Fun With Research

Bill Cheswick
AT&T Labs - Research
ches@research.att.com
Outline

• A bio and some personal “wisdom”
• The differential equations of love
• Mr. Thumbnail
Outline

• A bio and some personal “wisdom”
• Rethinking Passwords (a current stump speech, but with a little research in it)
• Mr. Thumbnail
Rethinking Passwords

Bill Cheswick
AT&T Labs - Research
ches@research.att.com
OAG password rules

* The password must be at least seven characters long and cannot exceed fifty characters.
* The password is case sensitive and must include at least one letter and one numeric digit.
* The password may include punctuation characters but cannot contain spaces or single or double apostrophes.
* The password must be in Roman characters
World of Warcraft
Wizard Rules

* Your Account Password must contain at least one numeric character and one alphabetic character.
* It must differ from your Account Name.
* It must be between eight and sixteen characters in length.
* It may only contain alphanumeric characters and punctuation such as A-Z, 0-9, or !"#$%. 
United Airlines rules

Passwords may be any combination of six (6) characters and are case insensitive.

Your password will grant you access to united.com, as well as other United features such as our wireless flight paging service, EasyAccess.

For security, certain passwords, such as "united" and "password" are not allowed.

Passwords are case insensitive; please remember how it is entered.
Minimum password length is six (6) characters and must include characters from at least two (2) of these groups: alpha, number, and special characters.
New Password: **************
Verify Password: **************
Secret Question: - Select Secret Question -
Secret Question Answer: 

* New Password must be minimum 7 alpha/numeric characters. 
* New Password must contain at least 1 numeric symbol. 
* Answer to Secret Question needs to be from 2 to 32 characters.
Passphrase Rules:

It must be a minimum of 4 words separated by blanks, at least 1 word must be 5 characters or longer.

It is case sensitive and cannot be less than 11 characters or more than 50 characters long including blanks.

It cannot contain single quotes, double quotes or ascii newline characters.

It cannot contain 3 or more consecutive identical characters.

You may NOT reuse any of the last 6 previously used passphrases.
• The password may not contain your user name.
• The password must contain a minimum of six characters although eight characters are recommended since future complexity parameters will require an eight-character minimum.
• The password must contain three of the following characteristics:
  ◦ Uppercase alphabet characters (AZ)
  ◦ Lowercase alphabet characters (az)
  ◦ Arabic numerals (09)
  ◦ Non-alphanumeric characters (for example, !,$,#,%)

Thursday, July 30, 2009
- Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character. Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password.
- Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123".
- Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123.
- Pass phrases, if used in addition to or instead of passwords, should follow the same guidelines.
- Passwords shall not be the same as the User ID.

Create a password between 8 to 15 characters. Your password must contain at least:

- one special character (shift-number)
- one uppercase character
- one lowercase character
- and NOT contain any spaces
Use A Different Password on each Target System
Change Your Password Frequently
Don’t Reuse Passwords
Don’t Write Your Password Down
Who is Responsible For This Eye-Of-Newt Password Fascism?
Well I am a Little
What are these rules for?
Dictionary Attacks

How many times can I try to guess your password?
How Many Guesses?

History of passwords

- A: a lot
- A: jillions
- A: zillions
- A: three
- A: three, and the correct answer changes each time you try
A lot of guesses

- Late 1970s, when Unix passwords were hashed with a salt (Morris and Thompson)
- That made pre-computation impractical
- Access is mostly timesharing
A: Jillions

- Moore’s Law carries on, people don’t pick better passwords
- Networked services offer access to password files on misconfigured sites
- WAYWYT?
A: Zillions

• Today

• Multicore computers are perfect for password cracking

• Clouds, botnets, screen savers are all perfect for dictionary attacks

• If brute force doesn’t work, use more.
The Dictionary Attack Arms Race

- Moore’s Law: 12 doublings since 1990
- And multi-core CPUs are perfect for password cracking
- Can a human choose and remember a password that a computer can’t guess when limited only by computer speed and time available?
Evolution of the bad guys

• academics
• teens without girl friends
• governments
• organized crime, drug lords, terrorists
We Knew People Pick Weak PWs by 1990

It is simply poor engineering to expect people to select and remember passwords that are resistant to dictionary attacks.
Results

• People violate many of these rules routinely, for usability reasons

• Stringent rules increase use of fall-back systems, which are usually less secure, or more expensive

• The rules don’t make most things more secure in the face of most current threats
A: Three guesses

• Lock the account for a while or forever if there are too many wrong guesses in a row, or too many wrong guesses forever

• A locked account is a pain, but much better than illicit access

• Any non-moronic password can now be used
Non-moronic password rule

- Pick something a friend, colleague won’t guess in a few tries.
Summary solution

- Limited guesses and lock the account
- Non-moronic passwords
The Problem: the threat model has changed

- Dictionary attacks are not used very much any more
- Keystroke loggers and phishing beat any strong password
- If I watch (or listen!) to you type, I can get the full password regardless of complexity!
A: three, and the correct answer changes

- This is done with one-time passwords
- The answer is based either on the time, or the response to a changing challenge
- Usually requires hardware, or a piece of paper (but see below)
SecureID
SecureNet Key
SNK-004
A login from my distant past

RISC/os (inet)
Authentication Server.

Id? ches
Enter response code for 70202: 04432234

Destination? cetus
$
Challenge/Response passwords

- Gets us out of the game
- Sniffing is not useful
- Man-in-the-middle can still be used
- Pretty much nothing to forget
- A PIN is helpful to make two-factor
- Surprisingly cheap
Why aren’t these ubiquitous?

- Cheap devices available before 1990
- People hate:
  - Having to carry the device
  - Entering the challenge (why SNK lost)
  - Entering the response
  - Carrying multiple devices
Further password criteria?

• Text-only is most general

• The web isn’t the only place we need these solutions

• But maybe iPhone-like interfaces will be ubiquitous enough

• Memorability? Shoulder-surfing?
Password Properties

• Memorable?
  • Daily, monthly, yearly?
  • Cost if forgotten

• Hardware needed?
• Training steps needed
• User selected?

• Single use?
• Changeable?

Text
• Easy to write down?

• Easy to describe or transmit?
• Authentication speed
• Text, graphical, bio, other

42 of about 115
Some Password Ideas
Passpoints

from Dirik, Memon, Birget; SOUPS 2007
Passfaces

Welcome to Passfaces, Please Log On

Click on your passface to logon

(go on!)
Passfaces

Meet your passfaces

Here are your passfaces ...

Press Next
(Don't worry about remembering your passfaces at this stage)
Deja Vu
(Recognition-based)
Draw a Secret

Lin, Dunphy, et al. SOUPS 2007
Use Your Illusion (SOUPS 2008)

Please memorize the three distorted images shown above.
Some Whacko Ches Ideas

Passmaps
TODO: Find a point in New York State

Adirondacks are nice
Lakes have interesting shapes, let’s zoom in on the middle
Upside down dog in the upper left
Dogs bark, check out the voice box
PW is lat/long of the center island
Passmaps?

- Reproducibly zoom in on a remembered set of map features?
- Nice for a touch screen?
- Lots of bits
- Maybe hard to shoulder surf
- Not challenge/response
- Memorable over a year?
Some Whacko Ches Ideas

How about passgraphs? Get Google out of the loop
Passgraphs?

• Similar to passmaps, but Google is out of the equation

• Maps can have a personal meaning

• Is this a good thing, or a bad thing?
Some Whacko Ches Ideas

Obfuscated human-computed challenge response
Problem

• One-time passwords solve a lot of password problems

• One-time passwords (usually challenge/response) require something you have

• Equipment can be expensive, and it may be necessary to authenticate when equipment is not available
Baseball players

- Under a lot of stress
- Information is often vital to the game
- Not always the sharpest knife in the drawer
  - Babe Ruth forgot the signs five steps out on the field
Key insight?

• Humans can’t compute well, but perhaps they can obfuscate well enough
Proposed approach

• Use human-computed responses to computer challenges for authentication

• Though the computation is easy, much of the challenge and response is ignored

• Obfuscation and lack of samples complicate the attacker’s job beyond utility
Challenge:

ches 00319 Thu Dec 20 15:32:22 2001   23456bcd;f.k
root 00294 Fri Dec 21 16:47:39 2001   nj3kdi2jh3yd6fh:/
ches 00311 Fri Dec 21 16:48:50 2001   /ldh3g7fgl
ches 00360 Thu Jan 3 12:52:29 2002   jdi38kfj934hdy;dkf7
ches 00416 Fri Jan 4 09:02:02 2002   jf/13kf.12cxn. y
ches 00301 Fri Jan 4 13:29:12 2002   j2mdjudurut2jdnch2hdng3kdjf;'/s'
ches 00301 Fri Jan 4 13:29:30 2002   j2mdgj/.m3hdʻk4hfz
ches 00308 Tue Jan 8 09:35:26 2002   /16k3jdq,
ches 84588 Thu Jan 10 09:24:18 2002   jf010fk;/.j
ches 84588 Thu Jan 10 09:24:35 2002   heu212jdg431j/
ches 00306 Thu Jan 17 10:46:00 2002   jfg.bv,vj',/1
ches 00309 Fri Jan 18 09:37:09 2002   jzw                          * no *
ches 00309 Fri Jan 18 09:37:36 2002   jzw                          * no *
ches 00368 Tue Jan 22 09:51:41 2002   84137405jgf/
ches 77074 Tue Feb 19 09:02:52 2002   d                          * no *
ches 77074 Tue Feb 19 09:02:57 2002   hbcg3j'ld/
ches 00163 Mon Feb 25 09:24:30 2002   d                          * no *
ches 00163 Mon Feb 25 09:24:35 2002   ozhdkf0ey2k/,.vk01
ches 00156 Tue Mar 12 12:41:12 2002   3+4=7 but not 10 or 4/2
ches 00161 Fri Mar 15 09:41:20 2002   /.kl9djhfr
ches 00161 Fri Mar 15 09:41:36 2002   3                          * no *
ches 00160 Mon Mar 25 08:52:59 2002   222
ches 00160 Mon Mar 25 08:53:09 2002   2272645
ches 29709 Mon Apr 1 11:36:34 2002   4
ches 41424 Mon Apr 8 09:49:09 2002   ab3kdhf
ches 85039 Tue Apr 9 09:46:06 2002   04
ches 00161 Thu Apr 18 10:49:14 2002   898for/dklf7d

Response:

23456bcd;f.k
nj3kdi2jh3yd6fh:/
/ldh3g7fgl
jdi38kfj934hdy;dkf7
jf/13kf.12cxn. y
j2mdjudurut2jdnch2hdng3kdjf;'/s'
j2mdgj/.m3hdʻk4hfz
/16k3jdq,
jf010fk;/.j
heu212jdg431j/
jfg.bv,vj',/1
jzw                          * no *
84137405jgf/
d                          * no *
hbcg3j'ld/
d                          * no *
ozhdkf0ey2k/,.vk01
3+4=7 but not 10 or 4/2
/.kl9djhfr
3                          * no *
222
2272645
4
ab3kdhf
04
898for/dklf7d
Pass-authentication

• Literature goes back to 1967

• A variety of names used: reconstructed passwords, pass-algorithms, human-computer cryptography, HumanAut, secure human-computer identification, cognitive trapdoor games, human interactive proofs
Possible uses

• emergency holographic logins ("passwords of last resort")

• use from insecure terminals, when single session eavesdropping is probably not a problem

• if a solution is found: daily logins

• home run: online transactions: banking
Problems

• Can Joe Sixpack do this?
• Math is hard
• Procedural vs informational knowledge
Current Threats and Some Revised Advice
Disclaimer

- These are all guidelines, suggestions, thoughts for your own risk/benefits analysis

- Every security person I’ve discussed this with has a somewhat different take

- Rethink and reengineer these systems, when appropriate
Threats to casual targets

• Password capture by phishing
• Password capture by keystroke logging
• *Not* dictionary attacks
  • Most online systems limit password guessing
• Most attacks are wholesale, not targeted
Dictionary attacks still a concern

- For standard Unix logins
- For ssh password logins
- Against captured oracle streams, like PGP and ssh key files, cleartext challenge/response fields in protocols
- These are not mainstream attacks these days. Stolen laptops/iPhones a concern
Recommendations for users

• Use three levels of passwords based on importance:
  • No importance: NY Times, etc.
  • Inconvenient if stolen: Amazon
  • Major problem if abused: bank access, medical records(?)
For users (cont.)

• Write down the rare ones if you must
• Don’t write down the password, write a reminder of the password
• Use variations to meet “strong” password requirements.
• Do note required variations (i.e. lower case, no spaces)
Save your passwords with Firefox?

- Little difference against keystroke logging
- Key-ring protection mechanisms subject to dictionary attacks
- If stolen, you have given away an authentication factor
If you must, here are at least 60 random bits

- value part Peter sense some computer
- anxiety materials preparation sample experimental
- bliss rubbery uncial Irish
- 2e3059156c9e378
If you must

• not user-chosen, but user can veto, waiting for a “good one”

• User-chosen phrases have much lower entropy

• they are going to write it down, for a while

• for daily use: who’s going to remember this over a year?
Words are better than eye-of-newt

- much easier to type
- spelling checking (iPhone) is your friend, not enemy
Entropy, >41 bits per line

You grim-faced pipe of pleuritic snipe sweat
You dire chiffonier of foul miniature poodle squirt
You teratic theca of pathogenic moth dingleberry
You worrying pan broiler of bilious puff adder slobber
You vile wok of tumorigenic aphid leftovers
You baneful reliquary of pneumonic miller stumps
You atrocious terrine of harmful Virginia deer vomition
You excruciating pony of septic redstart eccrisis
You blotted kibble of unhygienic wild sheep spittle
You hard-featured fistula of podagric macaque flux
Uncial

uncial |ˈən shəl; -sēəl|  adjective

1 of or written in a majuscule script with rounded unjoined letters that is found in European manuscripts of the 4th–8th centuries and from which modern capital letters are derived.

2 rare of or relating to an inch or an ounce.

noun

an uncial letter or script.
iPhone-friendly passwords?

- grade likes jokes guess
- goes joke gold gods rode fire rows
- votes mines bored alike yard
- what knit bomb unit star grow
- actor agent above angel abuse
- honey learn least lemon links
Easy words?

- a
- inch
- adapt
- charm
- fruit
- media
- relax
- thick
- m
- iron
- admit
- chart
- fully
- meets
- reply
- think
- v
- isle
- adopt
- cheap
- funny
- mercy
- rings
- throw
- at
- item
- adult
- check
- giant
- minus
- rival
- toxic
- by
- keen
- again
- cheek
- gifts
- model
- round
- track
- cm
- keep
- agent
- choir
- given
- money
- rural
- trail
- ft
- kept
- ahead
- civil
- grant
- month
- salad
- trees
- ii
- knit
- alarm
- claim
- graph
- moral
- scale
- trial
- la
- know
- album
- clear
- group
- motor
- scene
- trips
- my
- lamb
- alive
- clerk
- habit
- mouth
- scope
- truly
- act
- lamp
- alpha
- clock
- happy
- movie
- serve
- twice
- aha
- left
- angel
- coach
- harsh
- mummy
- seven
- uncle
- all
- lend
- anger
- coast
- heart
- music
- shall
- under
- arm
- loch
- angle
- could
- heels
- nails
- shape
- union
- ask
- main
- apart
- crack
- hello
- nasty
- sharp
- units
- bed
- many
- apply
- crime
- hence
- naval
- shelf
- unity
- cup
- mark
- argue
- cruel
- honey
- nerve
- shell
- until
- erm
- meal
- array
- curve
- hotel
- never
- shock
- upset
Rethinking Passwords

Bill Cheswick
AT&T Labs - Research
ches@research.att.com