at&t

Rethinking Passwords

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

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

- User IDs must be 7-20 characters
- User IDs must contain at least one letter; numbers are allowed, but not required
- User IDs cannot contain spaces
- User IDs cannot contain your Social Security Number, Tax Identification Number, or your Customer Access Number
- No special characters are allowed, such as: ! @ # $ % ^ &
- Use of an underscore is allowed but not required: _
- Do not use your Password as your User ID

Password:

- 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**).

AT&T (Uverse)

1. Passwords are case sensitive.
2. Passwords must be 6-24 characters long.
3. Password characters must be alphanumeric.
4. Password must contain at least one alpha character and at least one numeric character.
5. Password cannot match Member ID.
6. Password cannot have any special characters except hyphen (-) and/or underscore (_).
7. Avoid using personal information, such as name, birth date or ZIP code.

AT&T Global Network Services

Passwords can contain alpha or numeric characters (No special characters).
A password must begin with an alphabetic character.
Passwords are a minimum of 5 characters and a maximum of 8 characters.
You may not reuse a password for six months.
Passwords are not case sensitive.

Note: **Your password will expire every 60 days**.

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 !"#$%.**

DHS

- 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

at&t

CalNet passphrases

1. A minimum length of 9 characters (maximum 255). It may also include spaces (which is why we call it a pass*phrase*).
2. It must contain characters from at least three of the following four character groups:
   a. English uppercase (A through Z)
   b. English lowercase (a through z)
   c. numeric digits (0 through 9)
   d. non-alphanumeric characters (such as !, $, #, or %)
3. Without regard to case, the passphrase may not contain your first name, middle name, last name, or your CalNet ID itself if any of these are three characters or longer.
4. Any time you change your passphrase, the new one may not be the same as the current or previous passphrase.

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.

	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		
Dart-mouth	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						

I’m thinking we need an ANSI/ISO standard for passwords!

Use A Different Password on each Target System

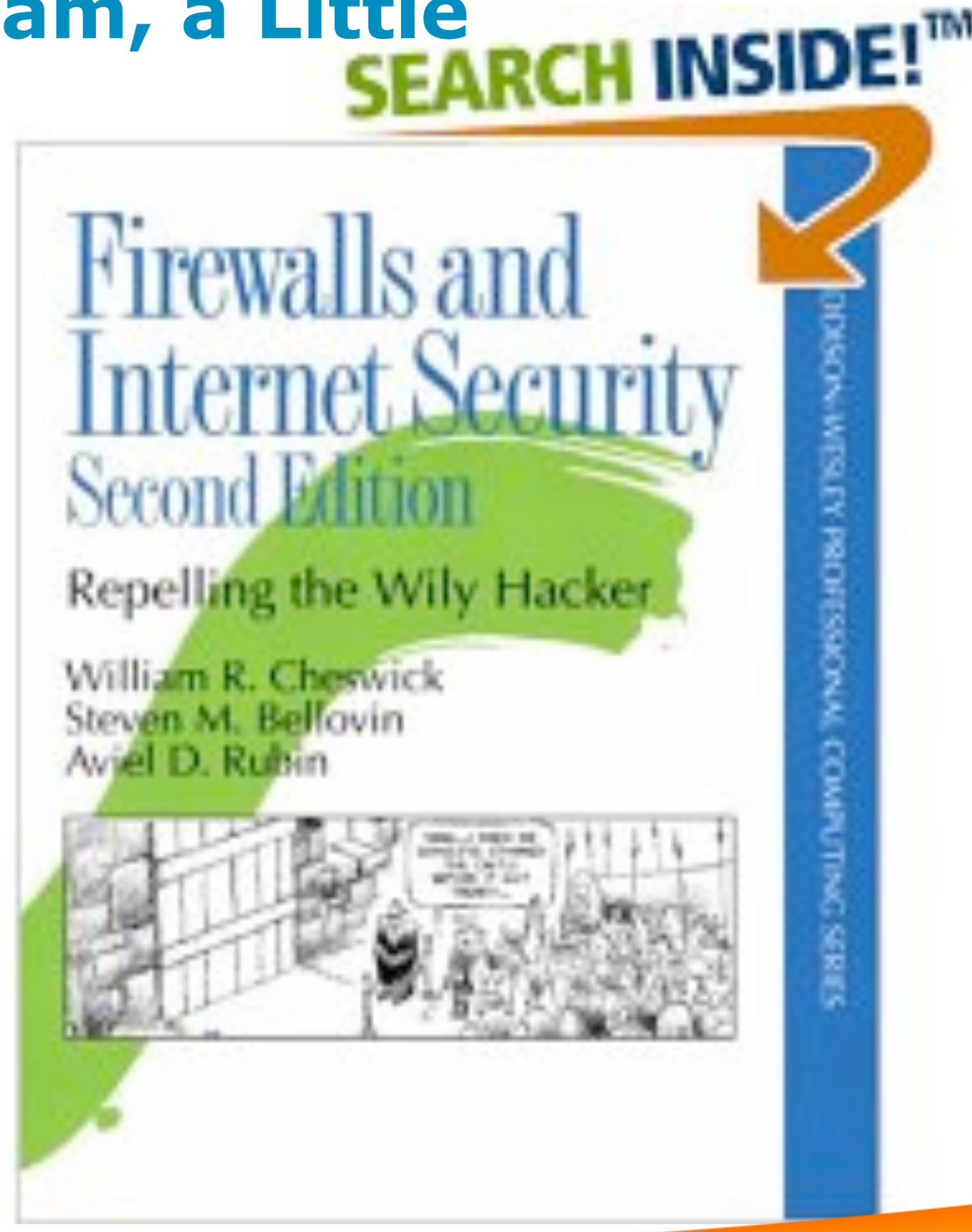
Change Your Password Frequently

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?

- **The users need to know, because rules that make sense increase compliance**
- **A marine guarding nuclear weapons knows why his job is important**
- **Grandma doesn't understand why her password isn't a word, it's a trial**

A Short Excerpt From a 1950s Security Training Film

If you let Hassan guess long enough, he's going to get it right

- **We tried to make it harder to guess, because computers are doing the guessing, and they can make *lots* of them**
  - **And Moore's law just makes computers better guessers**
- **If you limit the guesses, this game goes away**
  - **but we play it any way**

We knew that people are lousy at picking passwords by 1990 (actually much earlier)

- **Klein, D. V.; *Foiling the Cracker; A Survey of, and Improvements to Unix Password Security*, Proceedings of the United Kingdom Unix User's Group, London, July 1990.**

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?**

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**

What are the most common current threats

- **Keystroke loggers**
- **Phishing attacks**
- **Password database compromise**

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**

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

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

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**

A note on Grandma

Another Solution: Don’t allow common passwords

Popularity* is *Everything

Stuart Schechter, Cormac Herley, Michael Mitzenmacher;

HOTSEC 2010.

Count and limit password choices

- **I.E. only 100 people (out of a million?) may use *password* as a password**
- **Makes the dictionary attack much harder: common targets vanish**
- **Makes passwords harder to choose, like picking a gmail account name: *dragonslayer6478***

Summary solution

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

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**

We need research on account locking

- **Not studied much in the open literature**
- **Practitioners could contribute:**
  - **what does a lost password cost?**
  - **how long will a user wait for an unlock?**

Better Solutions

Getting out of the game

SecureNet Key SNK-004

A login from my distant past

RISC/os (inet)

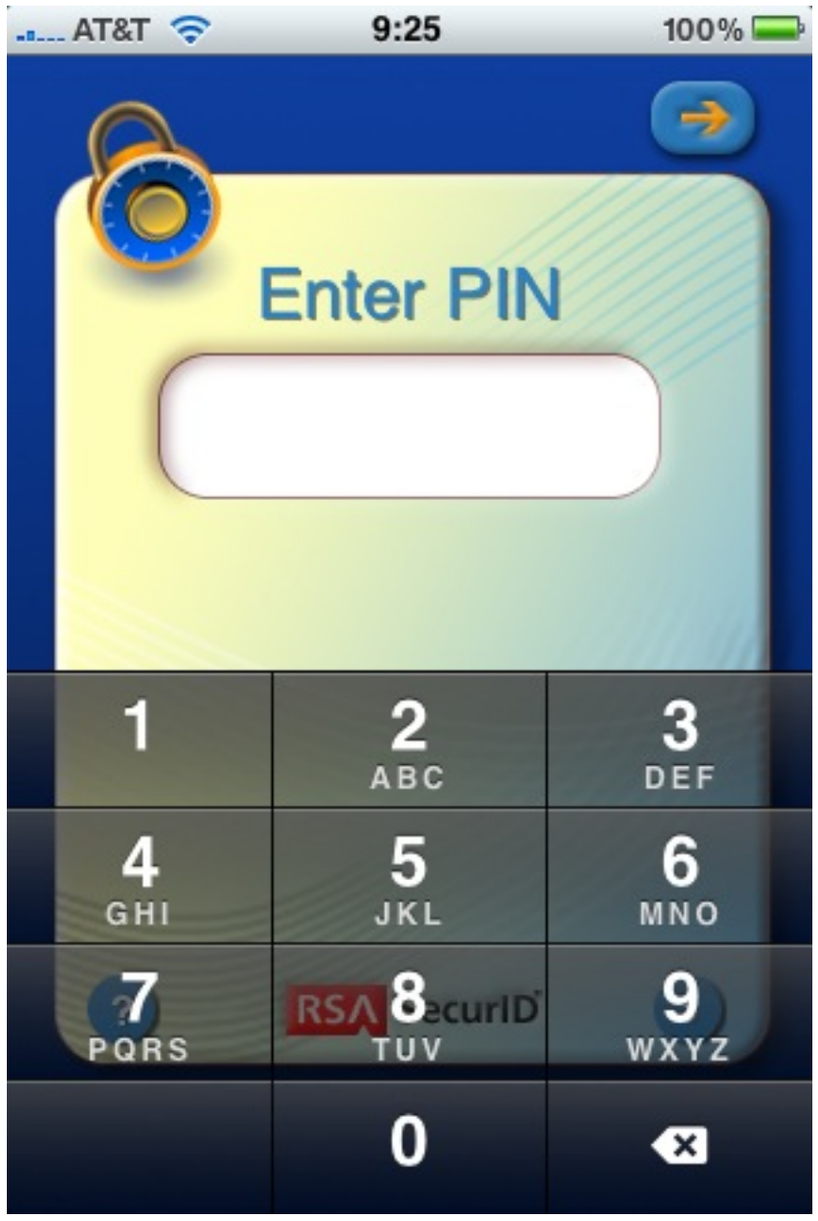
Authentication Server.

Id? ches
Enter response code for 70202: 04432234

Destination? cetus
$

SecureID

RSA Softkey


AT&T
9:25
100%
Enter PIN
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
RSA SecurID


AT&T
9:25
100%
Passcode
8621 1490
27 sec remaining
RSA SecurID

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**

Still Want Your Strong Passwords?

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

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

A Very Short Course on Entropy

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 = 10bits (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, our two words

- **“example early”**

Good stuff!

- **The list of words isn't secret**
- **so spelling checker is okay!**
- **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**

If you must, each line has 60 bits of entropy

- value part peter sense some computer
- anxiety materials preparation sample experimental
- bliss rubbery uncial Irish
- 2e3059156c9e378

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?**

Words Are Better Than Eye-of-Newt

- **Much easier to type**
- **Spelling checking (iPhone) is your friend, not enemy**

Uncial

uncial |ˈən sh əl; -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.

www.cheswick.com/insult
(42 bits)

```
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
```

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

Some Password Ideas

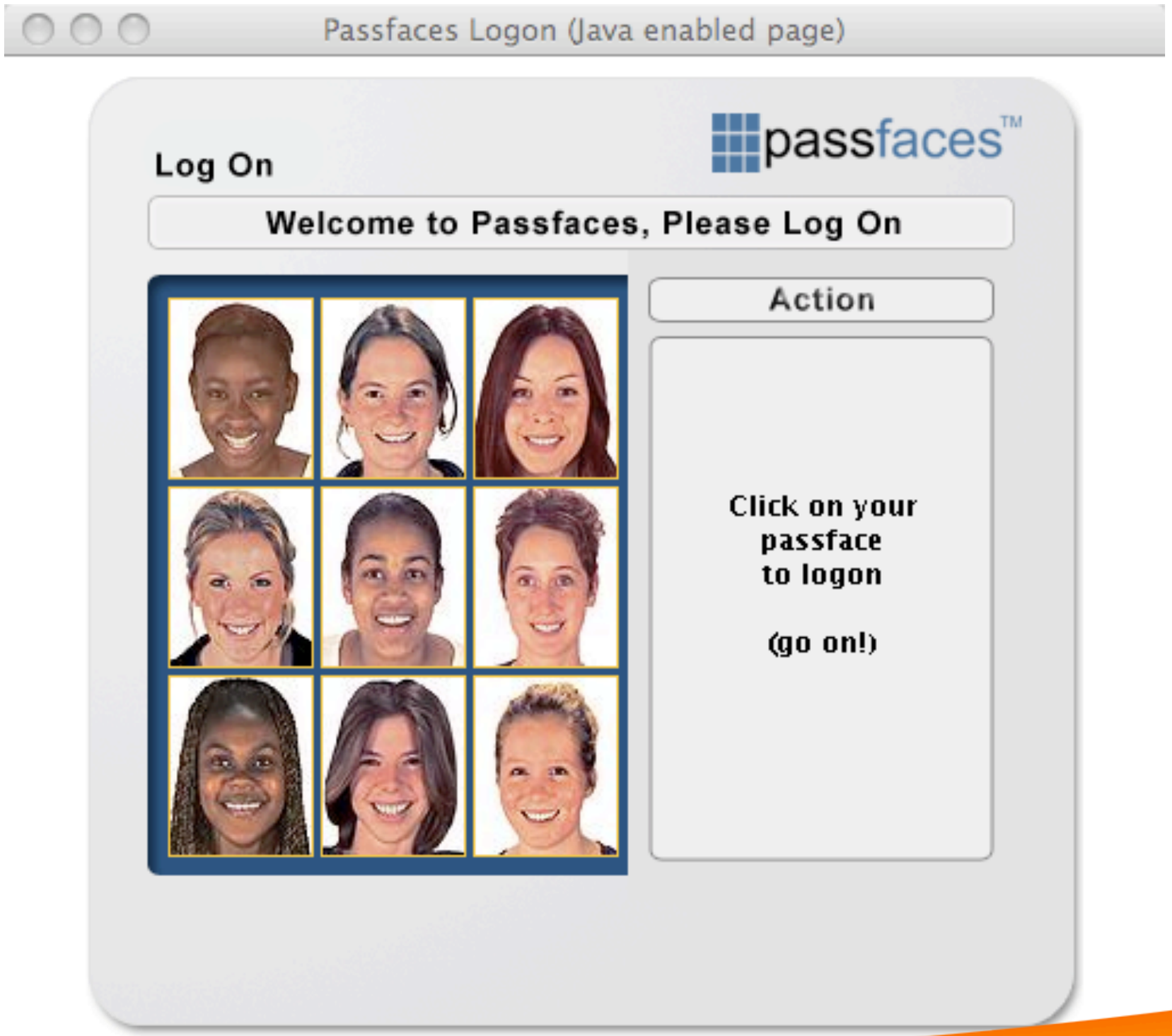
From academia, and me

For a complete survey, see

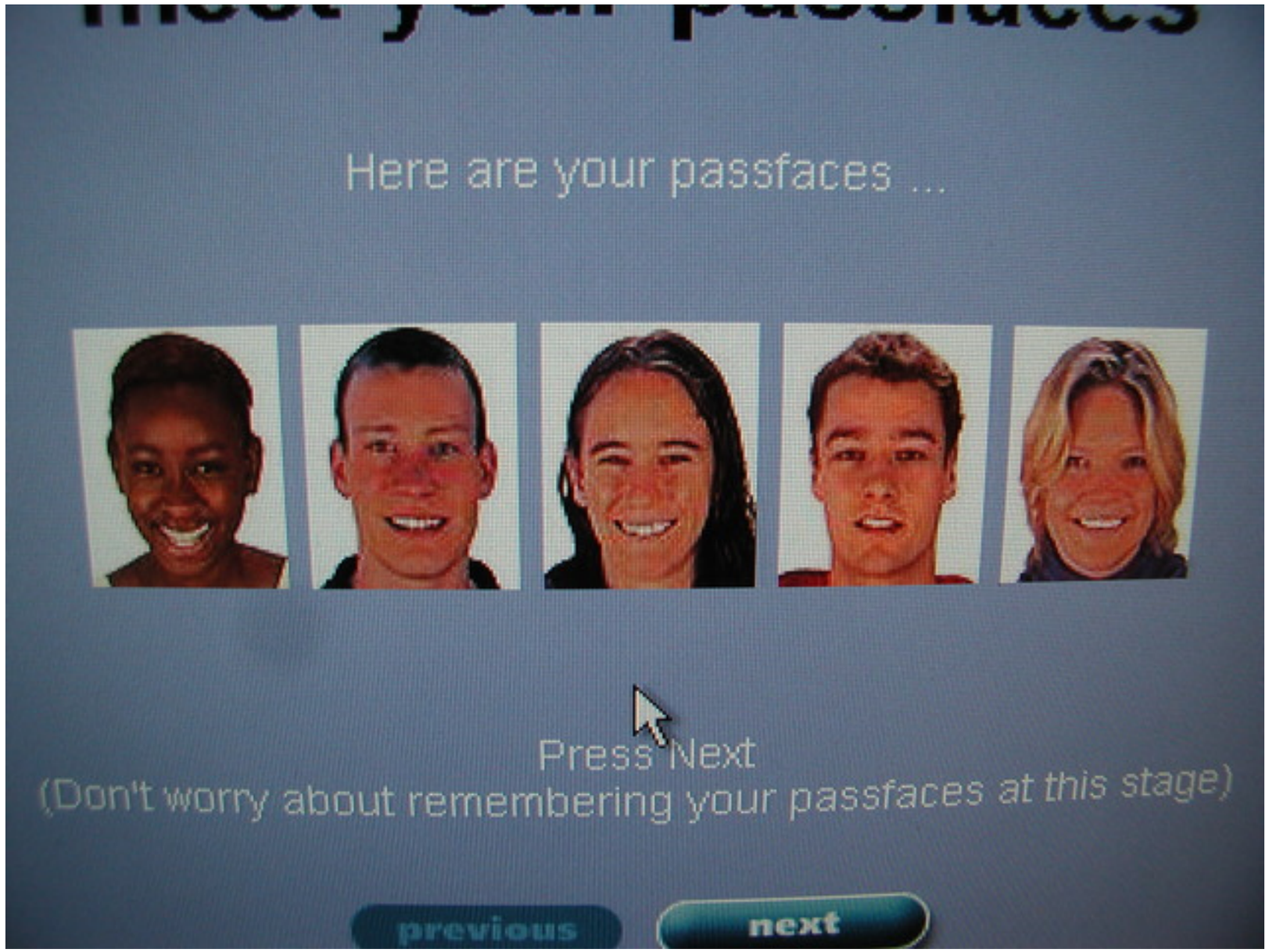
- http://people.scs.carleton.ca/~paulv/papers/gpsurvey-27sept2010.pdf

from *Dirik, Memon, Birget*; SOUPS 2007

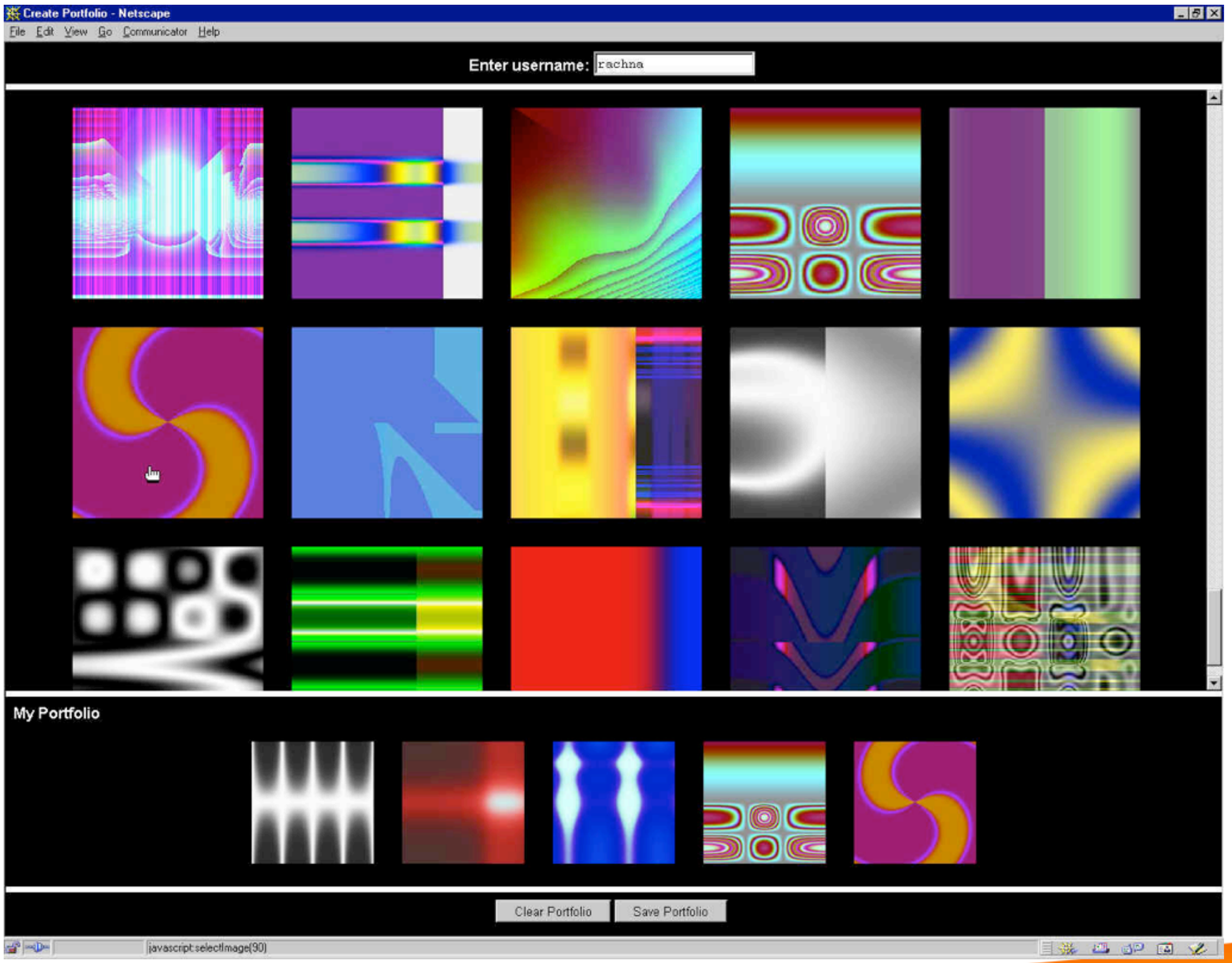
Passfaces


Passfaces Logon (Java enabled page)
Log On
passfaces™
Welcome to Passfaces, Please Log On
Action
Click on your passface to logon
(go on!)

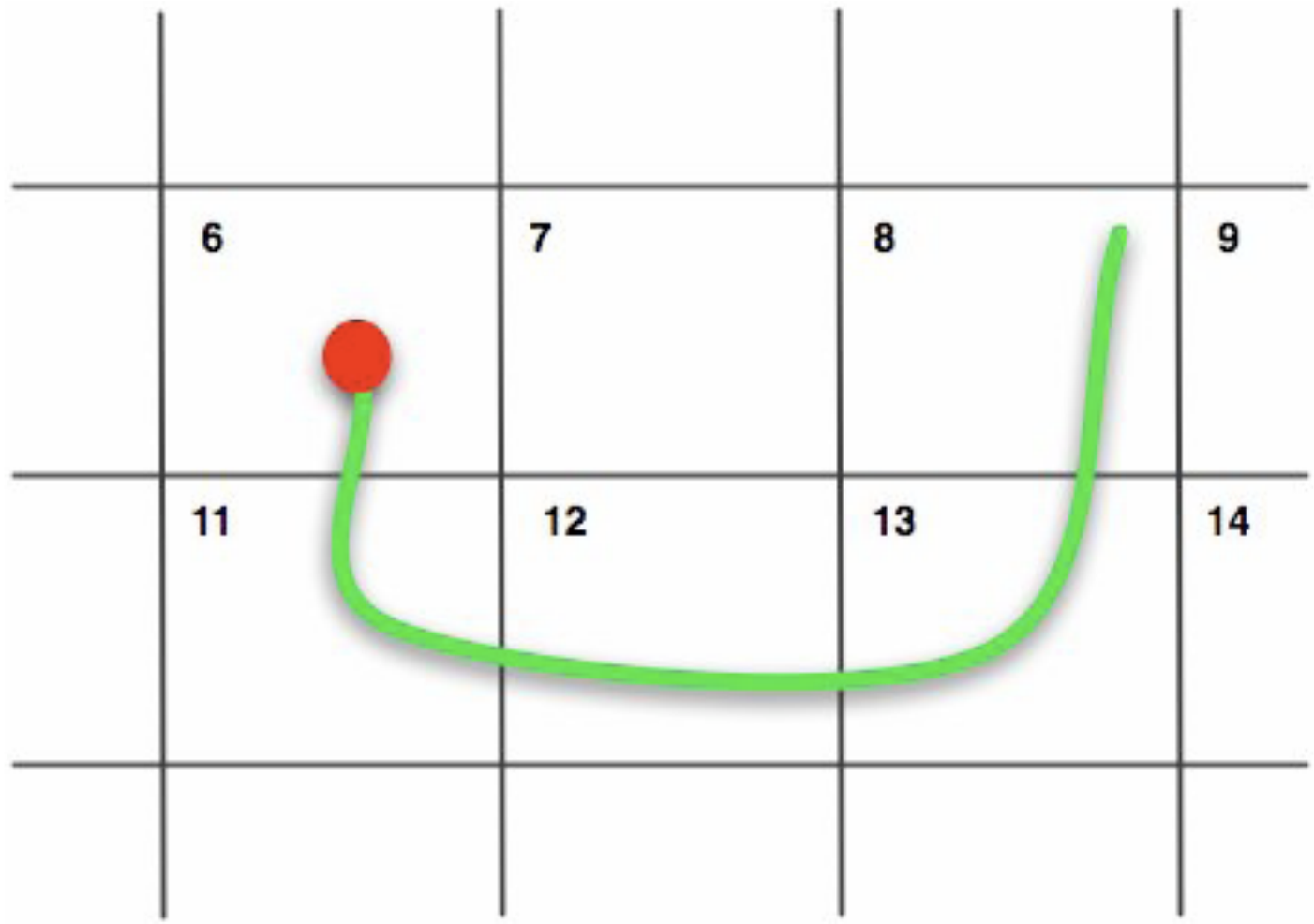
My passfaces



Deja Vu (Recognition-based)



Draw a Secret



Lin, Dunphy, *et al.* SOUPS 2007

Use Your Illusion (SOUPS 2008)

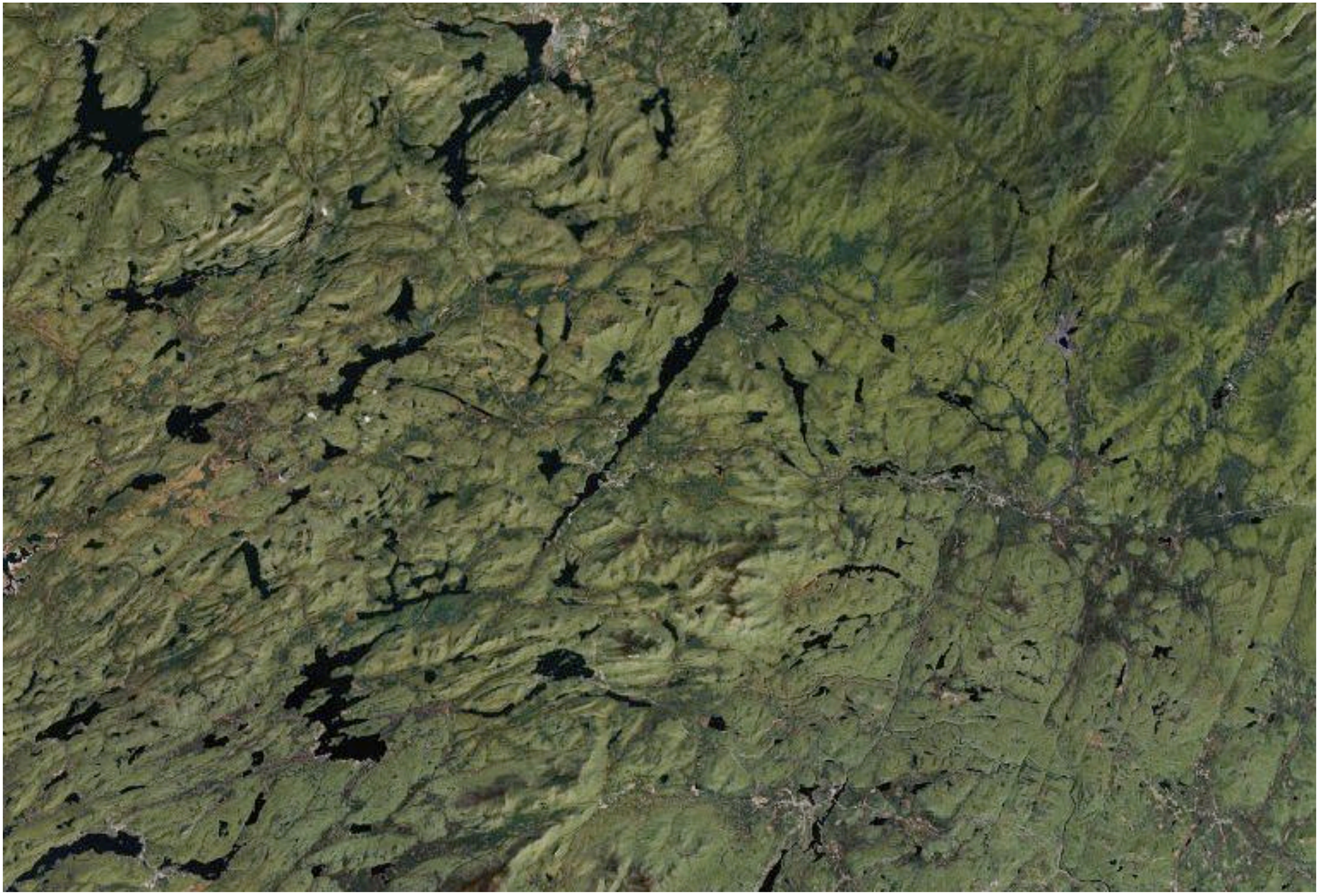
Some Whacko Ideas from ches

Passmaps

TODO: Find a point in New York State
Adirondacks are nice

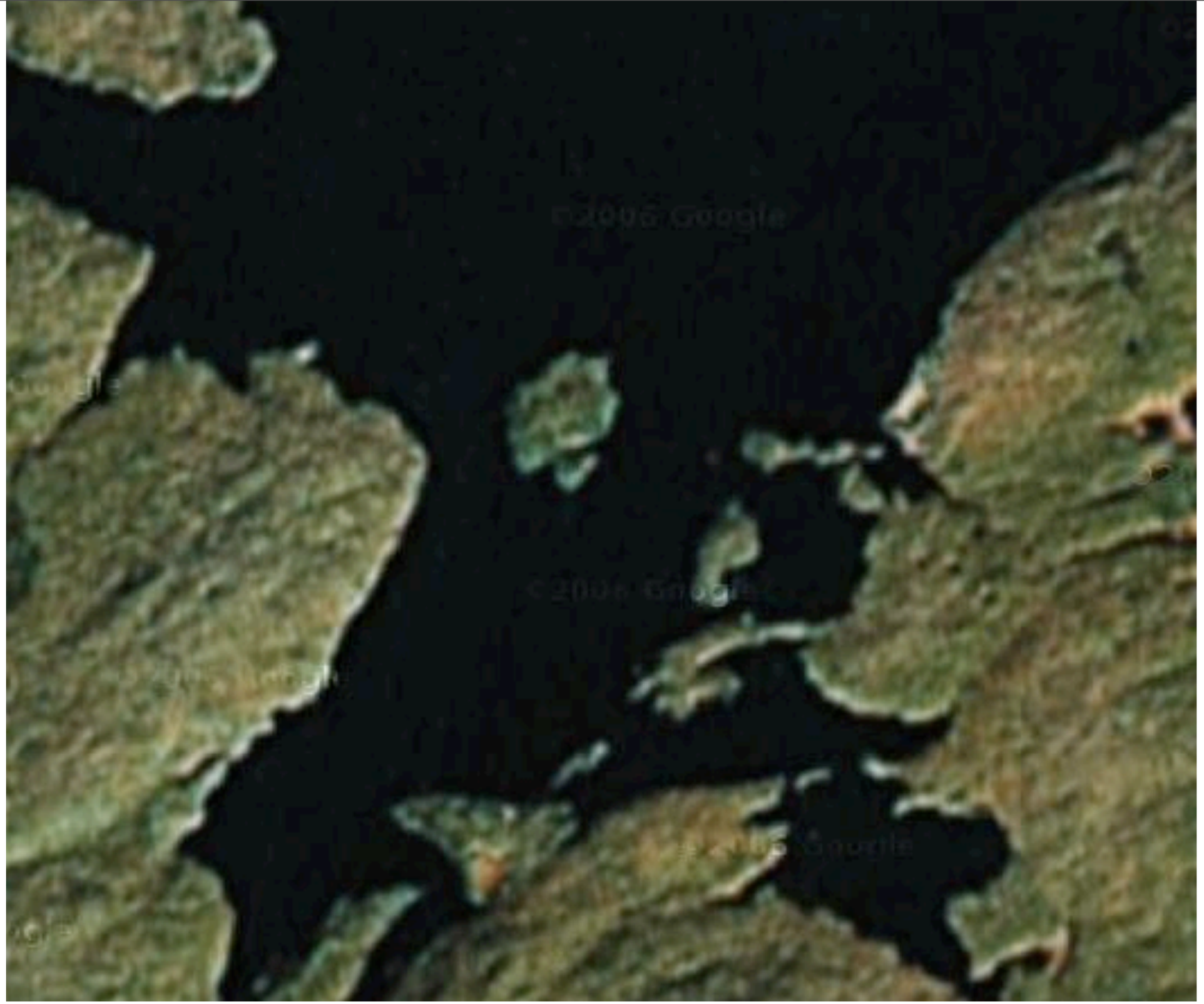

South Dundas
Massena
Malone
56
11
Norwood
Potsdam
Canton
Ogdensburg
11
Gouverneur
3
812
Star Lake
Tupper Lake
3
Saranac Lake
Lake Placid
9N
73
87
Dannemora
Plattsburgh
St Albans
Milton
Peru
Keeseville
Burlington
Jericho
Shelburne
Essex
Hinesburg
Vergennes
Bristol
Middlebury
Adirondack Park
Ticonderoga
Brandon
Rutlan
Whitehall
Fair Haven
Warrensburg
22
Poultney
Lake George
149
Granville
Glens Falls
Hudson Falls
Lowville
Boonville
Rome
90
Utica
Little Falls
Gloversville
29
Saratoga Springs

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

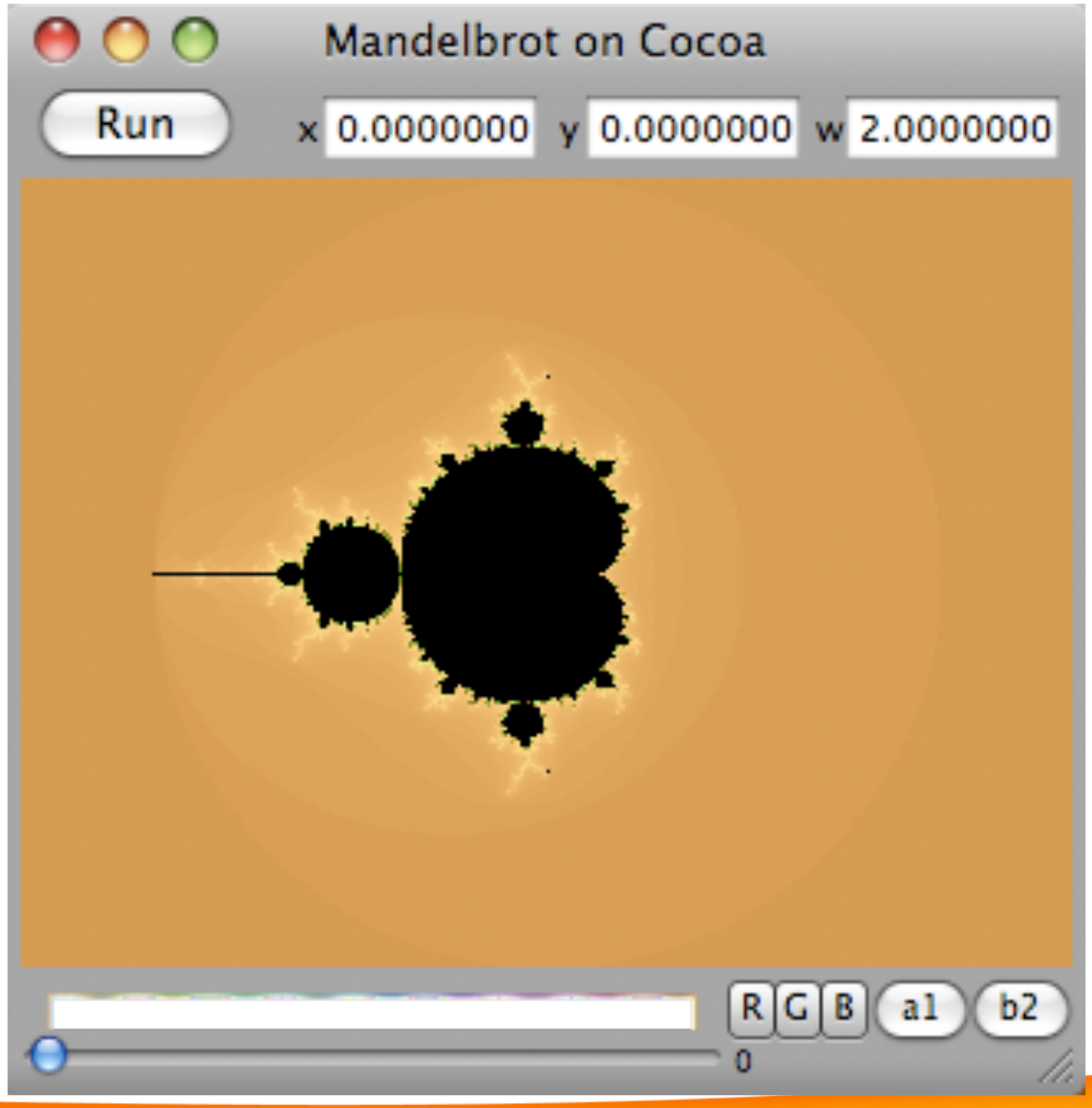
Passmaps?

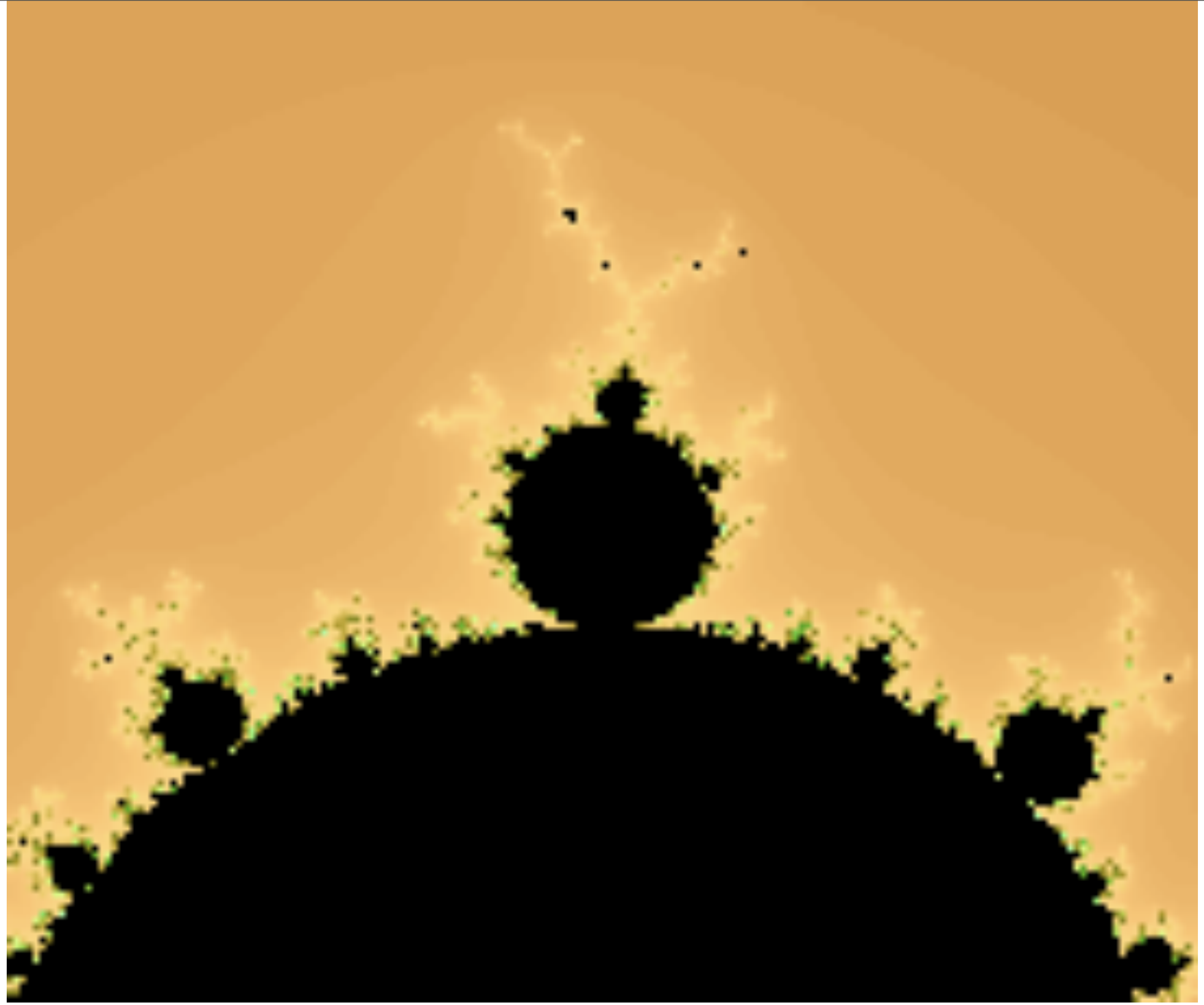
- Reproducibly zoom in on a remembered set of map features?
- Lots of bits
- Maybe hard to shoulder surf
- Not challenge/response
- memorable over a year?
- Nice for a touch screen?

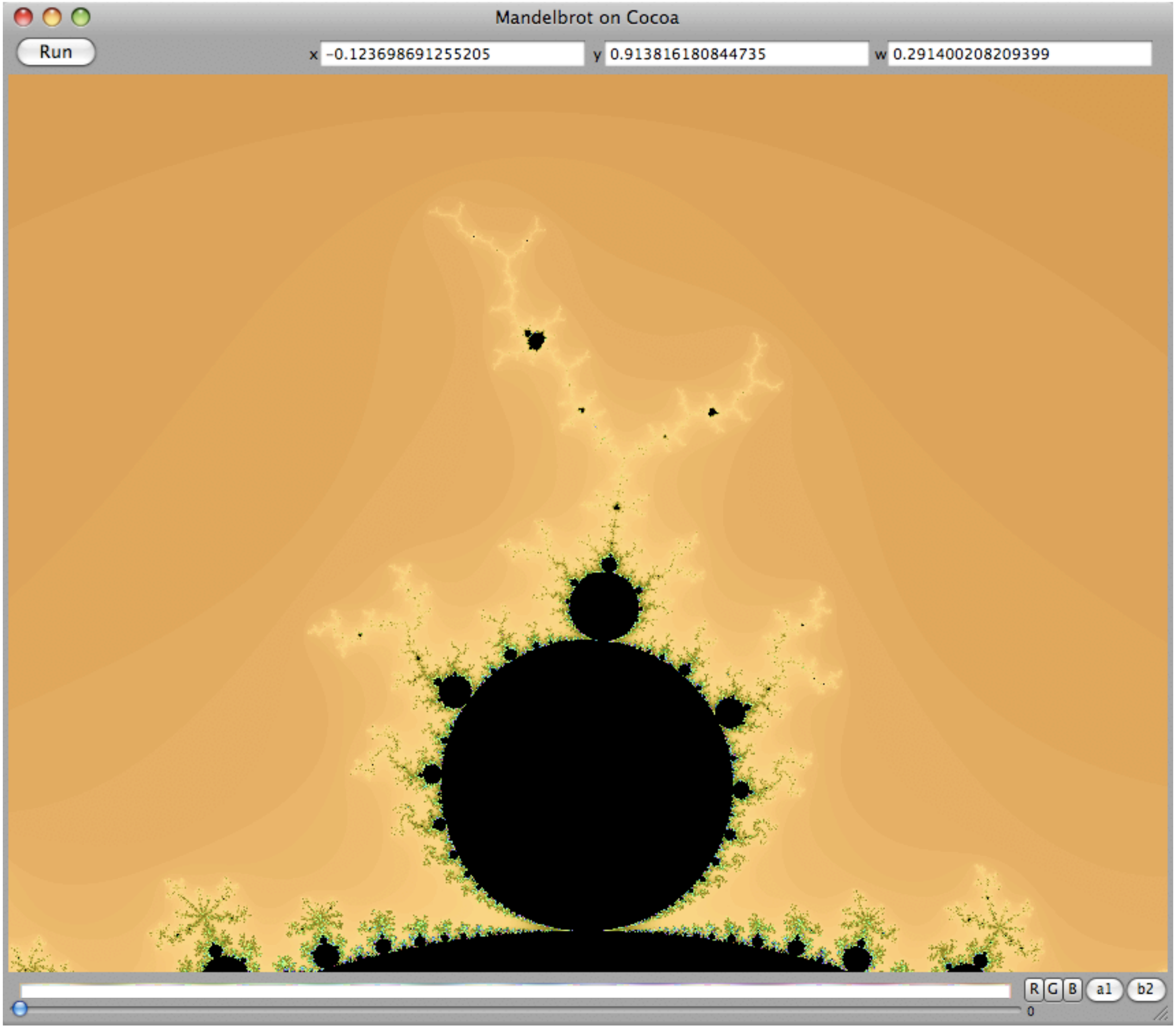
Some Whacko Ches Ideas

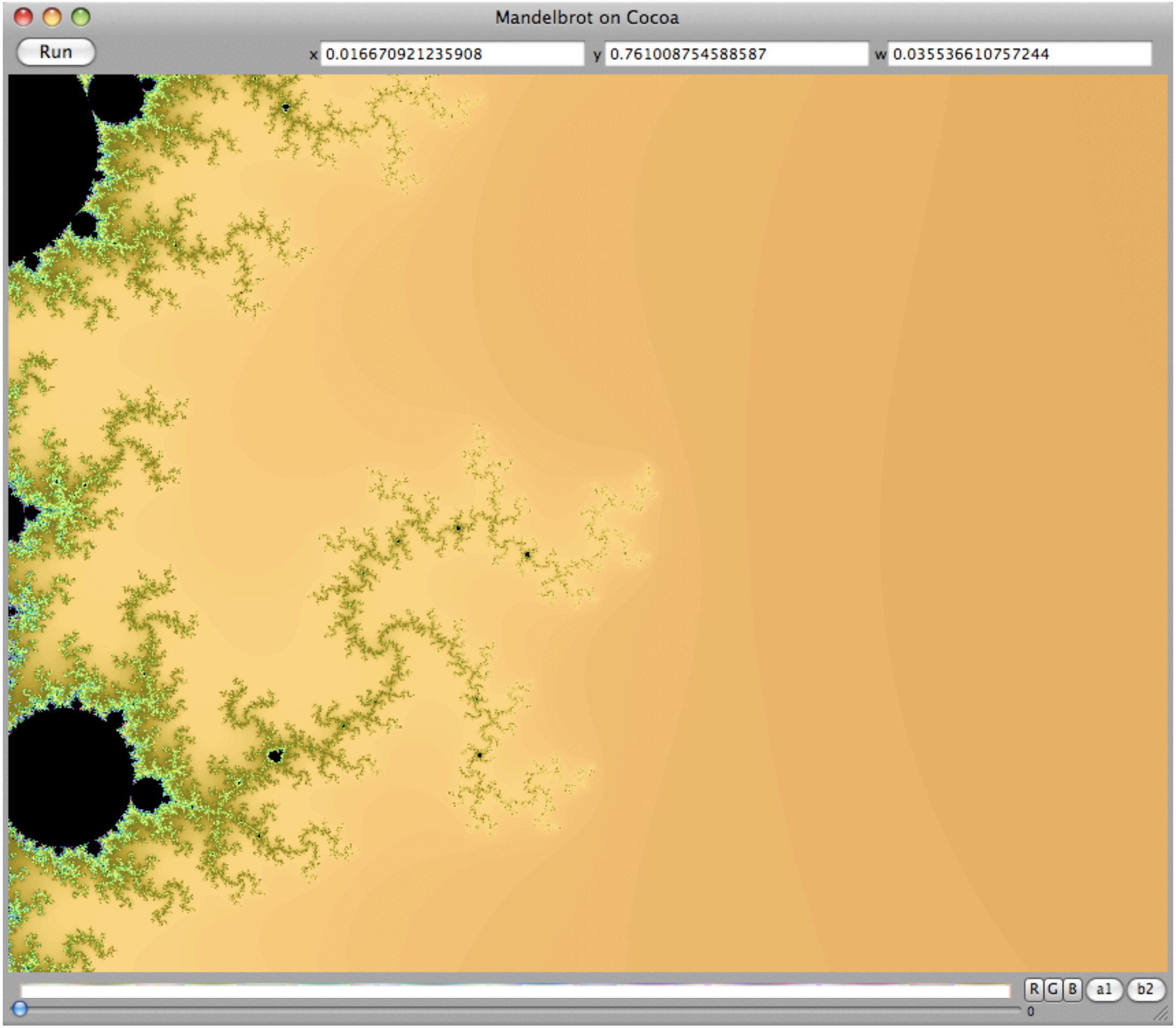
How about passgraphs? Get Google out of the loop

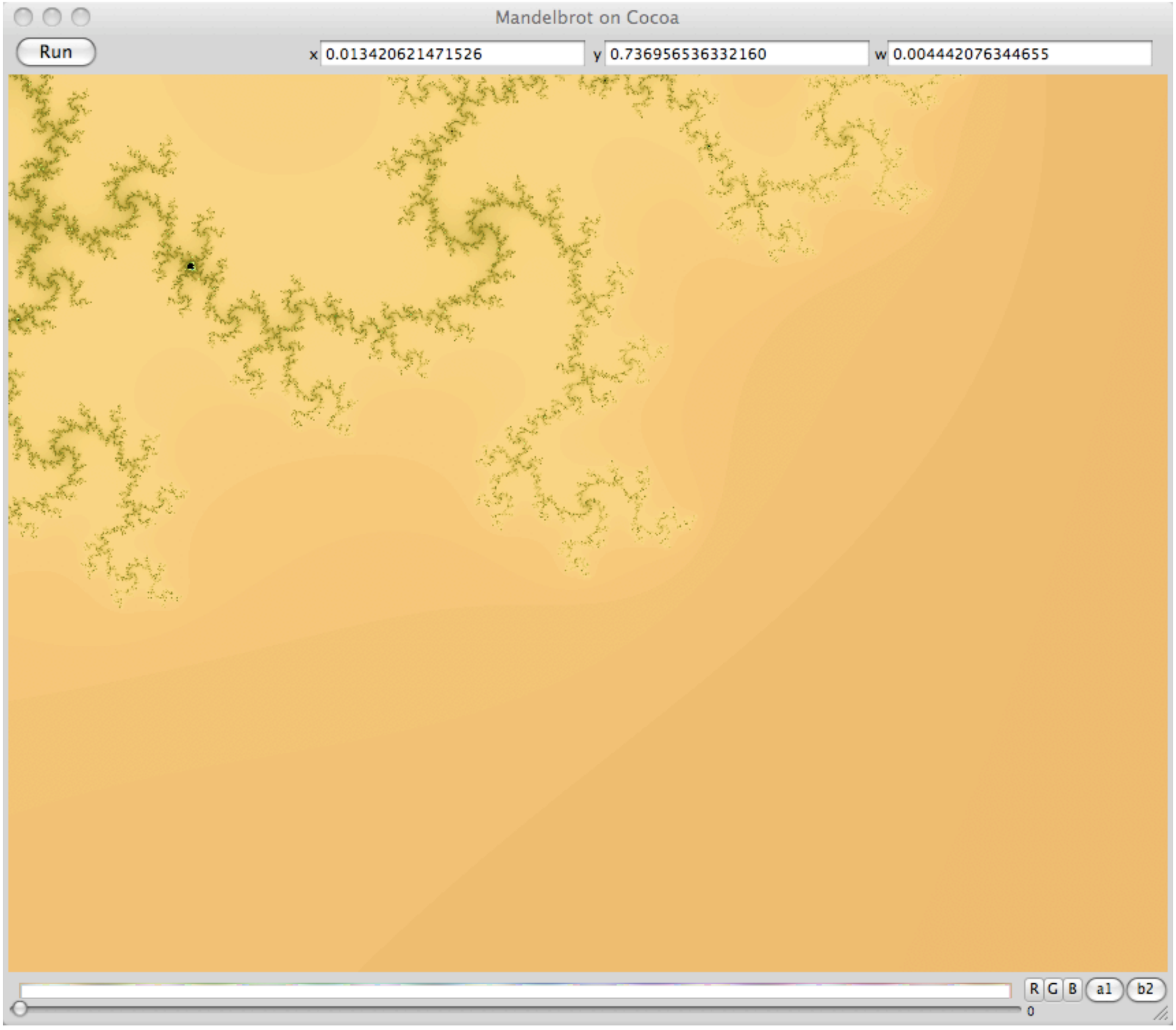
The Mandelbrot Set

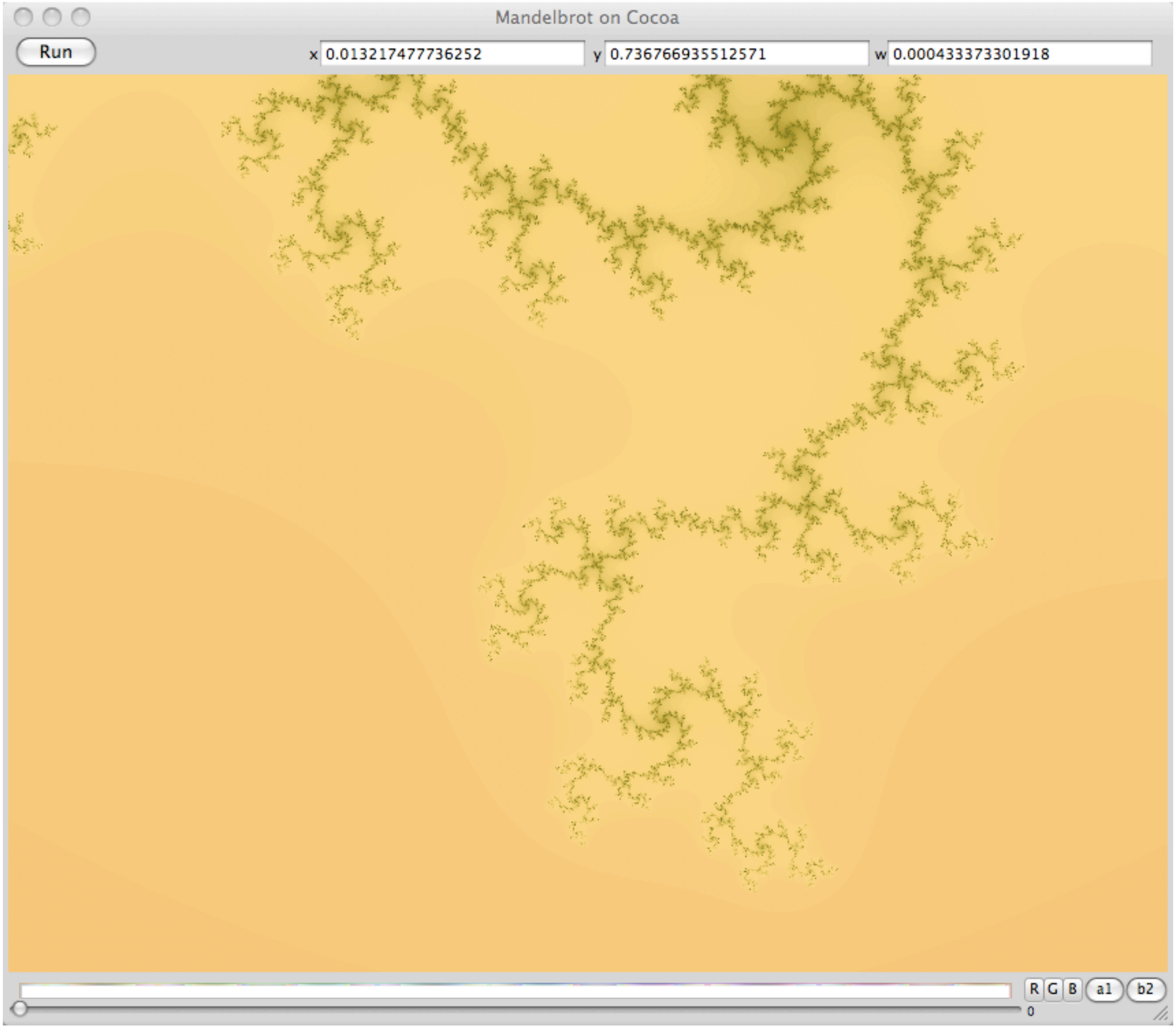


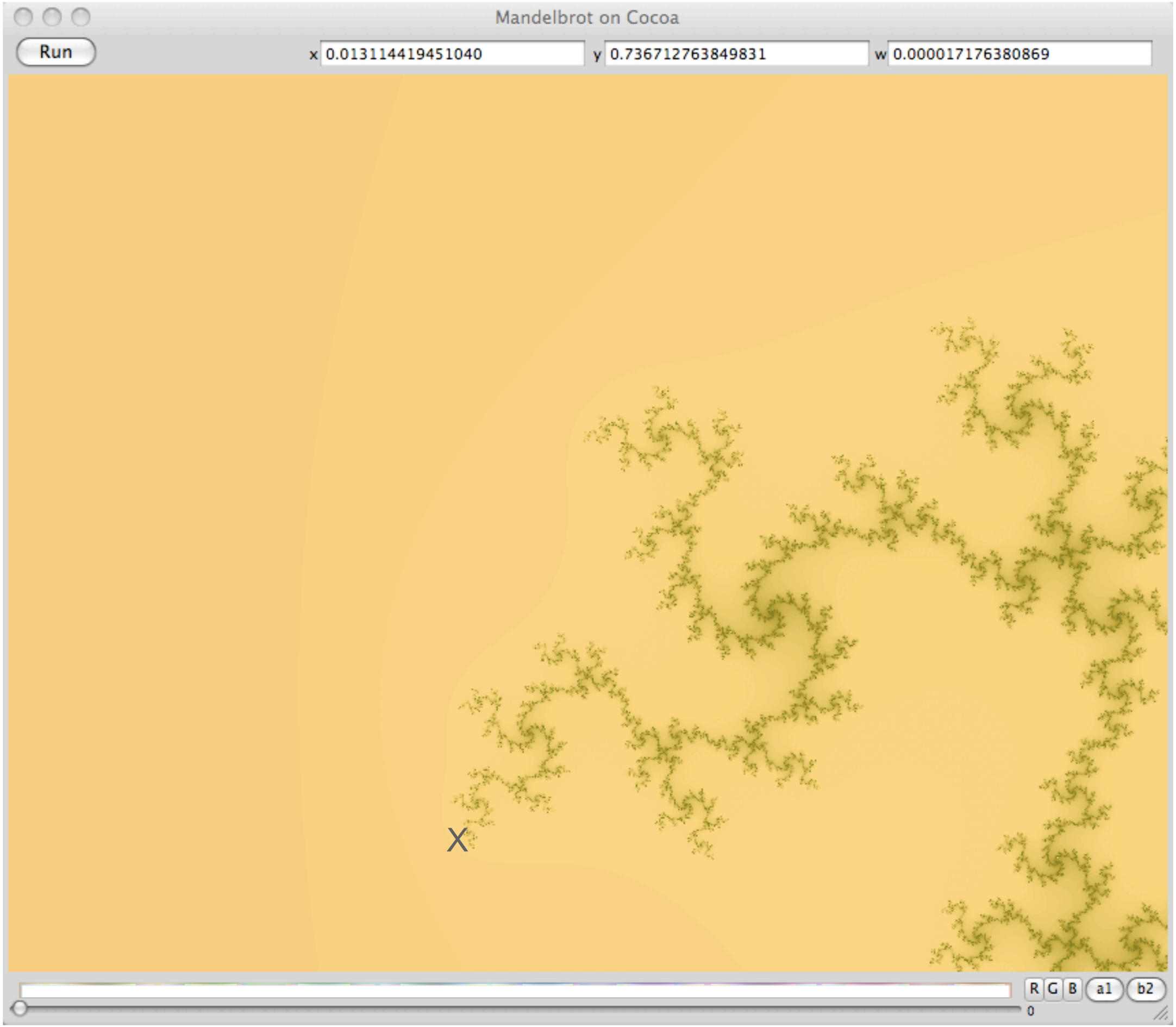



Mandelbrot on Cocoa
Run
x -0.123698691255205
y 0.913816180844735
w 0.291400208209399
R
G
B
a1
b2
0


Mandelbrot on Cocoa
Run
x 0.016670921235908
y 0.761008754588587
w 0.035536610757244
R
G
B
a1
b2
0


Mandelbrot on Cocoa
Run
x 0.013420621471526
y 0.736956536332160
w 0.004442076344655
R
G
B
a1
b2
0


Mandelbrot on Cocoa
Run
x 0.013217477736252
y 0.736766935512571
w 0.000433373301918
R
G
B
a1
b2
0


Mandelbrot on Cocoa
Run
x 0.013114419451040
y 0.736712763849831
w 0.000017176380869
R
G
B
a1
b2
0

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**

Thursday, November 11, 2010

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:	Response:	
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/l3kf.l2cxn. 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	/l6k3jdq,	
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	* 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	hbcg3]'d/	
ches 00163 Mon Feb 25 09:24:30 2002	d	* no *
ches 00163 Mon Feb 25 09:24:35 2002	ozhdkf0ey2k/.,vk0l	
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	* 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	

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**

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**

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(?)**

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**

Updated Advice

For Implementors

Out of the Dictionary Attack Game Game

- **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**
- **Avoid strong passwords in most cases**

Use an authentication server

- **Centralizes the security function**
- **Make it strong and robust**
- **Replication is dangerous, reliability is better**
- **Limit authentication attempts**
- ***DO NOT LET IT BE COMPROMISED***

Near-public authentication servers

- OpenID
- Openauth
- The general idea is appealing

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**

Don’t make acct. names 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**

PIN != password

- **A PIN is a sequence of digits only**
- **A password is a superset of PINs**
- **A passphrase is a series of words, but probably should not be called a *phrase*. *Passcode* is probably better**

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**

Use Client certificates to limit attack surface

- **Limiting connections to those with known client certificates gets you mostly out of the game**
- **Many mail clients do not offer client cert. processing, and should**

Yeahbuttal

Yeahbuttal

- **These ideas will take time to deploy, if they do**
- **Huge installed base**
- **Corporate conglomerates have hundreds or thousands of these!**

Yeahbuttal

- **Who owns the app?**
- **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?**

Fix it anyway

- **This is one of those economies of scale you told the shareholders the merger was going to buy**
- **Authentication servers should be relatively simple to code and maintain**
- **If you don't understand who your users are, your security is shot from the start**

Fix it Anyway

- **Annoyed users are uncooperative users**
- **There is a substantial cost when a large community has to deal with authentication foolishness on a routine basis**

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**

Selling weaker passwords

- **ATM PINs of 4 digits work fine**
- **Cut user support costs**
- **Backup passwords are usually weaker**
- **Improve the users' experience**
- **Annoyed users are less cooperative**
- ***Tell them I said it was probably a good idea***

Summary

- **Distribute and require client certificates**
- **Use ssh with pass-phrased locked digital key, never passwords**
- **Use crypto services, like IMAPS, SMTPS**
- **Limit password attempts**

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

There is plenty new to worry about

- **Dangerous browsing**
- **Dangerous patches**
- **Dangerous COTS CPUS?**
- **Hidden malware**
- **The bad guys are pros, not disaffected teenagers**

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.**

at&t

Rethinking Passwords

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