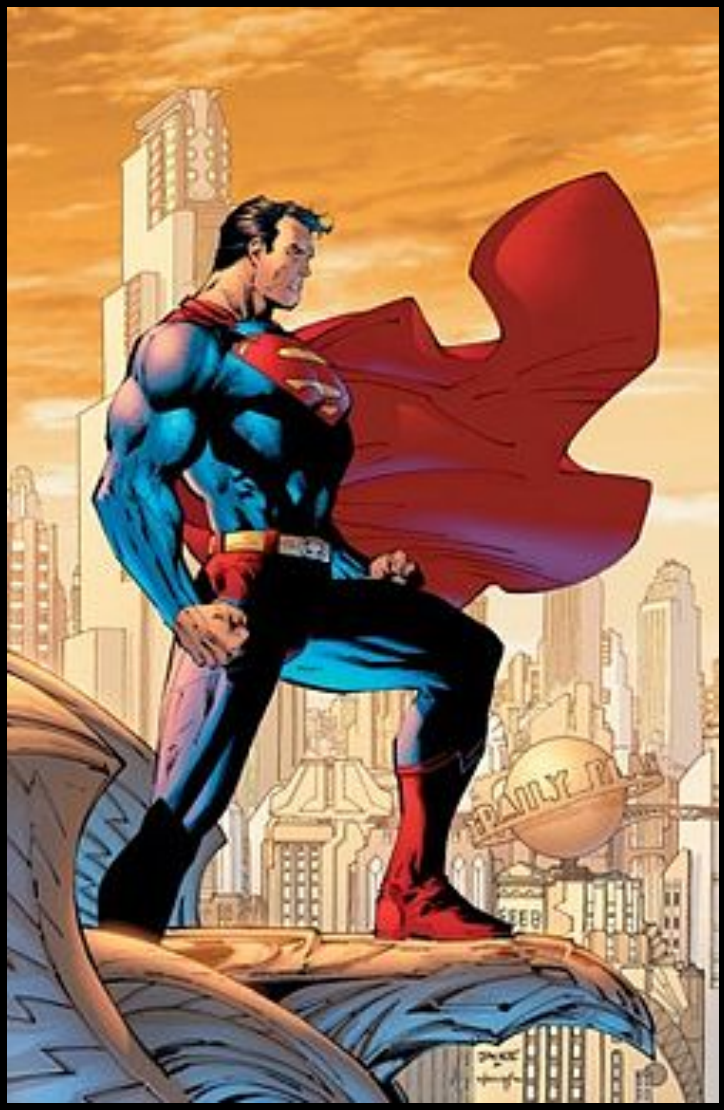
- Passwords are an example of "something you know".
- The most common mode of authentication.
- Opportunities for an attacker?

Password Weaknesses

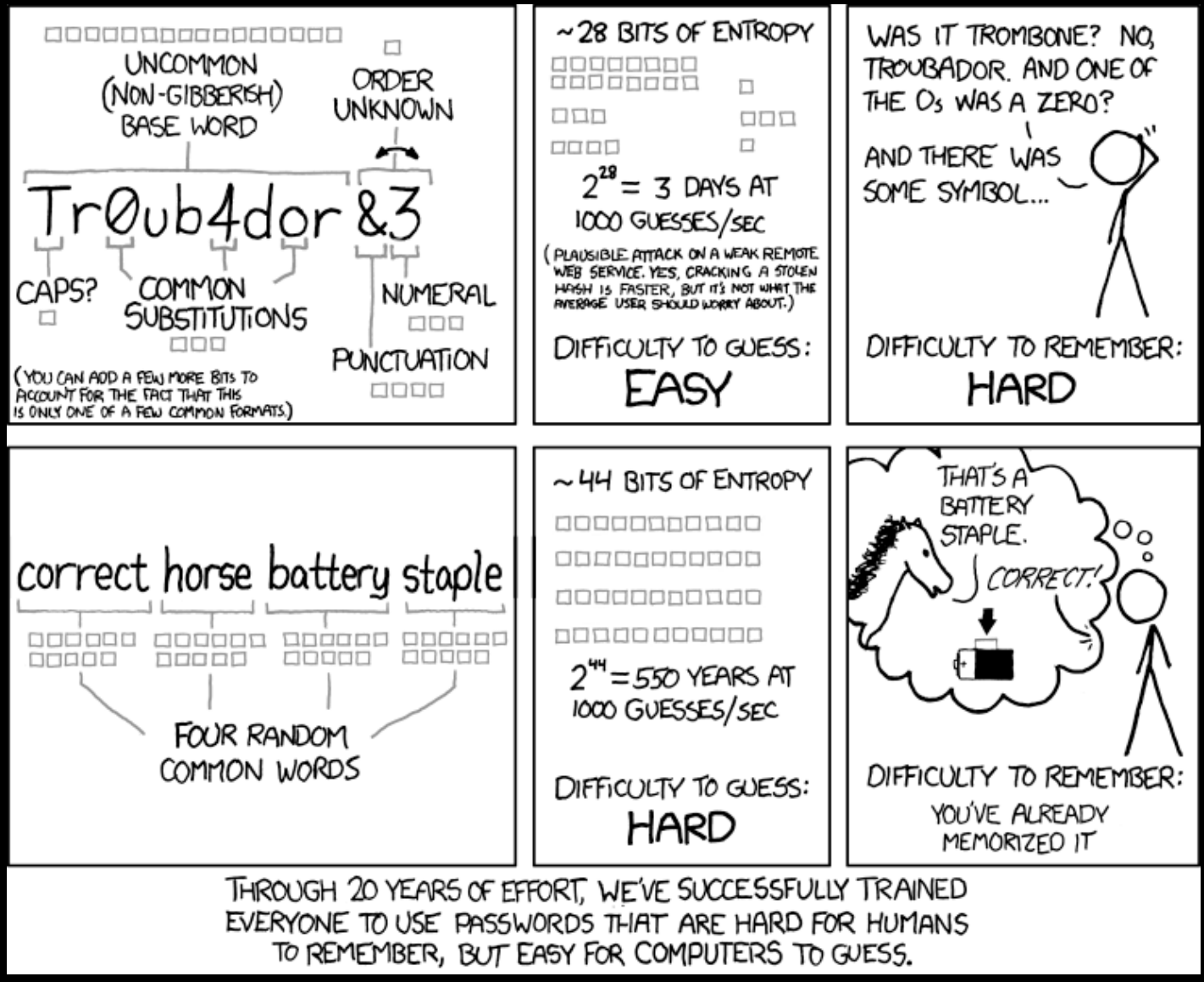
- Users choose poor passwords
- Users forget their passwords
- Site developers do not store passwords securely

Common advice given for passwords

- Do not reuse passwords for different sites
- Passwords should include:
  - mixed case
  - numbers
  - punctuation
- Everyone has heard this advice
- **No one follows it**



"Correct horse battery staple" from http://xkcd.com/936/



Password game

Remember this pass phrase:

spooky hook UFO pathology

Password game

What was the password on the previous slide?

spooky hook UFO pathology

Password game

Now remember this password:

4rx99t3ch!

Password game

What was the password on the previous slide?

4rx99t3ch!

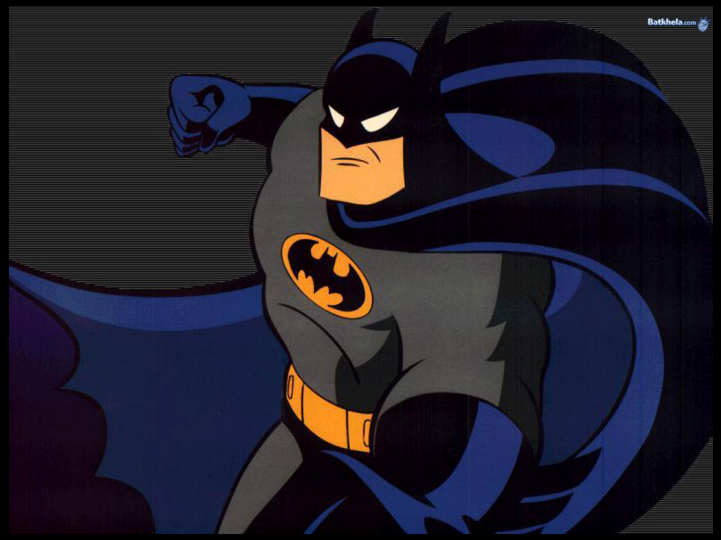
But do you still remember the pass phrase?

spooky hook UFO pathology

The problem

There are ways of choosing strong passwords, but many actual passwords are easily guessed.

Heroes and Villains



Computer security is often taught from the defender's perspective.

In this course, we will consider the defender's and the attacker's perspective.

In Class Exercise: Think Like a Villain

1. Log in to Canvas.
2. Click on "Lab 1".
3. Working in teams of 2-3, try to log in to http://cs31.cs.sjsu.edu/basic_login/.
4. Every **student** should submit his/her own version of the assignment by the end of class.

Some logins you may have discovered

Username	Password
aquaman	fish
guest	guest
admin	admin123
wolverine	harley
superman	superman
wonderwoman	letmein
spiderman	password

Searching for common passwords can be effective, but is time-consuming.

Other vulnerabilities allow information to be stolen more quickly.

We will explore how in future classes.

Homework 1 has been posted

Available in Canvas and at http://www.cs.sjsu.edu/~austin/cs166-fall17/hw/hw1/.