Logistics

Assignment 2 posted

- Posted, due Thu 10/27 11:59pm
- Discuss briefly later today

Assignment 1 grades
Grading commencing, will finish by next week sometime

Midterm Grades
Will post next week, advisory only

Reading

- For today:
  - Online Readings (FB and Honan Hacks, secure passwords)
  - Quinn Ch 7 on Security + Interview with Matt Bishop

- Next week: Quinn Ch 5 on Privacy
## Accountability Results

### (S)afe/(R)isky/(H)igh/(L)ow : Stars

<table>
<thead>
<tr>
<th>Sec/Suit</th>
<th>S</th>
<th>C</th>
<th>D</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue 001</td>
<td>S:0</td>
<td>H:0</td>
<td>R:1*</td>
<td>H:1*</td>
</tr>
<tr>
<td>Tue 003</td>
<td>R:1*</td>
<td>H:1*</td>
<td>R:1*</td>
<td>H:1*</td>
</tr>
<tr>
<td>Thu 002</td>
<td>R:2</td>
<td>H:2</td>
<td>R:2</td>
<td>H:2</td>
</tr>
<tr>
<td>Thu 007</td>
<td>R:0</td>
<td>L:0</td>
<td>R:0</td>
<td>H:0</td>
</tr>
</tbody>
</table>

### Comments

- Stressful, made me nervous
- Let us pick groups
- Weren’t sure how detailed the questions were going to be
- Like HW: never enough time
- There is no perfect knowledge
- Didn’t want to insult those that weren’t taking notes
- Seemed dumb at first, but now seems relevant
- Forcing ppl to read is good
- Mis-communication can cause bad problems
- Experienced work time crunches
- Real world more than 1 person responsible for stuff
- Repercussions for failure should be worse
- Only as strong as weakest link / element of luck
An Amusement

- Trivia or Cheating?
- Definitely Cheating
Goals

Basic computer security

- How the Internet works
- Identifying fraudulent sites/messages
- Good passwords
- Sensible practices
- A short video on security
The Internet

Don’t have wires between our machine and every other machine out there

- How do we communicate with so many others?
- What security risks does this create?
- How do we get around the problem of no shared secrets?
I needed an example of a phishing email.

good day chris. candice explained me this web page --> socialipad3 . com <<<-- is giving away an ipad three to people which are usually at face book for free...almost all these people need is your own opinion about it and u can keep it forever. however u should hurry up just before they close it

See also Department of Grants
Spot the Differences

http://en.wikipedia.org/wiki/File:Spot_the_difference.png

How about this versus that
Today’s Reading

Textbook topics
- Types of Attacks
- Notable Instances
- Dilemmas

Online readings
- Various notable hacks
- Picking passwords
- Identifying Scams
Both Facebook and Twitter were breached through a well-publicized vulnerability in Oracle’s Java software. The number of attacks reported by government agencies last year topped 48,500 — a ninefold jump from the 5,500 attacks reported in 2006...

In the last month alone, The New York Times, The Wall Street Journal and The Washington Post all confirmed that they were targets of sophisticated hackers. But security experts say that these attacks are just the tip of the iceberg.

A common saying among security experts is that there are now only two types of American companies: Those that have been hacked and those that don’t know they’ve been hacked.

– "Facebook Says Hackers Breached Its Computers", Nicole Perlroth and Nick Bilton, NYT 2/15/2013, Source
Irregularities

I was playing with my daughter when my iPhone suddenly powered down... It then rebooted to the setup screen... My phone automatically backs up every night. I just assumed it would be a pain in the ass, and nothing more. I entered my iCloud login to restore, and it wasn’t accepted. Again, I was irritated, but not alarmed. I went to connect the iPhone to my computer and restore from that backup — which I had just happened to do the other day. When I opened my laptop, an iCal message popped up telling me that my Gmail account information was wrong. Then the screen went gray, and asked for a four-digit PIN. I didn’t have a four-digit PIN... For the first time it occurred to me that I was being hacked.

– Mat Honan, How Apple and Amazon Security Flaws Led to My Epic Hacking (Wired Magazine)
Accountability the Hard Way

Mat Honan:

▶ My accounts were daisy-chained together.
▶ Had I been regularly backing up the data on my MacBook, I wouldn’t have had to worry about losing more than a year’s worth of photos, covering the entire lifespan of my daughter.
▶ Had I used two-factor authentication for my Google account, it’s possible that none of this would have happened.
▶ Remote wipe is dangerous for laptops
▶ Those security lapses are my fault, and I deeply, deeply regret them.
Assignment 2

Use this as an opportunity to beef up your security

- Improve 2 things about your computing systems
- Examples: Password login, locked phone, back-ups, anti-virus, firewall, encrypt files, encrypt hard drive, setup a password manager, encrypt e-mail, etc.
- Analyze why companies don’t provide software like this by default
Picking a Good Password

- Simplest way you can trivially increase security
- Trouble: Required to make frequent changes
  - Makes remembering harder
  - GMU: change every 180 days
  - Compliance with some Virginia State Mandate but can’t seem to find where it is written
- \textbf{Never reveal your password to anyone}
- GMU: Passwords are kept encrypted in a secure location and cannot be looked up by anyone (not even the ITU Support Center). (more info)
Attacking Passwords

### Input
- Fox
- The red fox jumps over the blue dog

### Digest
- DFCD 3454 BBEA 788A 751A 696C 2D9 7009 CA99 2D17
- 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABE
- 8F88 7558 7851 4F32 D1C6 76B1 70A9 0DA4 AEFE 4819

<table>
<thead>
<tr>
<th>id</th>
<th>username</th>
<th>password</th>
<th>passwordHint</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>admin</td>
<td>645E2A7B0C1F4D45EF859725386B605D</td>
<td>k3wl dud</td>
</tr>
<tr>
<td>2</td>
<td>pumpkin22</td>
<td>614B1F421A1F52727FF72A13CAC74F56</td>
<td>my favorite holiday</td>
</tr>
<tr>
<td>3</td>
<td>johndoe</td>
<td>8598500975B68DD9F2616A2B1A471F4E</td>
<td>Freddie Mercury’s band</td>
</tr>
<tr>
<td>4</td>
<td>alexa45</td>
<td>14BC2B3E56370B1FF4B8EFFC5DA13226</td>
<td>password</td>
</tr>
<tr>
<td>5</td>
<td>guy</td>
<td>7BB9FE4E6292A5D7CCD749755BC6B593</td>
<td>NULL</td>
</tr>
<tr>
<td>6</td>
<td>maryjane</td>
<td>8598500975B68DD9F2616A2B1A471F4E</td>
<td>I'm one!</td>
</tr>
<tr>
<td>7</td>
<td>dudson123</td>
<td>614B1F421A1F52727FF72A13CAC74F56</td>
<td>scary movie!</td>
</tr>
</tbody>
</table>
Password Selection Methods

General Guidelines
Never include personal info that can be looked up
▶ Your name, family names, birthdays, favorites, car you drive
▶ Anything on FB is a bad idea
▶ Any single dictionary word...

Two Methods
You have to remember the password; here are two methods
▶ OK: Sentence Method
  ▶ Traditional method of picking hard passwords
  ▶ Inferior to...
▶ Awesome: CorrectHorseBatteryStaple Method
  ▶ Picking a password that’s easy to remember and hard to crack

Participation
Try both of these; which one do you prefer?
Open Debate: White Hat Hackers ≡ Whistleblowers?

I BROKE INTO THE WEB SITE TO HELP YOU!

THANKS, BUT IT'S BETTER IF WE DON'T KNOW THE SITE IS INSECURE.
Now the Ethical Question

Is reporting on security holes unethical?

Mat Honan Article describes how to penetrate Apple account

[The hack is] so easy that Wired was able to duplicate the exploit twice in minutes.

Eric Butler Produced Firesheep a tool for sidejacking

The attack that Firesheep demonstrates is easy to do using tools that have been available for years.
For Next Week

- Privacy: Quinn Ch. 5 (all) (privacy)