CS 166 – Information Security

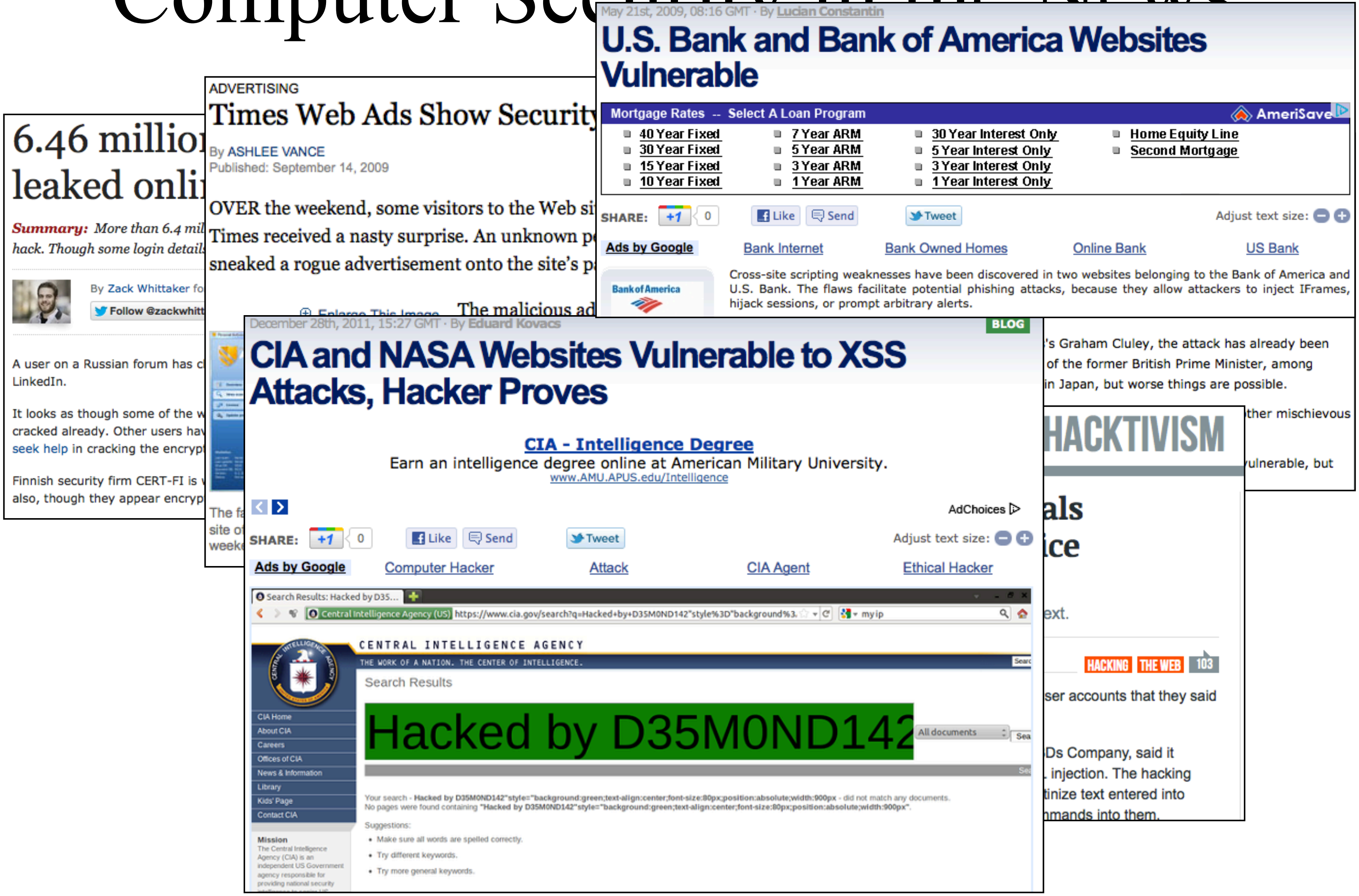
Prof. Tom Austin

San José State University

Spring 2014

Why should we learn about information security?

Computer Security in the News



6.46 millio
leaked onli

Summary: More than 6.4 mil
hack. Though some login detail

By Zack Whittaker fo
Follow @zackwhitt

A user on a Russian forum has c
LinkedIn.

It looks as though some of the w
cracked already. Other users hav
seek help in cracking the encrypt

Finnish security firm CERT-FI is w
also, though they appear encryp

ADVERTISING

Times Web Ads Show Security

By ASHLEE VANCE
Published: September 14, 2009

OVER the weekend, some visitors to the Web si
Times received a nasty surprise. An unknown p
sneaked a rogue advertisement onto the site's p

⊕ Enlarge This Image

The malicious ad

The fa
site of
weeke

May 21st, 2009, 08:16 GMT · By Lucian Constantin

U.S. Bank and Bank of America Websites Vulnerable

Mortgage Rates -- Select A Loan Program — AmeriSave

40 Year Fixed	7 Year ARM	30 Year Interest Only	Home Equity Line
30 Year Fixed	5 Year ARM	5 Year Interest Only	Second Mortgage
15 Year Fixed	3 Year ARM	3 Year Interest Only	
10 Year Fixed	1 Year ARM	1 Year Interest Only	

SHARE: +1 0 Like Send Tweet Adjust text size:

Ads by Google Bank Internet Bank Owned Homes Online Bank US Bank

Bank of America

Cross-site scripting weaknesses have been discovered in two websites belonging to the Bank of America and U.S. Bank. The flaws facilitate potential phishing attacks, because they allow attackers to inject IFrames, hijack sessions, or prompt arbitrary alerts.

's Graham Cluley, the attack has already been
of the former British Prime Minister, among
in Japan, but worse things are possible.

ther mischievous

ulnerable, but

December 28th, 2011, 15:27 GMT · By Eduard Kovacs BLOG

CIA and NASA Websites Vulnerable to XSS Attacks, Hacker Proves

CIA - Intelligence Degree
Earn an intelligence degree online at American Military University.
www.AMU.APUS.edu/Intelligence

AdChoices

SHARE: +1 0 Like Send Tweet Adjust text size:

Ads by Google Computer Hacker Attack CIA Agent Ethical Hacker

Search Results: Hacked by D35...
Central Intelligence Agency (US)
https://www.cia.gov/search?q=Hacked+by+D35M0ND142"style%3D"background%3.
myip

CENTRAL INTELLIGENCE AGENCY
THE WORK OF A NATION. THE CENTER OF INTELLIGENCE.

CIA Home
About CIA
Careers
Offices of CIA
News & Information
Library
Kids' Page
Contact CIA

Search Results

Hacked by D35M0ND142

All documents

Your search - Hacked by D35M0ND142"style="background:green;text-align:center;font-size:80px;position:absolute;width:900px - did not match any documents.
No pages were found containing "Hacked by D35M0ND142"style="background:green;text-align:center;font-size:80px;position:absolute;width:900px".

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.

Mission
The Central Intelligence Agency (CIA) is an independent US Government agency responsible for providing national security

HACKTIVISM

als
ice

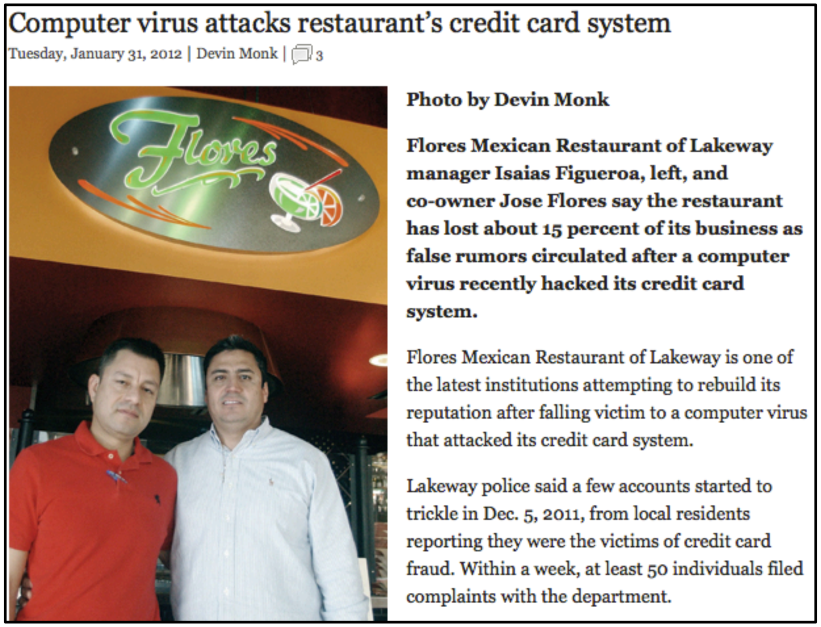
ext.

HACKING THE WEB 103

ser accounts that they said

Ds Company, said it
. injection. The hacking
tinize text entered into
mmands into them.

Computer Crime for Fun & Profit



Computer virus attacks restaurant's credit card system

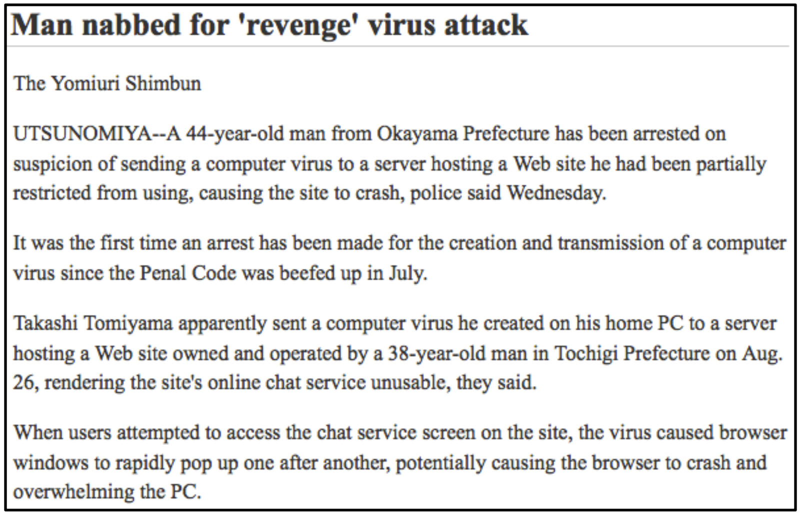
Tuesday, January 31, 2012 | Devin Monk | 3

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.

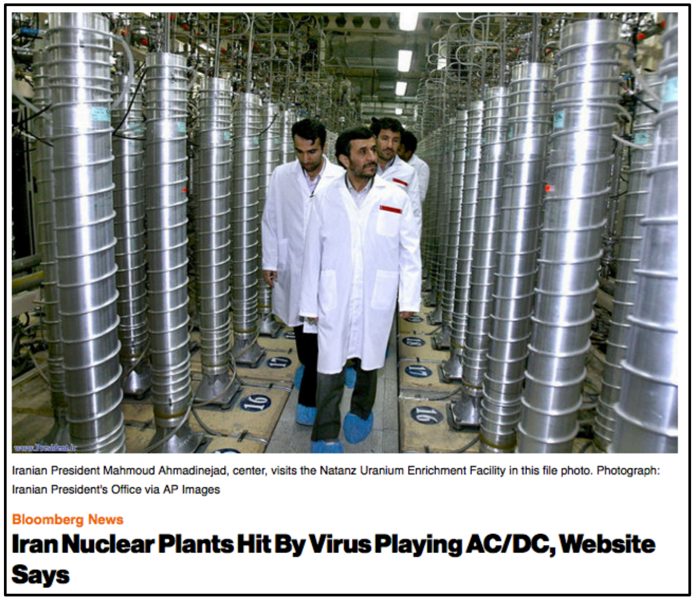
It was the first time an arrest has been made for the creation and transmission of a computer virus since the Penal Code was beefed up in July.

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.

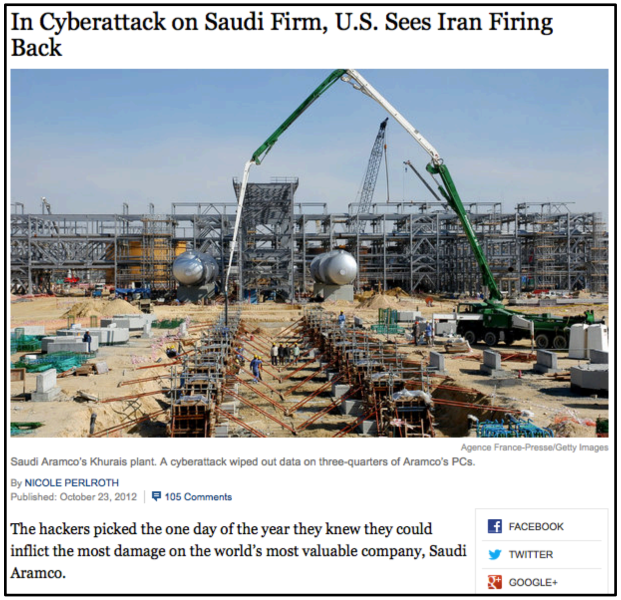
Now Part of Warfare



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.

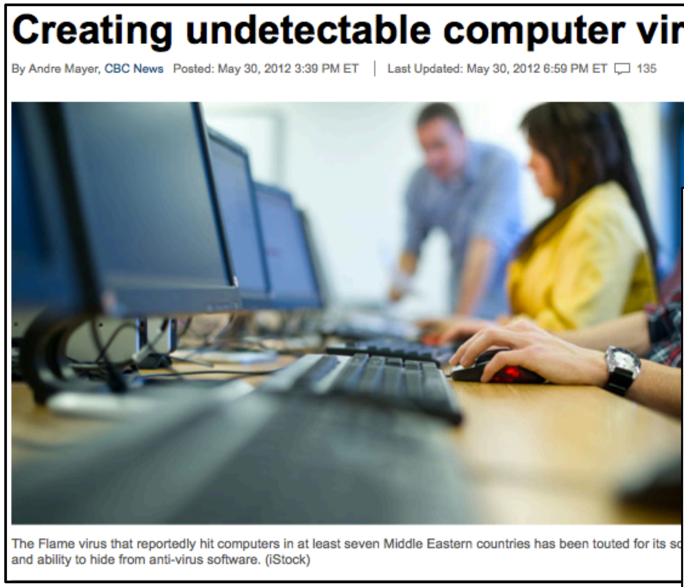
By NICOLE PERLROTH

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.

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

The Defenders Are Falling Behind

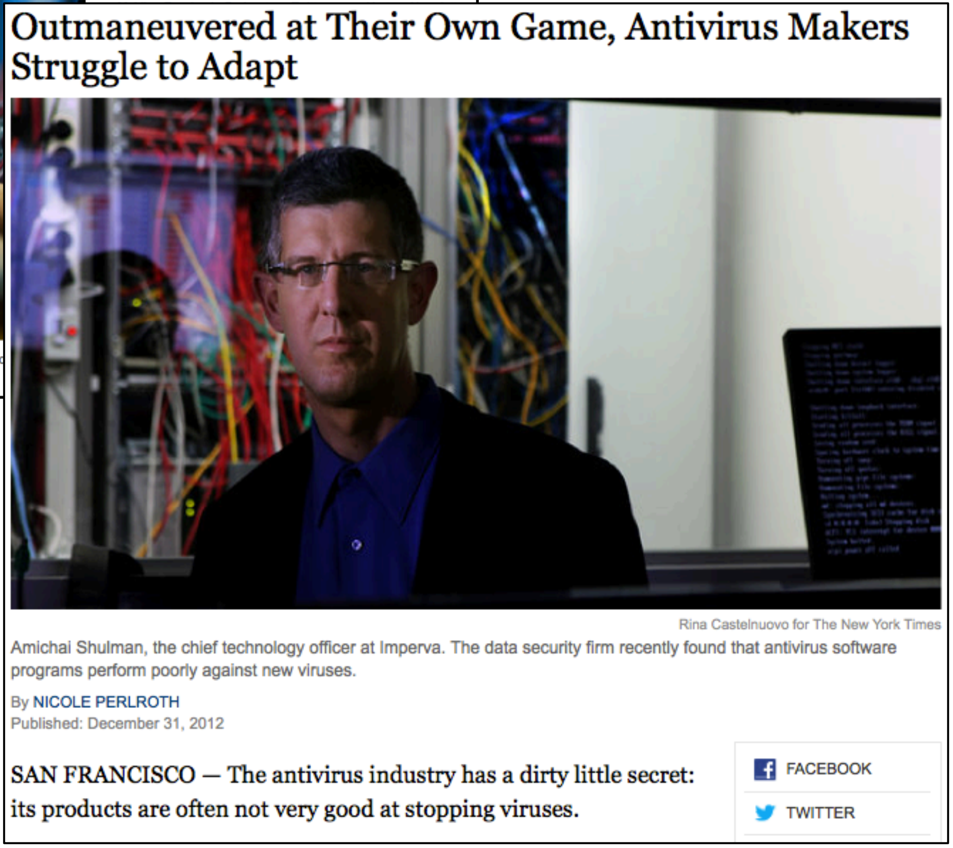


Creating undetectable computer virus 'surprisingly simple'

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

Stay Connected with CBC News

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)



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.

Administrative Details

- Green sheet available at http://cs.sjsu.edu/~austin/cs166-spring14/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

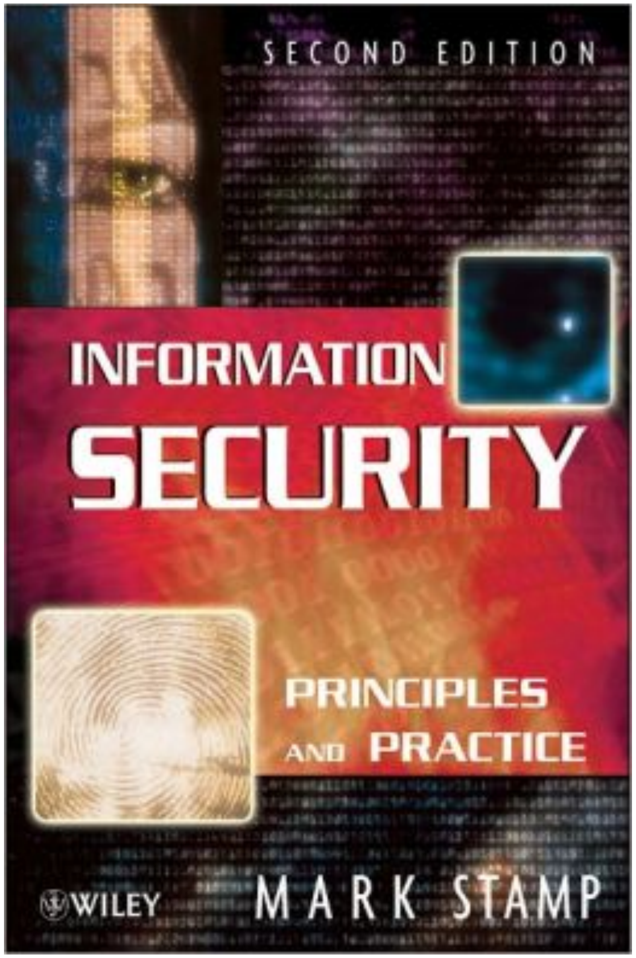
- The homework schedule is available through Canvas
- Late homeworks will not be accepted
- Check the schedule before every class
- Check the schedule before every class
- And finally, CHECK THE SCHEDULE BEFORE EVERY CLASS.

Textbook

Information Security: Principles and Practice,

2nd edition, Mark Stamp, (Wiley, May 2011,

ISBN-10: 0470626399, ISBN-13: 978-0470626399).



Grading

- 120 points: Homework
- 100 points: Test 1
- 100 points: Test 2
- 120 points: Final exam http://info.sjsu.edu/static/catalog/final-exam-schedule-spring.html
- 40 points: Participation (in-class labs)

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

Office hours

- MacQuarrie Hall room 216.
- Monday 10:30 – 11:30 am.
- Tuesday noon – 1 pm.
- If you need to meet with me another time, send me an email.

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:

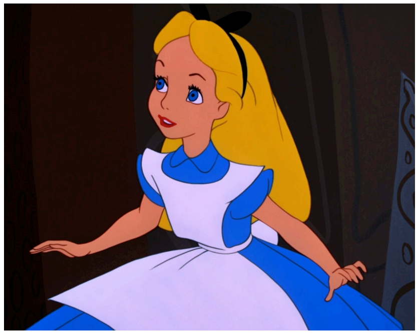
- 3 exams
- Almost weekly homework assignments
- Programming assignments in Java **AND** C
- A moderate of math (big O notation, high school algebra, etc)

But have fun!

Abandon hope all ye who enter here

The Cast of Characters

In security literature, **Alice** and **Bob** are the traditional "good guys".



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

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

Alice’s Online Bank

- Alice opens *Alice’s Online Bank*
- What are Alice’s security concerns?
- If Bob is a customer of the bank, what are his security concerns?
- How are Alice’s and Bob’s concerns similar? How are they different?
- How does Trudy view the situation?

CIA

This CIA?

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

CIA

- *Confidentiality:*
  - keeping information secret
  - preventing unauthorized "reads"
- *Integrity:*
  - defending data from being corrupted
  - preventing (or detecting) unauthorized writes
- *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, but just part of the story.
- *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

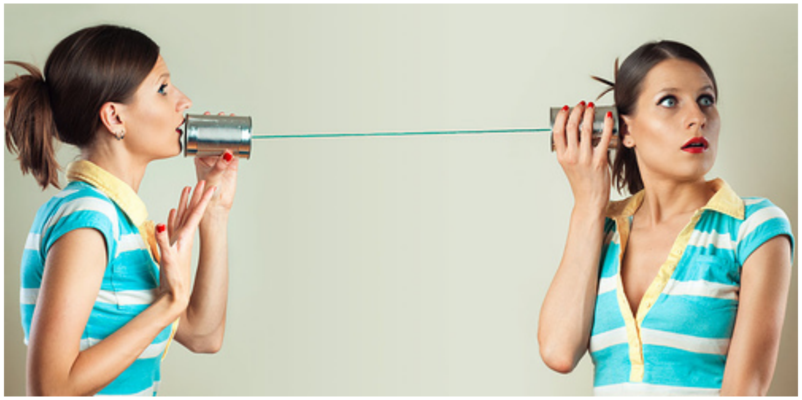
This umbrella term refers to security issues related to access of system resources.

One of the primary areas of interest is *authentication:* are you who you say you are?

Another is *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 is almost guaranteed to have 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

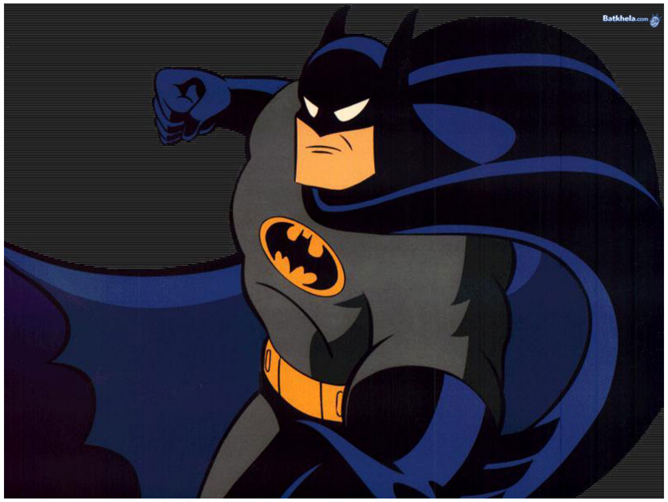
"While amusing, this is unfair: users are never offered security"

--Mark Pothier

We can't get rid of the users.
They are the whole point.
We need to design **usable** security.

"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.

Heroes and Villains



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

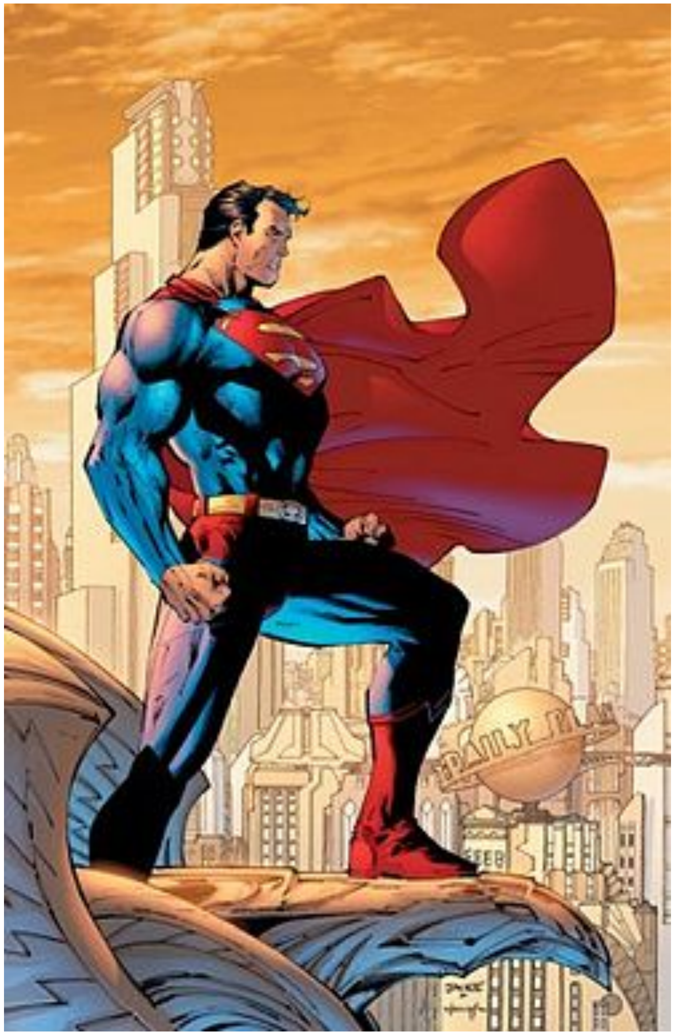
In this course, we will consider the defender's and the attacker's perspective.

Passwords

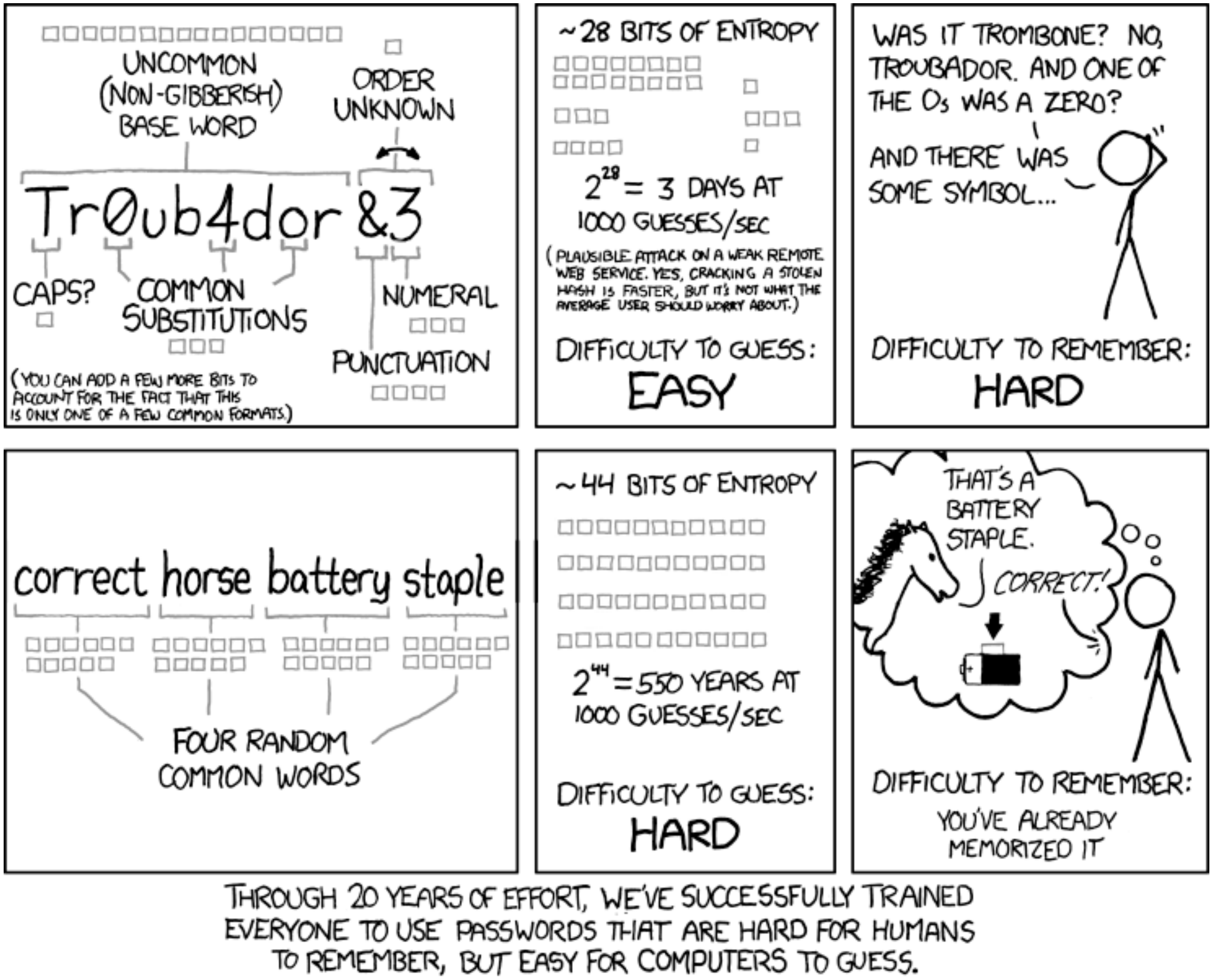
- Passwords are an example of "something you know", and the most common mode of authentication.
- Opportunities for an attacker:
  - Users choose poor passwords
  - Site developers do not store passwords securely

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/


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

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.

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 the website listed in your assignment description.
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://cs.sjsu.edu/~austin/cs166-spring14/hw1/.