Rethinking
Passwords

Bill Cheswick
AT&T Labs - Research
ches@research.att.com
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
FIPS 112

• Specification for Password Usage. (May 1985)

• Based on twenty years of computer experience
  • time sharing
  • minicomputers
  • “Early” in Moore’s Law curve
FIPS 112

• The basis of most of our password wisdom
• Mostly still right
• Threats have changed
• We need to change some of the rules, and should have done so quite a while ago
Outline

• Review of old threats and the associated password rules.
• Some properties of passwords, and some of the research to improve them
• Current threats and revised password advice
• Conclusion
Old Threats and Associated Password Rules
Old Threats

• Time sharing terminals open to the public
• Time sharing systems accessible to the public
• Early Unix daemons with simple authentication
• Early Internet protocols, no crypto
The set of acceptable passwords should be large enough to assure protection against searching and testing threats to the password system (and hence the data or resources that it protects) commensurate with the value of the data or resources that are being protected.

--- FIPS 112, Appendix, section 3.1
Poor engineering

• To expect people to create and remember passwords that computers can’t guess, given unlimited attempts

• This is especially true in the face of Moore’s Law

• multi-core CPUs are perfect for dictionary attacks
Some Bad Examples

• Audix: monthly password change
• It just isn’t that important
• Lockout is fine
• PIN is longer than my bank card!
• Same requirements as my online stock access!
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.
4.3 Password System for High Protection Requirements

1. Length Range: 6-8
2. Composition: Full 95 character set
3. Lifetime: One month
4. Source: Automated password generator within the authentication system
5. Ownership: Individual
6. Distribution: Registered mall, receipt required; personal delivery, affidavit required
7. Storage: Encrypted passwords
8. Entry: Non-printing keyboards
9. Transmission: Encrypted communication with message numbering
10. Authentication Period: Login and after 5 minutes of terminal inactivity.
Poor engineering

- To expect people to differentiate authentication to numerous different, but related services
FIPS 112 complaints

• Maximum password life of one year (3.3.1)

• The risk associated with an undetected compromise of a password can be minimized by frequent change --- Appendix 3.3

• But what about accounts we use annually?
FIPS 112 complaints

• Passwords protecting shared data should only be known by the individuals authorized for that data (3.5.3), but see Appendix 3.5
Poor security

- Passwords should not be shared.
FIPS 112 complaints

- Select a password not related to the user’s identity, history, or environment (3.4.4)
Poor engineering

• To expect people to remember a password they use only twice a year

• To expect people to differentiate authentication to numerous different, but related services
Poor engineering

- To change passwords often. Strong passwords are hard to generate.
- To allow dictionary attacks
- To lock most accounts indefinitely
- To protect most important systems with single-factor authentication
Some Outdated rules

• Change your password often
• Make passwords resistant to dictionary attacks through strength rules
• Use a different password on each machine
• Don’t write your passwords down
The Problem

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

• Stringent rules increase use of fall-back systems, which are expensive

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

• If brute force doesn’t work, use more.
Properties of Passwords
Password Properties

• Memorable?
• Daily, monthly, yearly?
• How easy to write down password
• How easy to describe or transmit password?
• Single use?
Password properties

• Cost if forgotten
• Changeable?
• Susceptible to dictionary attack
• Susceptible to eavesdropping?
• Susceptible to replay?
• User selected?
• Susceptible to shoulder surfing?
Some Graphical Solutions
Passpoints

from Dirik, Memon, Birget; SOUPS 2007
Passfaces

Welcome to Passfaces, Please Log On

Click on your passface to logon

(go on!)
Passfaces

Here are your passfaces ...

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

• Out of Berkeley, 1999-2000

• recognize previous images, rather than memorizing them.
Draw a Secret
Hotsec 2007

• “yesterday’s answers to today’s questions”
Use Your Illusion (SOUPS 2008)

Please memorize the three distorted images shown above.

OK
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?
• 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
Text-only, please

- Most general interface and solution
- Fits into PAM and other challenge/response processing
Key insight?

• Humans can’t compute well, but perhaps they can obfuscate well enough
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
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   j2mdjudurut2jdnch2hdtg3kdjf;s'/s
ches 00301 Fri Jan 4 13:29:30 2002   j2mdgfj./m3hd’k4hfz
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   no way 1 way is best!/1
ches 00309 Fri Jan 18 09:37:36 2002   jzw
ches 00368 Tue Jan 22 09:51:41 2002   84137405jgf/
ches 77074 Tue Feb 19 09:02:52 2002   d
ches 77074 Tue Feb 19 09:02:57 2002   hbcg3]’d/
ches 00163 Mon Feb 25 09:24:30 2002   d
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   /.,kl9djfir
ches 00161 Fri Mar 15 09:41:36 2002   3
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
j2mdjudurut2jdnch2hdtg3kdjf;s'/s
j2mdgfj./m3hd’k4hfz
/16k3jdq,
jf010fk;.j
heu212jdg431j/
jfg.bv,vj/,1
no way 1 way is best!/1
jzw
84137405jgf/
d
hbcg3]’d/
d
ozhdkf0ey2k/.,vk01
3+4=7 but not 10 or 4/2
/.,kl9djfir
3
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
Two Kinds of P-A Solutions

- ad hoc
- information theoretic
Ad Hoc solutions

- familiar to the designer
- idiosyncratic
- hard to analyze
Information theoretic

- Strong proof of work factor to crack
- None seem usable to me, and certainly not useable to Joe Sixpack
Problems

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

For Most Casual Users
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
WOW

• Almost all passwords are stolen with key loggers

• After compromise, multi-factor authentication required to reactivate, including faxed and notarized legal documents.
Updated Advice
For Users
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(?)

78 of about 100
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)
Updated Advice
For Implementors
Get Out of the Dictionary Attack Game
Get Out of the Dictionary Attack Game

• Avoid strong passwords in most cases
• Count and manage authentication attempts with a server
• pam_tally
• slow or block accounts (block is better than loss of control of an account)
• blacklist inquisitive IP addresses
Getting out of the game

• Humans will lose to dictionary attacks, period. We lost this game in the 80s. Why are we still playing it?

• Unix publicly-readable password hash was a mistake

• shadow password file is better
  • need system, not file, for attack
Getting out of the game

- slowing response to queries is good
- no file to consult: ssh passphrase, shadow file, PPTP authentication are examples
- when a computer is involved, it can count failures
Client certificates can limit attacks

- Limiting connections to those with known client certificates gets you out of the game
- Many mail clients do not offer client public keys
Use an authentication server

- Centralizes the security function
- Make it strong and robust
- Replication is dangerous, reliability is better
- Limit authentication attempts
Identify the auth.
server and pw rules

• Usually just an additional line to a web pages
• Yes, it leaks a little information
• It greatly eases the usability
  • name of server eliminates guessing and pw leakage
  • rules remind user of pw variation used
Locking an account

• Locking or slowing account authentication simplifies denial-of-service attacks

• A locked account is much better than a stolen account

• Slower authentication, or a timeout on lockout, mitigates user support costs
If password is forgotten

- Use a user-supplied reminder of the primary password
- Do not use a (usually weaker) secondary password
- The net has ancestor, and personal data, and will have lots more soon
- Blacklisting doesn’t have to be forever
Don’t make accounts too easy to guess

- Thwarts single password, multi-account scans

- U.S. Social security numbers are a little too guessable. Credit cards seem to be okay.

- But secret rules (hyphens in social security number?) reduce usability without improving security
Accounts should not be shared

- You want accountability, even (especially) on shared bank accounts.
- It doesn’t matter on the lowest grade authentication
One-time passwords can be stronger

- No replay attacks
- Bad guy (or his software) must be present to win
- May not be sharable
- Usually requires device or printout (but see below)
Challenge/Response passwords

• One time, one session password
• Closes up the S/Key race
A login from my distant past

RISC/os (inet) Authentication Server.

Id? ches
Enter response code for 70202: 04432234

Destination? cetus
$
SecureNet Key SNK-004
Solution: multi-factor authentication

- Dongle is fine, but requires PIN, or is single factor
- PC is fine: ssh public key plus pass phrase
- broken: pass phrase subject to dictionary attack, because a server not needed to check validity
Newer options: we have hardware

- laptops are fine containers of public keys
- use a passphrase to protect the key
- dictionary attack rules apply
- cell phones with SMS may give a secure path for challenge/response
Multi-factor authentication

- password or pass-phrase is usually one
- something you have, something you know, something you are
- I rely on a device (my laptop) with a strong key (ssh DSA) locked with a passphrase
Biometrics

- Generally around 90% accurate
- A variety of workarounds
- Users may be reluctant to give up data
- Not bad for an auxiliary factor in strong authentication
Protocol Streams: we have crypto, use it

• Unencrypted streams offer sniff-and-dictionary-attack opportunities
• Crypto fixes this, with public keys frustrating man-in-the-middle attacks
• https, POP3, IMAP, PPTP
Getting out of the game: ssh

- disable password logins. Use DSA key from a trustable client, that key locked with a strong pass-phrase
- two-factor authentication
- dictionary attack is rare endgame: you have to steal or own the client first
- Reasonably secure clients are doable
Routine on seismo.arpa.net

seismo.arpa.net login failures:
Oct 21 00:12:56 seismo sshd[14326]: Invalid user foobar from 209.160.73.63
Oct 21 00:13:17 seismo sshd[14392]: Invalid user test from 209.160.73.63
Oct 21 00:13:18 seismo sshd[14394]: Invalid user test from 209.160.73.63
Oct 21 00:13:18 seismo sshd[14396]: Invalid user test from 209.160.73.63
Oct 21 00:13:19 seismo sshd[14398]: Invalid user test from 209.160.73.63
Oct 21 05:32:43 seismo sshd[33315]: Invalid user admin from 209.160.73.63
Oct 21 05:32:43 seismo sshd[33317]: Invalid user admin from 209.160.73.63
Oct 21 05:32:44 seismo sshd[33319]: Invalid user admin from 209.160.73.63
Oct 21 05:32:45 seismo sshd[33321]: Invalid user admin from 209.160.73.63
Oct 21 05:32:46 seismo sshd[33323]: Invalid user admin from 209.160.73.63
Oct 21 05:32:46 seismo sshd[33325]: Invalid user admin from 209.160.73.63
Oct 21 05:48:24 seismo sshd[33399]: Invalid user eric from 209.160.73.63
Oct 21 05:48:25 seismo sshd[33401]: Invalid user johny from 209.160.73.63
Oct 21 05:48:38 seismo sshd[33445]: Invalid user edward from 209.160.73.63
Oct 21 05:48:39 seismo sshd[33447]: Invalid user edward from 209.160.73.63
Oct 21 05:48:39 seismo sshd[33449]: Invalid user edward from 209.160.73.63
Oct 21 05:48:40 seismo sshd[33451]: Invalid user russ from 209.160.73.63
....
Near-public authentication servers

- OpenID
- Openauth
- The general idea is appealing
These could be a commercial solution

- Simpler than Radius, X.509 certificates
- Name space issues
  - att/ches
  - ches@research.att.com seems to work well
Yeahbuttal

- These ideas will take time to deploy, if they do
- Huge installed base
- Corporate conglomerates have hundreds or thousands of these!
- Who owns the ap?
- Who hosts it?
• Third party applications? (401k, health, etc.)

• Who developed it? (often long gone)

• What is the business function

• Buy-in is needed from all parties

• Development costs?
Selling weaker passwords

- Cut user support costs
- Improve the users’ experience
- ATM PINs of 4 digits works fine
- Tell them I said it was probably a good idea (if that helps).
Strong Authentication, not strong passwords

- Use multi-factor authentication when it is really important
- Ubiquitous laptops and cell phones can be used for middle-level authentication
- Securenet Key is better than SecurID
Rethinking Passwords

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