Quick Reminder

- Online Notes – Do Your Part.

- I will tally student contributions in one week (currently 4 out of 54)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture and Online Notes</td>
<td>5 %</td>
</tr>
<tr>
<td>Recitation Participation</td>
<td>5 %</td>
</tr>
<tr>
<td>Recitation Exercices / Homeworks</td>
<td>10 %</td>
</tr>
<tr>
<td>Quizzes</td>
<td>15 %</td>
</tr>
<tr>
<td>Projects</td>
<td>30 %</td>
</tr>
<tr>
<td>Midterms</td>
<td>20 %</td>
</tr>
<tr>
<td>Final Exam</td>
<td>15 %</td>
</tr>
</tbody>
</table>
Essentials of Authentication

- Something you know
  - Name of high school, ...
  - Password
- Something you have
  - Dongle
- Something you are
  - Biometrics: Fingerprint, Face, Iris, ...
Something you Know
Often a password

- We’ve covered passwords
  - Minor note – textbook example
    - Good, example of asking database without ever letting password info leave the database
    - Bad, actually suggests passwords stored in database rather than hashed passwords.

- Beyond just webdev, consider ..
  - How do you manage passwords,
  - How do ‘most people’ handle them.
Most Popular Passwords

Arstechnica Story:
Internet users ditch “password” as password, upgrade to “123456
By Jon Brodkin - Jan 20, 2014

Before we go, here is SplashData’s list of the top 25 most common passwords in 2013:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Change from 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>Up 1</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td>Down 1</td>
</tr>
<tr>
<td>3</td>
<td>12345678</td>
<td>Unchanged</td>
</tr>
<tr>
<td>4</td>
<td>qwerty</td>
<td>Up 1</td>
</tr>
<tr>
<td>5</td>
<td>abc123</td>
<td>Down 1</td>
</tr>
<tr>
<td>6</td>
<td>123456789</td>
<td>New</td>
</tr>
<tr>
<td>7</td>
<td>111111</td>
<td>Up 2</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>Up 5</td>
</tr>
<tr>
<td>9</td>
<td>iloveyou</td>
<td>Up 2</td>
</tr>
<tr>
<td>10</td>
<td>adobe123</td>
<td>New</td>
</tr>
<tr>
<td>11</td>
<td>123123</td>
<td>Up 5</td>
</tr>
<tr>
<td>12</td>
<td>admin</td>
<td>New</td>
</tr>
<tr>
<td>13</td>
<td>1234567890</td>
<td>New</td>
</tr>
<tr>
<td>14</td>
<td>letmein</td>
<td>Down 7</td>
</tr>
<tr>
<td>15</td>
<td>photoshop</td>
<td>New</td>
</tr>
<tr>
<td>16</td>
<td>1234</td>
<td>New</td>
</tr>
<tr>
<td>17</td>
<td>monkey</td>
<td>Down 11</td>
</tr>
</tbody>
</table>
Strategy #1: Entropy

Truly minimize the ‘Odds of guessing’.

But there is a big problem! No human will remember such a password and so it MUST be recorded.
Use a Sentence: Strategy #2

Bruce Schneier's Method

Security expert Bruce Schneier put forth a password method back in 2008 that he still recommends today. It works like this: Take a sentence and turn it into a password.

- Provided your sentence is not “See Spot Sit” odds are in your favor that others have not gone down the same path.

Summary from: Four Methods to Create a Secure Password You’ll Actually Remember, by Kevan Lee.
Original post by Bruce Schneier on BoingBoing: Choosing a Secure Password
Select an image of an interesting place (Mount Rushmore). Select a photo of a familiar or famous person (Beyonce). Imagine some random action along with a random object (Beyonce driving a Jello mold at Mount Rushmore).

Think of a Person, an Action and an Object. Put them together in a story.

Taps into our innate ability to recall stories, particularly funny or absurd stories.

Another Thing: Pass The Salt

- Here is a challenge.
- Below is the md5 of a salted password.
- Email the instructor the original password and/or the salt.

<salt>::<password>

33a27522874215779a0ff1704589e892
FYI – This is Harder

Consider: What if you knew the salt?
Another Crack at It

FYI – This one also fails (2/26/2017)

MD5 Online

View Our Free Demo
Make Hiring Easier, Faster & Cost-effective.
www.cirns.com/RecruitingSoftware

MD5 Decrypter

Enter your MD5 hash here and cross your fingers:

33e27522674215779a0ff1704589e892

Captcha:
Security Questions
Mothers Maiden Name?

- Another entire class of information
  - Things you know without effort, and
  - presumably an attacker does not.

- But!
  - This information leaks
  - Pervasive use defeats the purpose.

- Take-home message for CT 310
  - Don’t create sites reliant on such info.
Something you Have

- This is not such a new idea ...
  - Do you have a key in your pocket?
- It can take on many forms.
- Tokens for example ...

Image from TokenGuard.com website
Have a Cell Phone?

- No extra equipment – just software.
- Major website use increasing.
- Example, RSA
- Example, Google is now using SMS
Oops, Things Change Fast

- Vulnerable to interception?

Schneier on Security

NIST is No Longer Recommending Two-Factor Authentication Using SMS

NIST is no longer recommending two-factor authentication systems that use SMS, because of their many insecurities. In the latest draft of its Digital Authentication Guideline, there's the line:

[Out of band verification] using SMS is deprecated, and will no longer be allowed in future releases of this guidance.

Tags: authentication, NIST, SMS, two-factor authentication

Posted on August 3, 2016 at 7:11 AM • 60 Comments
Have Email?

- Explosion in use of email accounts as ‘Something that you have’.
- Why is this so common ...

---

Conference Management Toolkit <cmt@microsoft.com>
To: Ross Beveridge
Reply-To: cmt@microsoft.com
CMT Password Assistance

March 28, 2013 12:52 PM
Hide Details 3

Dear Ross Beveridge,

A new password was requested for your account ross@cs.colostate.edu for https://cmt.research.microsoft.com/ICCV2013

Your new password is [HIDDEN]

For security reasons, please log into https://cmt.research.microsoft.com/ICCV2013 and change the password immediately using the “Change Password” link from the drop-down menu next to your name on the upper right side of any page.

If you have any questions, please send email to cmt@microsoft.com

Regards,

CMT Support Team
Something You Are

- Some measurable personal trait.
- Should be (mostly) unique.
- Common Examples:
  - Fingerprints, Voice, Hand Shape,
  - Iris, Face, Palm Scan, ...
- Good, nothing to loose or forget,
- But, how reliable!
Iris Recognition

➢ Still fairly intrusive, but very useful.
Face Recognition

- Our own homegrown example.
- Demonstration released in 2009
- Face Recognition is Unobtrusive.
Going to Market

Stop trading privacy & security for convenience.


Hoyos Labs is the global leader in mobile biometrics authentication, protecting the identity and data of customers and enterprises all from the palm of their hands, defending the industry and
... and of course ...

Image From How Touch ID works: Making sense of Apple’s fingerprint identity sensor, Rene Ritchie, iMore, September 14, 2013
Multifactor Authentication

- All one’s eggs in one basket:
  - Passwords can be weak, stolen ...
  - Tokens and keys can be lost,
  - Not all fingerprints easily read, ...

- Backups are usually a good idea
  - Two factor authentication is starting to become common on some areas.

- Already common: Bank card and PIN
Mistakes come in many forms. The following is not to pick on one company, but to highlight how easily security/authentication issues can come off the rails. Quoting Steve Gibson from Security Now 373 on October 10 2012:

Well, a security company, ElcomSoft, just noted back in August that there was a problem with UPEK's (fingerprint) software because, when you're setting it up and giving it the ability to log you into Windows, you need to give it your credentials. Now, the assumption is - and unfortunately that turns out to have been all it is - is that they would do something secure with those credentials. Turns out they're stored in the registry, not very well encrypted.

Here is the link to the transcript
http://www.grc.com/sn/sn-373.txt
Next Issue: Users

Have requested permission on 2/18/16 from Mike Wagganer http://www.mikewagganer.com
Using according to educational fair use pending reply from artist.
On the Internet, nobody knows you're a dog

"On the Internet, nobody knows you're a dog" is an adage which began as a cartoon caption by Peter Steiner and published by The New Yorker on July 5, 1993.[1][2] The cartoon features two dogs: one sitting on a chair in front of a computer, speaking the caption to a second dog sitting on the floor.[3] As of 2011, the panel was the most reproduced cartoon from The New Yorker, and Steiner has earned over US$50,000 from its reprinting.[1][4][5]
Who Can Have an Account?

- Does your site offer accounts to new users without human-in-the-loop screening?
  - Yes: your site is size limited.
  - No: does your site include dogs (bots).

- You are all therefore familiar with the next technology (Gotcha!)
Related Question

Are you a human being (prove it!)

CAPTCHA: Telling Humans and Computers Apart Automatically

A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text as the one shown below, but current computer programs can’t:

Type the two words:

The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University.
Still Relevant

What is reCAPTCHA?

Easy to add, advanced security

reCAPTCHA is a free service that protects your site from spam and abuse. It uses advanced risk analysis techniques to tell humans and bots apart. With the new API, a significant number of your valid human users will pass the reCAPTCHA challenge without having to solve a CAPTCHA. reCAPTCHA comes in the form of a widget that you can easily add to your blog, forum, registration form, etc.

GET STARTED

Powered by machine learning
Key Idea – Chain of Trust

- SSL trust certification authority.
- Trust user controls cell phone.
- Trust user has control of email.
- Trust user from known IP address.
- Trust person A endorses person B.
- ...
Learn to Inspect Certs

Safari is using an encrypted connection to www.cs.colostate.edu.

Encryption with a digital certificate keeps information private as it's sent to or from the HTTPS website www.cs.colostate.edu.

www.cs.colostate.edu
Issued by: InCommon RSA Server CA
Expires: Saturday, January 12, 2019 at 4:50:59 PM Mountain Standard Time

- Trust
- Details

Hide Certificate