

Rethinking Passwords

Bill Cheswick

ches@cheswick.com

Visiting scholar, U. Penn.

Intel's rules

- The password must be **at least 8 characters long**.
- The password **must** contain at least:
 - **one** alpha character [a-zA-Z];
 - **one** numeric character [0-9];
 - **one** special character from this set:
` ! @ \$ % ^ & * () - _ = + [] ; : ' " , < . > / ?
- The password **must not**:
 - **contain spaces**;
 - **begin with an exclamation [!] or a question mark [?]**;
 - contain your login ID.
- The first 3 characters cannot be the same.
- The sequence of the first 3 characters cannot be in your login ID.
- The first 8 characters cannot be the same as in your previous password.
- Passwords are treated as **case sensitive**.

Golden Rule Health

PASSWORD RULES (Please note the password is case sensitive)

Must contain at least 8 characters.

Must include a number and a letter.

No more than two consecutive characters may be the same.

Passwords must be changed at least every 180 days.

No password may be re-used for a period of 1 year.

3 invalid attempts to login will result in a 30 minute lockout.

Wachovia (now Wells Fargo)

Passwords must be 7-20 characters

Must include at least one letter and one number, with no spaces

Semi-colons cannot be part of a Password

Passwords are case sensitive

Do not use your User ID as your Password

Dartmouth

- It should be **eight characters long** using only numbers and **upper- and lower-case letters**. **Note:** Passwords longer than eight characters will not work to authenticate you with some applications used at Dartmouth, such as Kerberos and Oracle Calendar.
- There can be **no more than four characters in sequence** (e.g., **12345** or **abcde** are not allowed).
- It must contain at least **five different characters** (e.g., **2a3a2a3a** only contains three different characters so is not allowed).
- It **cannot be a word found in the dictionary, including foreign languages** (e.g., **password**).
- It cannot be a **reversal of a word found in the dictionary** (e.g., **drowssap**).
- It cannot be a **word found in the dictionary, plus one additional character** either before or after the word (e.g., **xalgebra** or **algebrax**).
- It cannot be a word found in the dictionary with numbers substituted for look-alike letters (e.g., **passw0rd** or **pa55word**).
- It cannot be a word found in the dictionary minus any punctuation, symbols, or numbers (e.g., **oclock** or **soninlaw**).

| | length | case sens. | A-Z | a-z | 0-9 | sym | OK | not OK |
|-------------|--------|------------|-----|-----|-----|-----|----|--------|
| Intel | >=8 | Yes | R | R | R | ok | | ⌋ |
| Golden Rule | >=8 | | | | | | | |
| Wachovia | 7-20 | Yes | ok | R | | no | | |
| Dartmouth | 8 | | ok | ok | ok | no | | |
| AT&T Uvers | 6-24 | Yes | R | | R | no | - | |
| AT&T GNO | 5-8 | No | | | | | | |
| OAG | 7-50 | Yes | R | | R | | | ⌋ ‘ ‘ |
| War-craft | 8-16 | | R | | R | | | -!"#\$ |
| DHS | 8-15 | | R | | R | | | ⌋ |
| Calnet | 9-255 | | 3 | 3 | 3 | 3 | ⌋ | |
| UAL | 6-24 | No | | | | | | |
| Lehigh | >=7 | | 2 | 2 | 2 | 2 | | |

Fillet of a fenny snake,
In the cauldron boil and bake;
Eye of newt and toe of frog,
Wool of bat and tongue of dog,
Adder's fork and blind-worm's sting,
Lizard's leg and howlet's wing,
For a charm of powerful trouble,
Like a hell-broth boil and bubble.

-- Macbeth, Act 1, Scene 1

**Use A Different Password on each
System**

Change Your Password Frequently

Don't Reuse Passwords

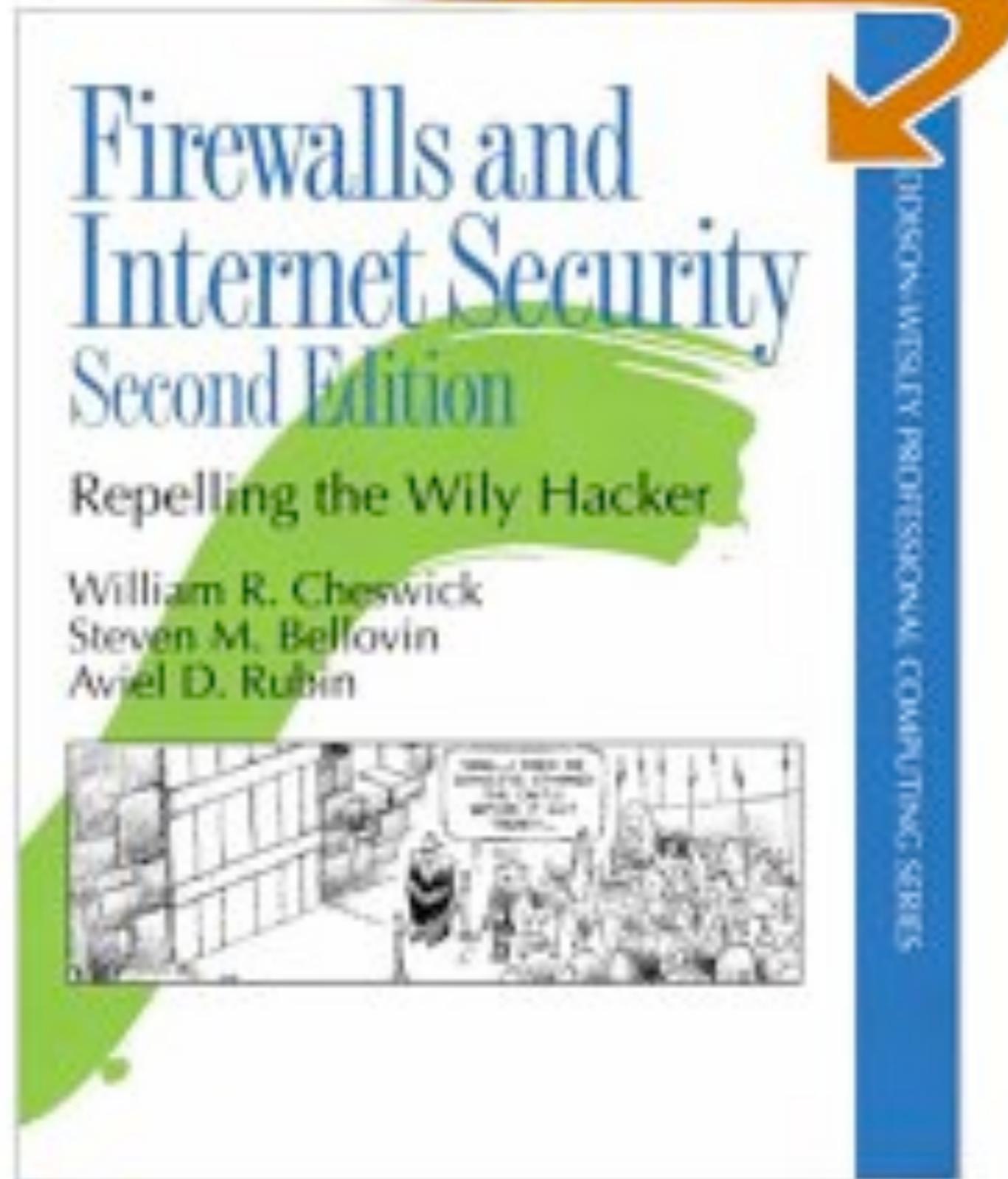
Don't Write Your Password Down

This is a usability nightmare!

Who's responsible for this?

Well, I am, a Little

SEARCH INSIDE!™



CSC-STD-002-85: DOD Password Management Guideline

- **The “green book”.**
- **A variety of mostly-excellent security suggestions**

| Scheme | Cracked in | | Change time | |
|---------------------------------|------------|-------|-------------|------|
| 8 character, full alphanumeric | 6.72 | mins. | 0.40 | ms. |
| 8 character, EoN | 9.25 | days | 31.19 | ms. |
| 11 character, EoN | 20,390 | years | 7.4 | days |
| 13 character, full alphanumeric | 906,123 | years | 331 | days |
| 12 character, Eye-of-newt | 1,896,229 | years | 692 | days |

Where Do Security Policies Come From?

Dini Florêncio and Cormac Herley

SOUPS 2010

Those that accept advertising, purchase sponsored links, or user has a choice have weakest password requirements

Strongest passwords: .gov, then .edu

These rules come from the Deep Past in computing and security

- **Time sharing terminals in public places**
- **Attacks on the login interfaces on network services**
- **Network eavesdropping was often trivial**
- **The stakes were usually much lower**
- **Institutionalized passwords on, say, telephone switches**
- **Changing passwords: lost military crypto gear**

Dictionary Attacks

- **Have a computer try as many password guesses as possible**
- **The required effort is called the “work factor”, and the resistance to attack is often (incorrectly) called the “entropy” of the password.**
- **These attacks can be directed at online authentication services, or against stolen hashed password files.**

mail.coastal.cheswick.com login failures:

Sep 21 03:11:03 mail sshd[90325]: Invalid user cgi from 219.139.108.134
Sep 21 03:11:15 mail sshd[90335]: Invalid user oracle from 219.139.108.134
Sep 21 03:11:18 mail sshd[90337]: Invalid user tomcat from 219.139.108.134
Sep 21 03:11:47 mail sshd[90361]: Invalid user nagios from 219.139.108.134
Sep 21 04:50:29 mail sshd[54849]: Invalid user devtest from 58.213.48.82
Sep 21 04:50:33 mail sshd[54851]: Invalid user dede from 58.213.48.82
Sep 21 04:51:49 mail sshd[54895]: Invalid user anja from 58.213.48.82
Sep 21 04:51:55 mail sshd[54897]: Invalid user anja from 58.213.48.82
Sep 21 04:51:59 mail sshd[54899]: Invalid user platinum from 58.213.48.82
Sep 21 04:52:03 mail sshd[54901]: Invalid user plcmspip from 58.213.48.82
Sep 21 04:52:06 mail sshd[54903]: Invalid user teamcity from 58.213.48.82
Sep 21 04:52:13 mail sshd[54905]: Invalid user teamspeak from 58.213.48.82
Sep 21 04:59:33 mail sshd[55143]: Invalid user addr from 58.213.48.82
Sep 21 04:59:37 mail sshd[55145]: Invalid user adempiere from 58.213.48.82
Sep 21 04:59:40 mail sshd[55147]: Invalid user admin2 from 58.213.48.82
Sep 21 04:59:43 mail sshd[55149]: Invalid user admin from 58.213.48.82
Sep 21 04:59:57 mail sshd[55157]: Invalid user admin from 58.213.48.82
Sep 21 05:00:02 mail sshd[55159]: Invalid user admin from 58.213.48.82
Sep 21 05:00:05 mail sshd[55177]: Invalid user adminftp from 58.213.48.82
Sep 21 05:00:08 mail sshd[55179]: Invalid user adminhelp from 58.213.48.82
Sep 21 05:00:12 mail sshd[55181]: Invalid user admin from 58.213.48.82
Sep 21 05:00:15 mail sshd[55183]: Invalid user admin from 58.213.48.82

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?**
- **Guessing rates can be 8×10^9 guesses per second per CPU!**

A note on Grandma



What are the most common current threats

- **Keystroke loggers**
- **Phishing attacks**
- **Password database compromise**
- ***NOT DICTIONARY ATTACKS!***

None of these are grandma's fault!

- ***Users are Not the Enemy*, A. Adams and M.A. Sasse, *Commun. ACM*, 42(12), 1999.**

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**

Some Password Ideas

From academia, and me

For a complete survey, see

- <http://people.scs.carleton.ca/~paulv/papers/gpsurvey-27sept2010.pdf>



from Dirik, Memon, Birget; SOUPS 2007

28 of about 93

Passfaces

Passfaces Logon (Java enabled page)

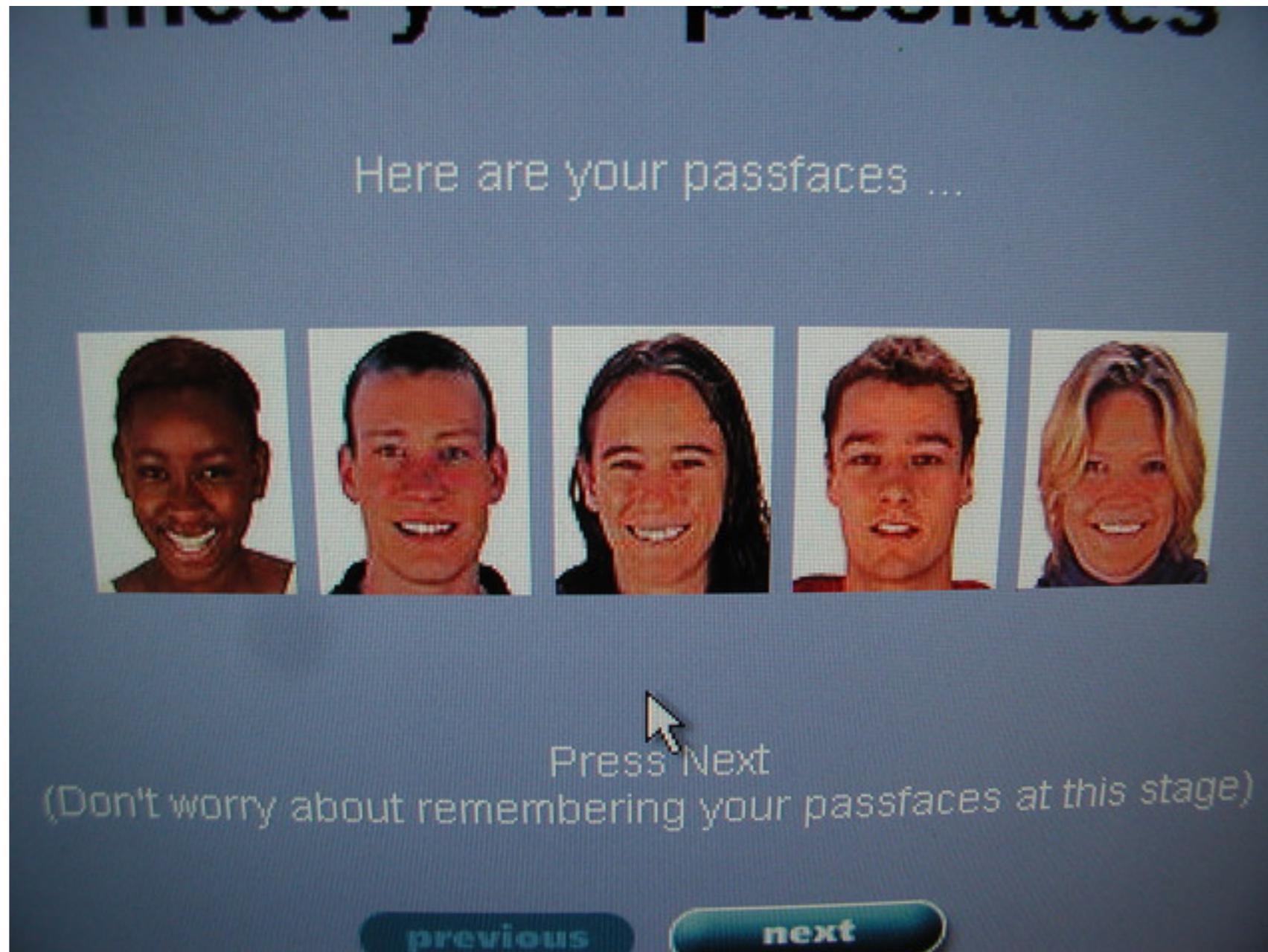
Log On 

Welcome to Passfaces, Please Log On

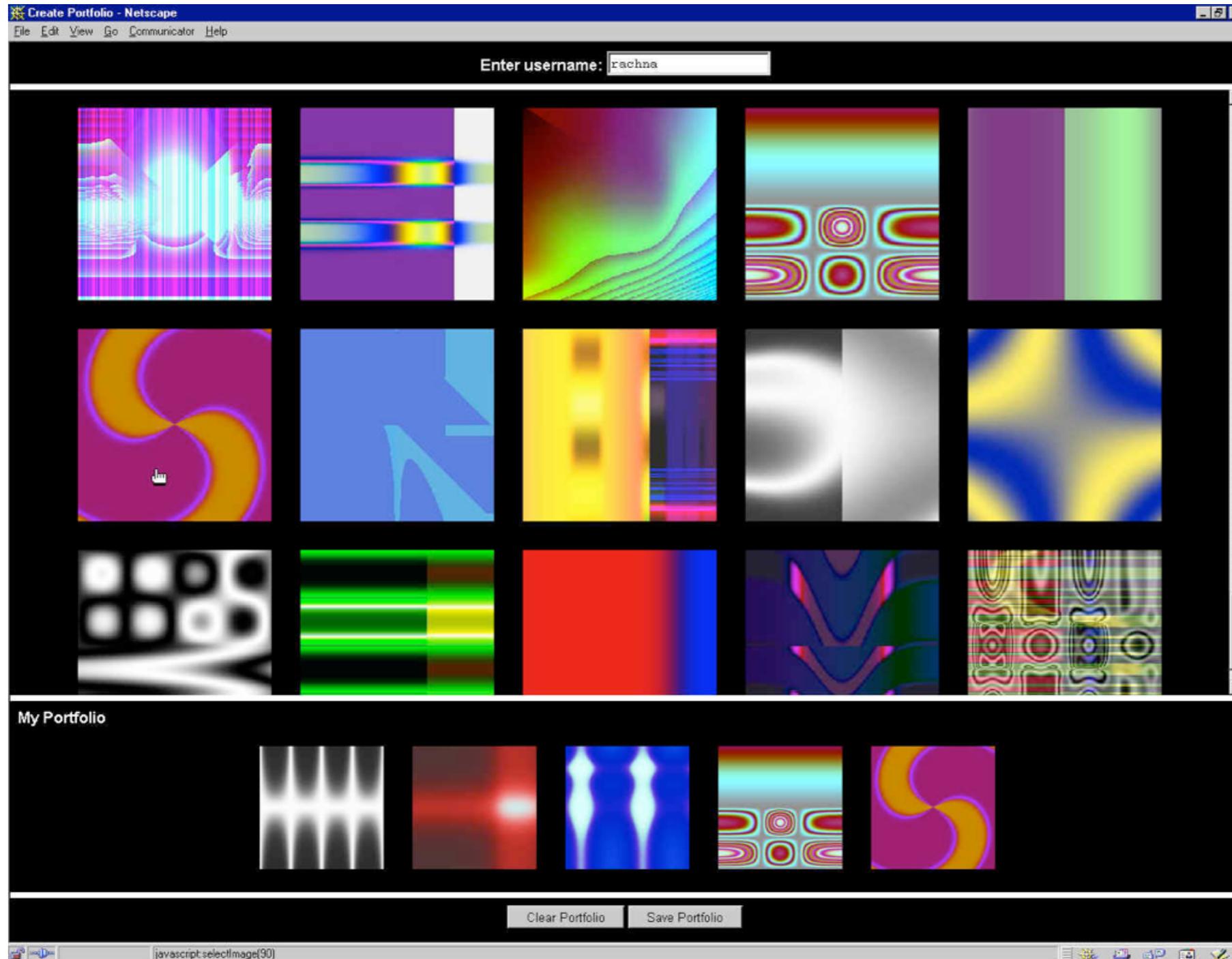
| Action | | |
|---|---|---|
|  |  |  |
|  |  |  |
|  |  |  |

Click on your passface to logon
(go on!)

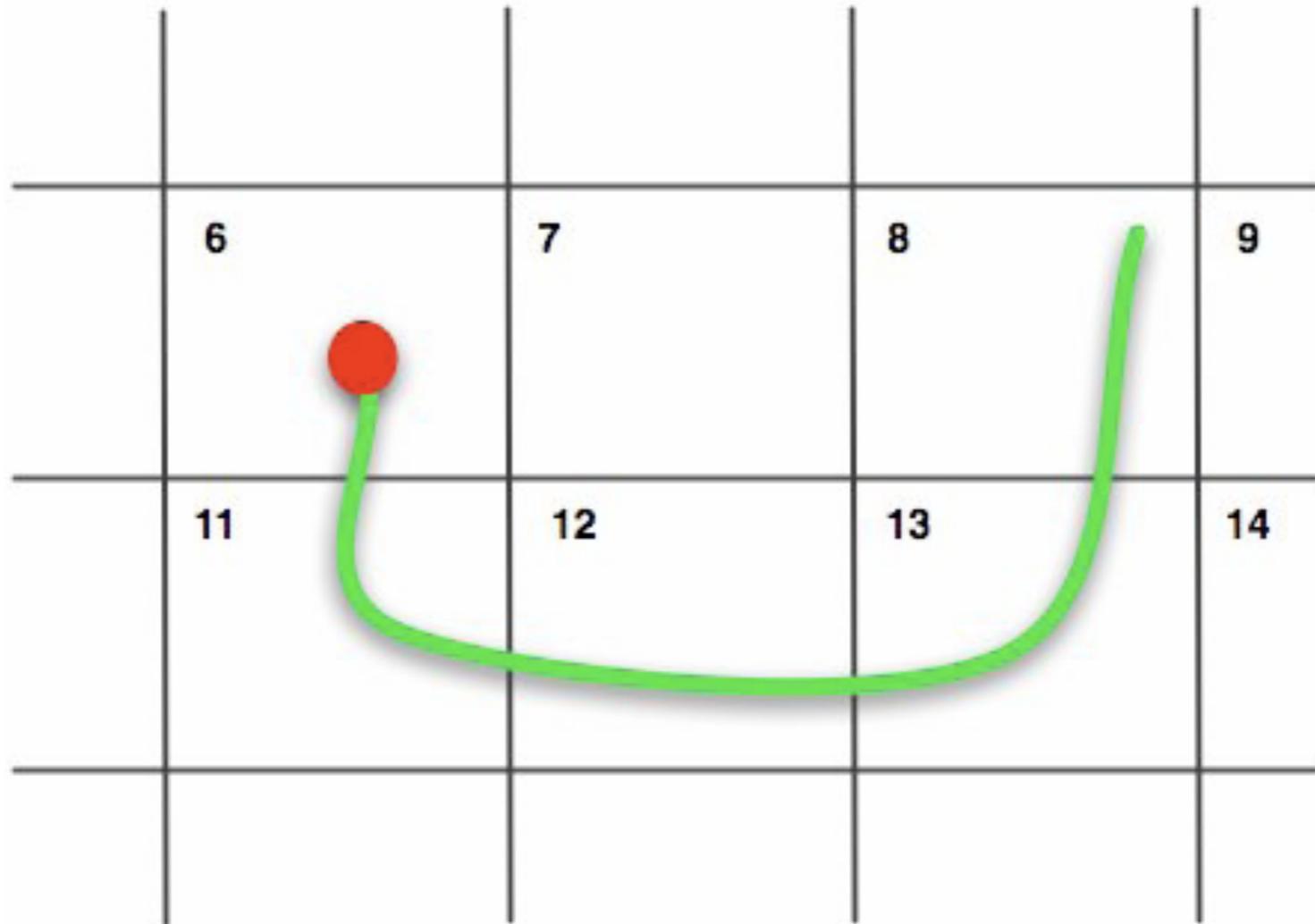
My passfaces



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.

OK

Can Something You Know Be Saved?

Baris Coskun and Cormac Herley, in *Proc. 11th Information Security Conference (ISC 2008)*, pp. 421-440, Springer-Verlag [September 2008]

Can “something you know be saved?”

- **I think so**
- **and, we don't have a choice in most cases**
- **security and convenience: tradeoff?**
- **It is going to be one of the authentication factors**
 - **something you know**
 - **something you have**
 - **something you are**
 - **where you are**
 - **.....**

Better Solutions

#1: Getting out of the game

SecureNet Key SNK-004



A login from my distant past

RISC/os (inet)

Authentication Server.

Id? ches

Enter response code for 70202: 04432234

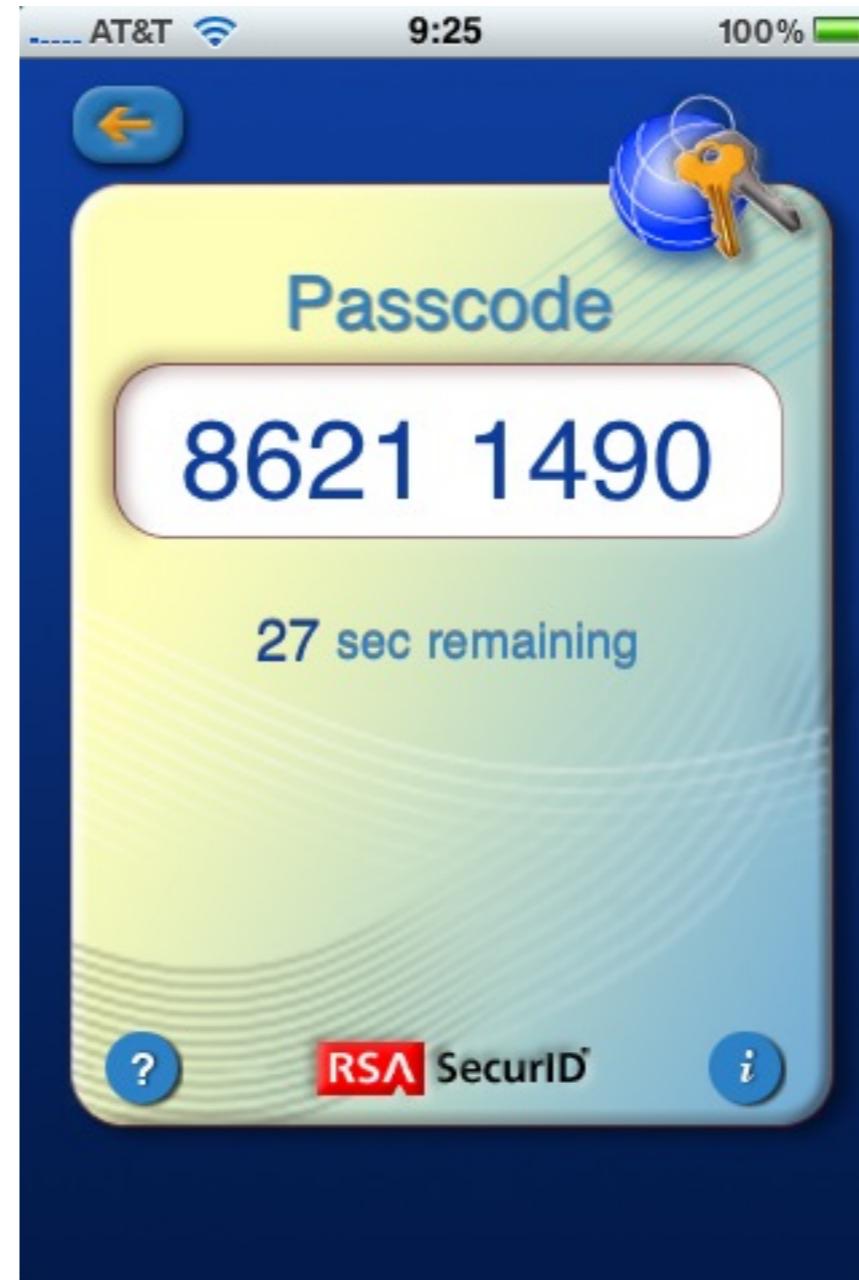
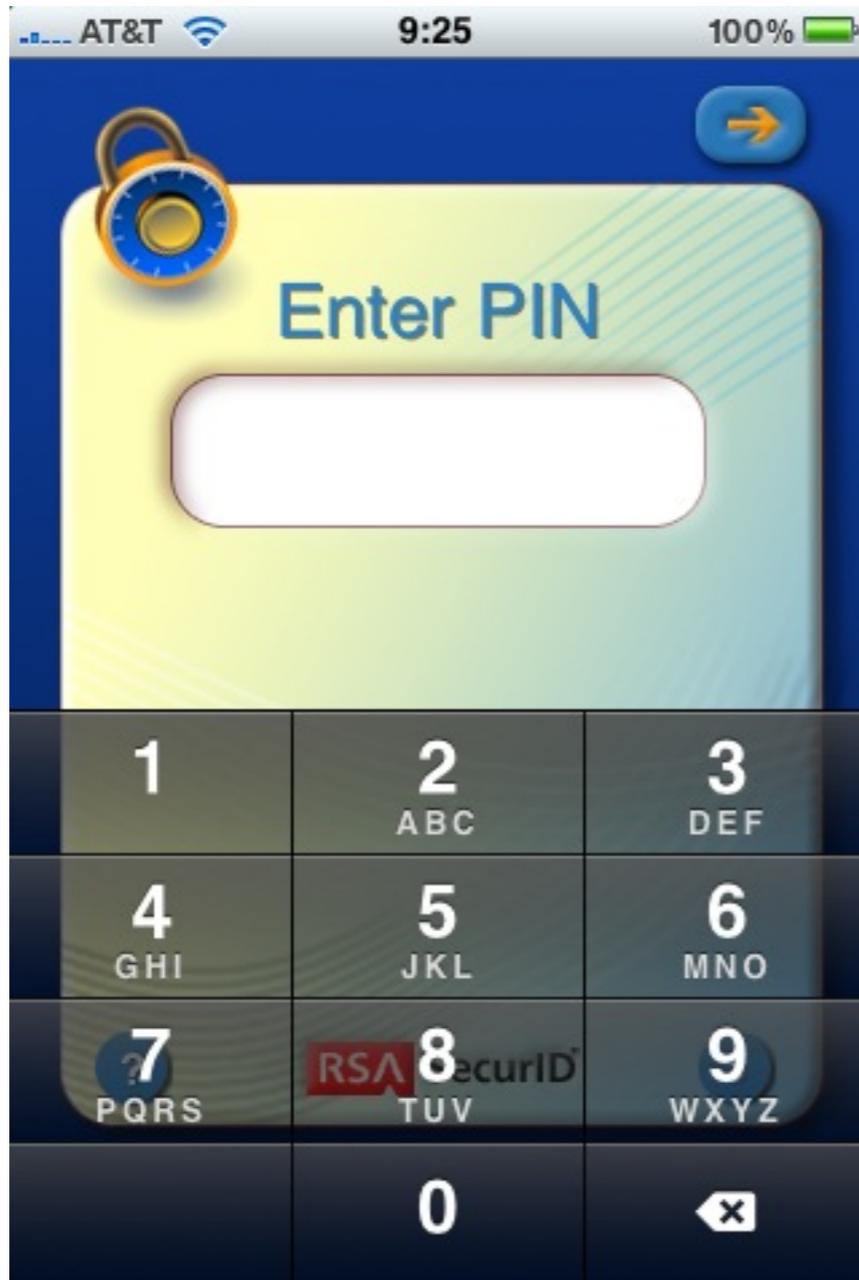
Destination? cetus

\$

SecureID



RSA Softkey



Great Things about the Softkey

- **You always have your iPhone with you**
- **A bad PIN simply gives the wrong answer**
- **That means that the program doesn't know the right answer**
- **That means that forensics can't run a dictionary attack on it with having an observed login**
- **That means that a lost iPhone isn't an authentication disaster**

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 authentication**
- **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**
- ***BUT*: You carry keys to use your car. Why not to authenticate on your computer?**

Better Solutions

#2: Limiting guesses

Limiting guesses

- **This has worked for ATM PINs since the early 1970s!**
- **It requires an authentication server, or some means to shut off the card/account**
- **It replaces the *eye of newt* rules with...**

An Engineering Goal: Non-moronic password rule!

**Pick something a friend, colleague won't
guess in a few tries,
and they can't figure out while watching you
type it**

Summary solution

- **Limited guesses and lock the account**
- **Non-moronic passwords**
- **Make locked accounts less painful**

Grandma can understand and comply with this rule

- **It makes sense**
- **Now, dictionary words are okay**
- **Simpler passwords are easier to remember**
- **You probably don't have to write them down**

Less painful account locking

- **Don't count duplicate password attempts**
 - they probably thought they mistyped it
- **Make the password hint about the primary password, and don't have a (weak) secondary**
- **Allow a trusted party to vouch for the user, so he can change his password**
- **Lock the account in increasing time increments**
- **Remind the user of password rules**

Better Solutions?

#3: Grasping the “passphrase” nettle

Still Want Your Strong Passwords?

Okay, fine. But let's make them fun, or at least easier to type (and tap)

A Very Short Course on Work Factor

$2^{10} = 1024$ of the most common British words

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might day yes however put world over another in want as life most against again never under old much something why each while house part number out off different went really thought came used children always four where without give few within about system local place great during although small before look next when case end things social most find group quite mean five party every company women says important took much men information per both national often seen given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself example space giving normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

Pick one at random, entropy = 10 bits ($2^{10} =$

1024)

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might day yes however put world over another in want as life most against again never under old much something why each while house part number out off different went really thought came used children always four where without give few within about system local place great during although small before look next when case end things social most find group quite mean five party every company women says important took much men information per both national often seen given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself **example** space giving normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

Two random choices = 20 bits

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might day yes however put world over another in want as life most against again never under old much something why each while house part number out off different went really thought came used children always four where without give few within about system local place great during although small before look next when case end things social most find group quite mean five party every company women says important took much men information per both national often seen given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking **early** making today mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself **example** space giving normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

20 bits = 2^{20} = 1,048,576

- **“example early”**
- **to guess our two words, requires:**
 - **1,048,576/2 guess, on average**
- **6 random words would be 2^{60}**
 - **1.15×10^{18}**
- **8 random words gives you Avogadro's number, a mole of work to do!**

Good stuff!

- **The list of words isn't secret**
- **so spelling checker is okay!**
 - **so is error correction! In a password!**
- **easy words to type**
- **on an iPhone, pick words where the "tappos" give the word you wanted**

Required entropy, according to Florêncio and Herley

- **Facebook, Twitter, etc. are a minimum of ~ 20 bits**
- **Banks are in the 30s**
- **Government in the mid 40s and up**

iPhone-Friendly? (40 bits)

- **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**

www.cheswick.com/ches/insults.html

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 unhygenic wild sheep spittle
You hard-featured fistula of podagric macaque flux

If you really need “high entropy” passwords

- **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?**

(105 demo)

Carrier 10:40 AM

Wallets Dictionaries Practice

Wallet name:

Work factor: 80

1k 4k 32k 64k 131k

problems sharing
workshop holy legend
gen equation

Pick another key

Carrier 10:40 AM

Wallets Dictionaries Practice

Wallet name:

Work factor: 80

1k 4k 32k 64k 131k

monitor crooks cutter
artaguette enchanting
decanted

Pick another key

Carrier 10:40 AM

Wallets Dictionaries Practice

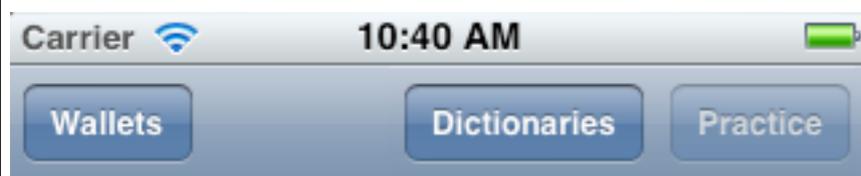
Wallet name:

Work factor: 80

1k 4k 32k 64k 131k

marechal hobbler
aurochs grinagog petiolar

Pick another key



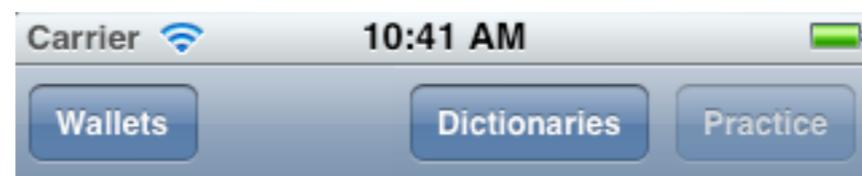
Wallet name:

Work factor: 105

1k 4k 32k 64k 131k

can evening reach
political applied whole
without needs door
member i

[Pick another key](#)



Wallet name:

Work factor: 105

1k 4k 32k 64k 131k

building award days
county rome why external
ran states

[Pick another key](#)



Wallet name:

Work factor: 105

1k 4k 32k 64k 131k

blokes hodgepodge
melissa jannequin vying
fha horseflesh

[Pick another key](#)

Use one Really Strong password to lock your password wallet

- You are not going to remember it immediately
- You will learn it after a while
- You don't have to change it
- 2^{105} bits means average work factor of 20,282,409,603,651,670,423,947,251,286,016 =
- $20 * 10^{30} = 33$ million times Avogadro's number

Frankly, I am sick of this!

Several solutions that work

Current threats vs. better passwords

- **Keystroke loggers**
 - needs strong, reliable clients. OS!
- **Phishing attacks**
 - some usability hacks would help
- **Password database compromise**
 - up to the pros. Need stiffer sentences.

People, we have to do better than this

- **The Bad Guys are getting much better**
- **Our computer systems are getting much more important to us**
- **Security has to be thought about, and reviewed**

Dangerous browsing

- ***All Your IFRAMES Point to Us*, Provos and Mavrommatis (Google), Rajab and Monrose (JHU); Usenix Security 2008**

Dangerous patches

- ***Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications.***
Brumley and Poosankam (CMU), Song (Berkeley), Zheng (Pitt); Proceedings of the IEEE Security and Privacy Symposium, May 2008.

Provably-hidden malware

- ***Analysis-Resistant Malware.*** Bethencourt and Song (BSD/CMU), Waters (SRI). ISOC NDSS, Feb 2008.

COTS CPUs dangerous?

- ***Designing and Implementing Malicious Hardware.* King, Tucek, Cozzie, Grier, Jiang, and Zhou (U Illinois at Urbana Champaign). Usenix LEET 2008, April, San Francisco.**

Stuxnet

- **The pros are *very* good at this sort of thing**

Rethinking Passwords

Bill Cheswick

ches@cheswick.com

Visiting scholar, U. Penn.

Our Digital House



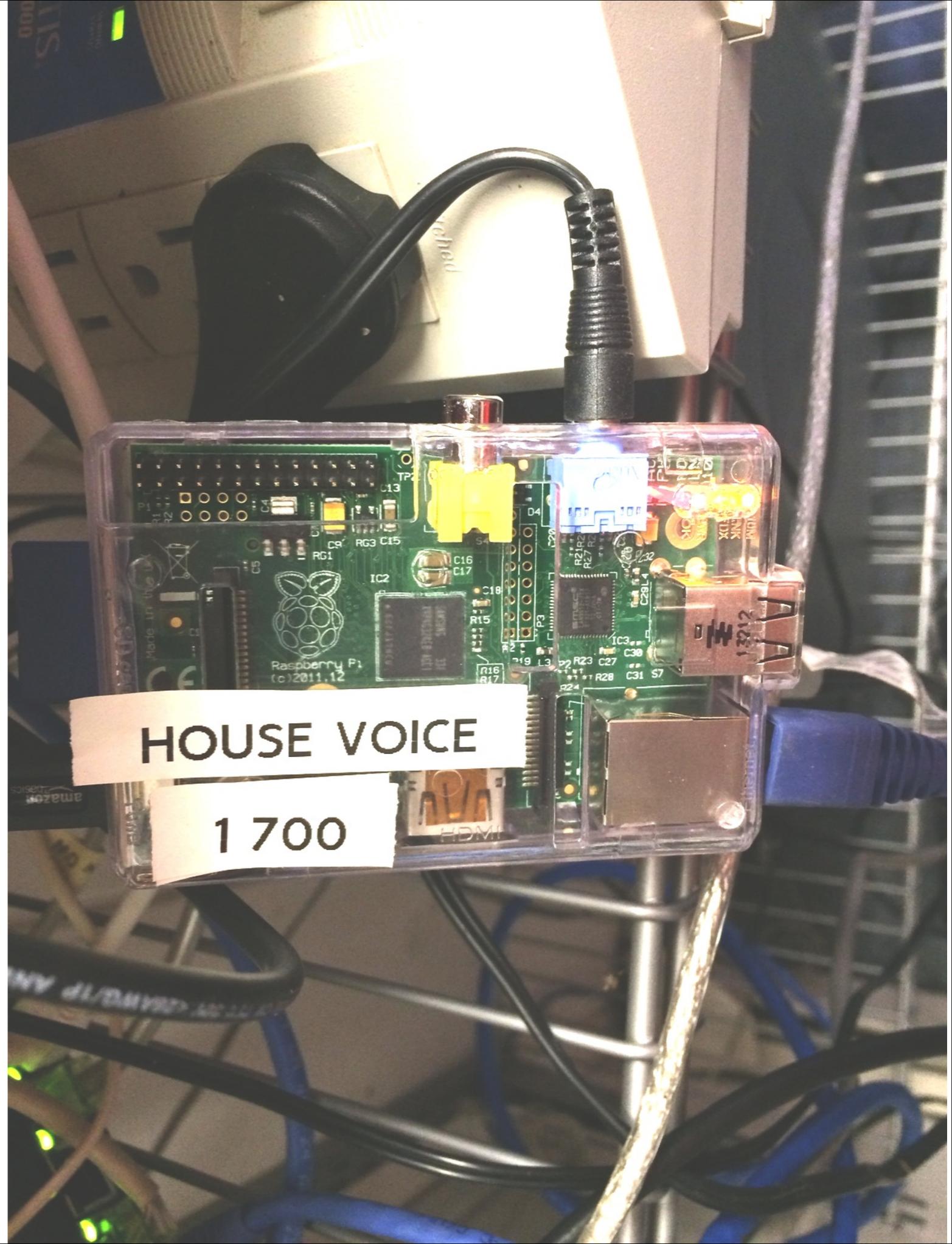
Our digital house

- **Many weekend projects over the past 25 years**
 - lots of pieces, not a clean package
- **Many features have been pleasant or useful over the years**

Equipment: Home intercom



**Equipment:
intercom
connected to
a networked
computer
(now a
Raspberry Pi
running
text-to-
speech)**



Equipment: voice modem connected to computer and landline



X10 controller connected to house wiring and the computer



X10 motion sensors, inside the mailbox and elsewhere



Webcams, wired and wireless



82 of about 93

Other sensors, via X10

- **Garage door position**
- **Water detector under the garage**
- **Circuit detector connected to a hacked smoke detector**
- **Front door bell voice announcement and circuit report**

Features: intercom + computer

- **Morning announcements**
 - weather, news, planets, trash day, recycling day
 - birthday and anniversary reminders
- **Telephone**
 - caller ID announcements, some crank call processing
- **Time/events**
 - Top-of-the-hour chimes (including Big Ben at noon)
 - Dusk, turning on outside lights and Christmas lights
- **Announcements from special email**

Features: intercom + computer

More time/events

- **Garage door open/close**
- **International Space Station passes**
 - interrupts parties
- **Iridium flares**
- **Eclipses and occultations**
- **Stock market results on closing**
- **You have real mail!**

Video monitoring and motion sensing: beehives









Video monitoring: home sweet home



Web services: summary of things

Summary for ches, Wednesday, Mar 19, 10:59
 up 36 days, 25 mins, 1 user, 0.15, 0.14, 0.10

| | M | T | W | T | F | S | S | M | T |
|------------|---|---|---|---|---|---|---|---|---|
| ap | m | m | m | m | m | m | m | m | m |
| ap-w-bw | m | m | m | m | m | m | m | m | m |
| backup | - | - | - | - | - | - | - | - | - |
| backup-h-b | m | m | m | m | m | m | m | m | m |

Tue [Terry is calling](#) 16:5
 917.
 Tue 14:31 925-
 SHE
 Tue 10:59 715
 SU
 Tue 10:08 20
 Dorothy wooden leg is
 calling
 noc

| | | | |
|----------------------|-----------------|-------|---|
| aapl | 534 | 1,118 | : |
| goog | 1204 | 1,358 | : |
| srcl | 116 | 440 | : |
| amzn | 375 | 2,013 | : |
| bcpc | 55 ⁴ | 1,110 | : |
| amba | 29 ⁰ | 3,073 | : |

ANTHONY STAZZONI

Today A chance of sprinkles before 1pm, then a slight c
 precipitation is 30%. Little or no snow accumulation exp
 Tonight Showers, mainly before 2am. Low around 36.
 Thursday Mostly sunny, with a high near 55. West win
 Thursday Night Mostly clear, with a low around 25. We
 Friday Sunny, with a high near 51. West wind 7 to 14
 Friday Night A slight chance of rain. Mostly cloudy, wi
 Saturday A chance of rain. Mostly cloudy with a high

Summary

- **It has enriched our lives**
- **We miss it when we are in a vacation home**
- **This is not an easy package to assemble and sell**
- **Microsoft standard house?**

Our Digital House

