Rethinking Passwords

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

OAG password rules

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

World of Warcraft Wizard Rules

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

United Airlines rules

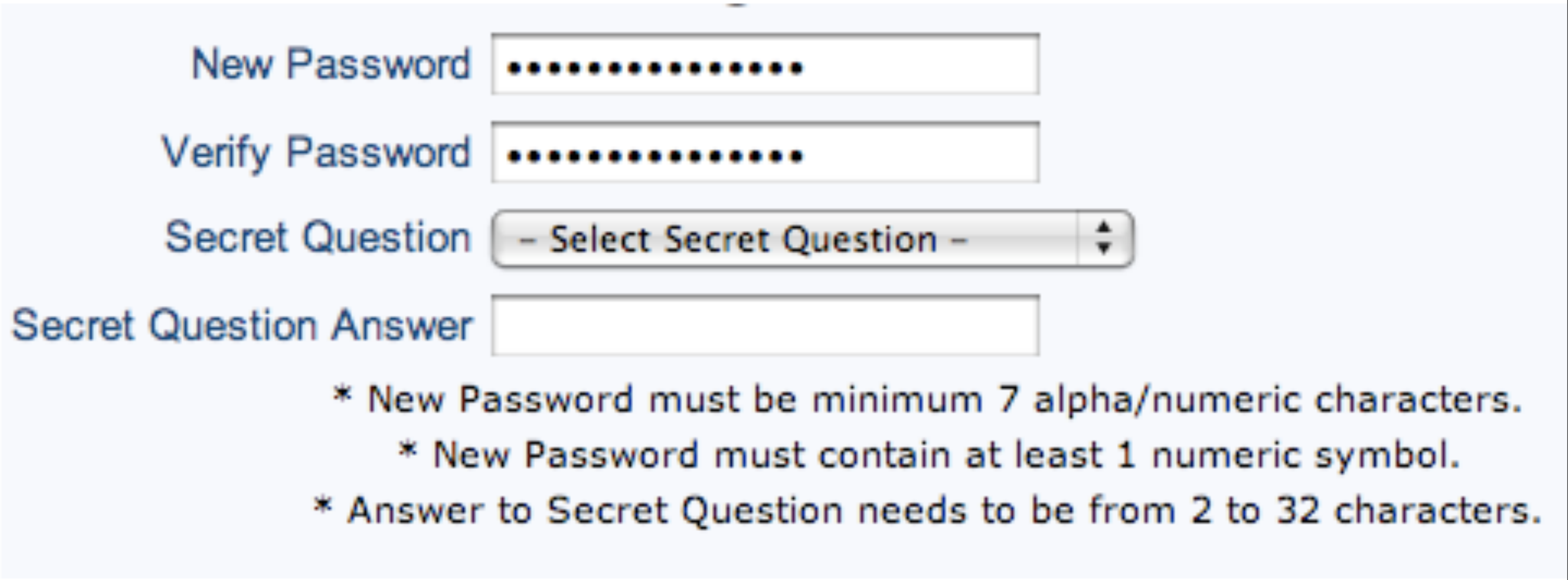
Passwords may be any combination of six (6) characters and are case insensitive.

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

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

Passwords are case insensitive; please remember how it is entered

Minimum password length is six (6) characters and must include characters from at least two (2) of these groups: alpha, number, and special characters.



New Password ••••••••••••••••

Verify Password ••••••••••••••••

Secret Question – Select Secret Question –

Secret Question Answer

* New Password must be minimum 7 alpha/numeric characters.

* New Password must contain at least 1 numeric symbol.

* Answer to Secret Question needs to be from 2 to 32 characters.

Passphrase Rules:

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

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

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

It cannot contain 3 or more consecutive identical characters.

You may NOT reuse any of the last 6 previously used passphrases

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

Use A Different Password on each Target System

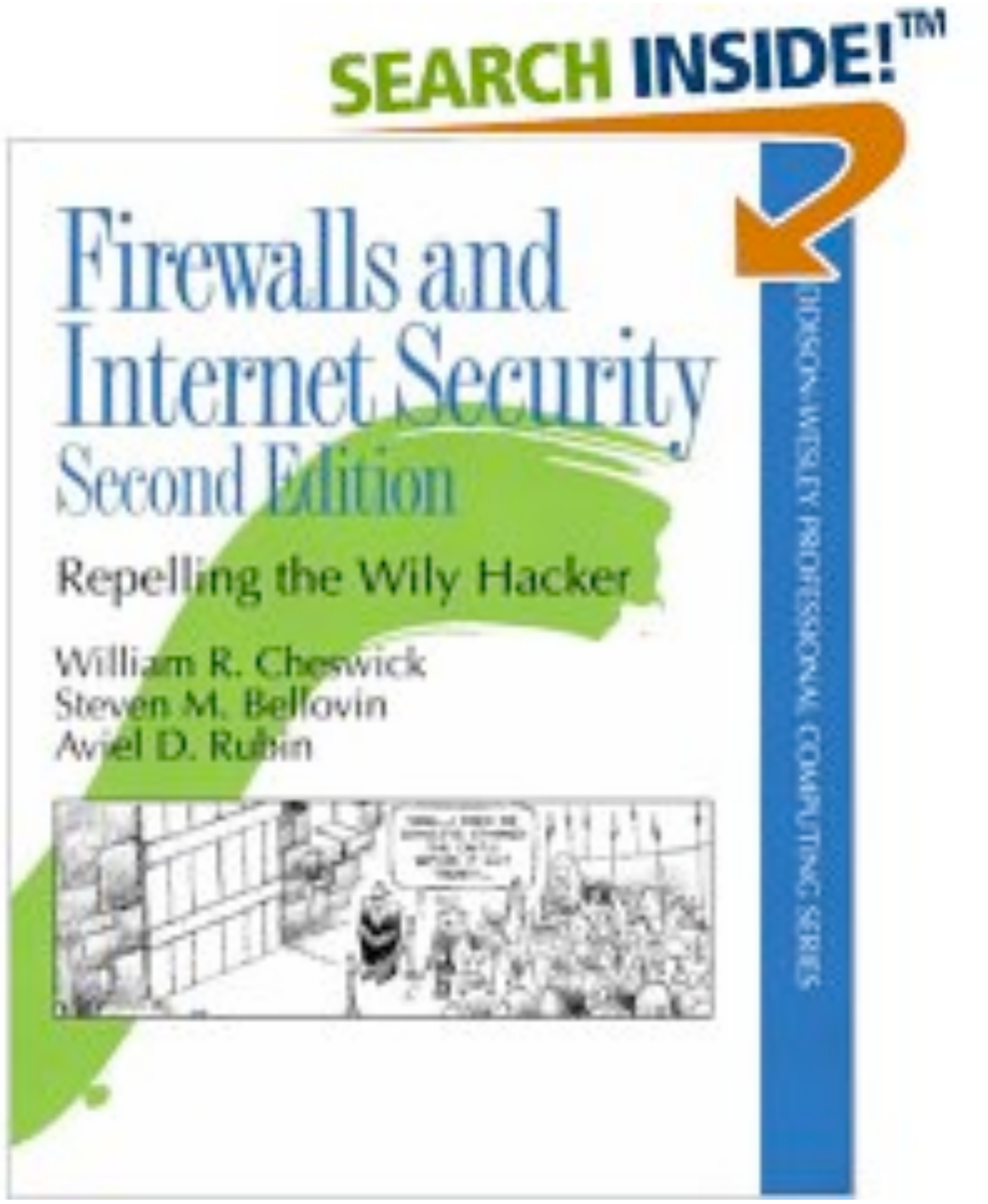
Change Your Password Frequently

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



SEARCH INSIDE!™

Firewalls and Internet Security

Second Edition

Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin
Aviel D. Rubin

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

What are these rules for?

Dictionary Attacks

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?

We Knew People Pick Weak PWs by 1990

- 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.

Old Threats

- Time sharing terminals open to the public
- Early Unix daemons with simple password authentication
- Early Internet protocols, no crypto

The Problem

- 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
  - If brute force doesn't work, use more.

FIPS 112

- *Specification for Password Usage.* (May 1985)
- Based on twenty years of computer experience
  - time sharing
  - minicomputers
  - "Early" in Moore's Law curve

Poor engineering

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

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

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

FIPS 112 complaints

- Maximum password life of one year (3.3.1)
  - But what about accounts we use annually?
- The risk associated with an undetected compromise of a password can be minimized by frequent change --- Appendix 3.3

Poor engineering

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

Poor engineering

- To change passwords often. Strong passwords are hard to generate.
- To allow dictionary attacks
- To protect most important systems with single-factor authentication

Poor engineering

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

Poor security

- Passwords should not be shared.
- Select a password not related to the user’s identity, history, or environment (3.4.4)

We Need New Rules, or at Least Need to Reevaluate our Authentication Systems

Password Properties

- Memorable?
  - Daily, monthly, yearly?
  - Cost if forgotten
- Hardware needed?
- Training steps needed
- User selected?

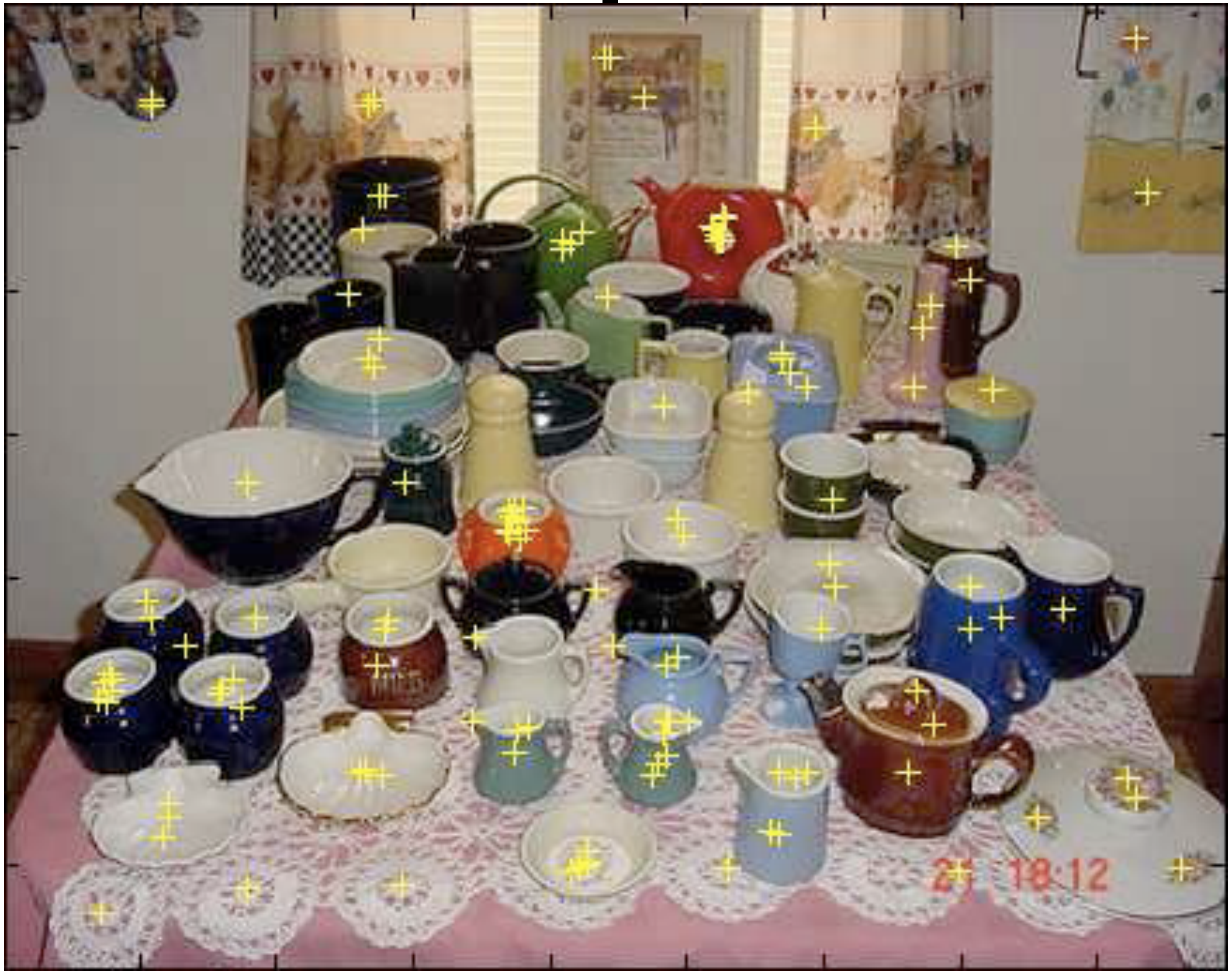
- Single use?
- Changeabe?
- Easy to write down?
- Easy to describe or transmit?
- Authentication speed
- Text, graphical, bio, other

Password properties

- Value of system accessed
- Attempts limited?
- Susceptible to dictionary attack
- Susceptible to eavesdropping?
- Susceptible to replay?
- Susceptible to shoulder surfing?

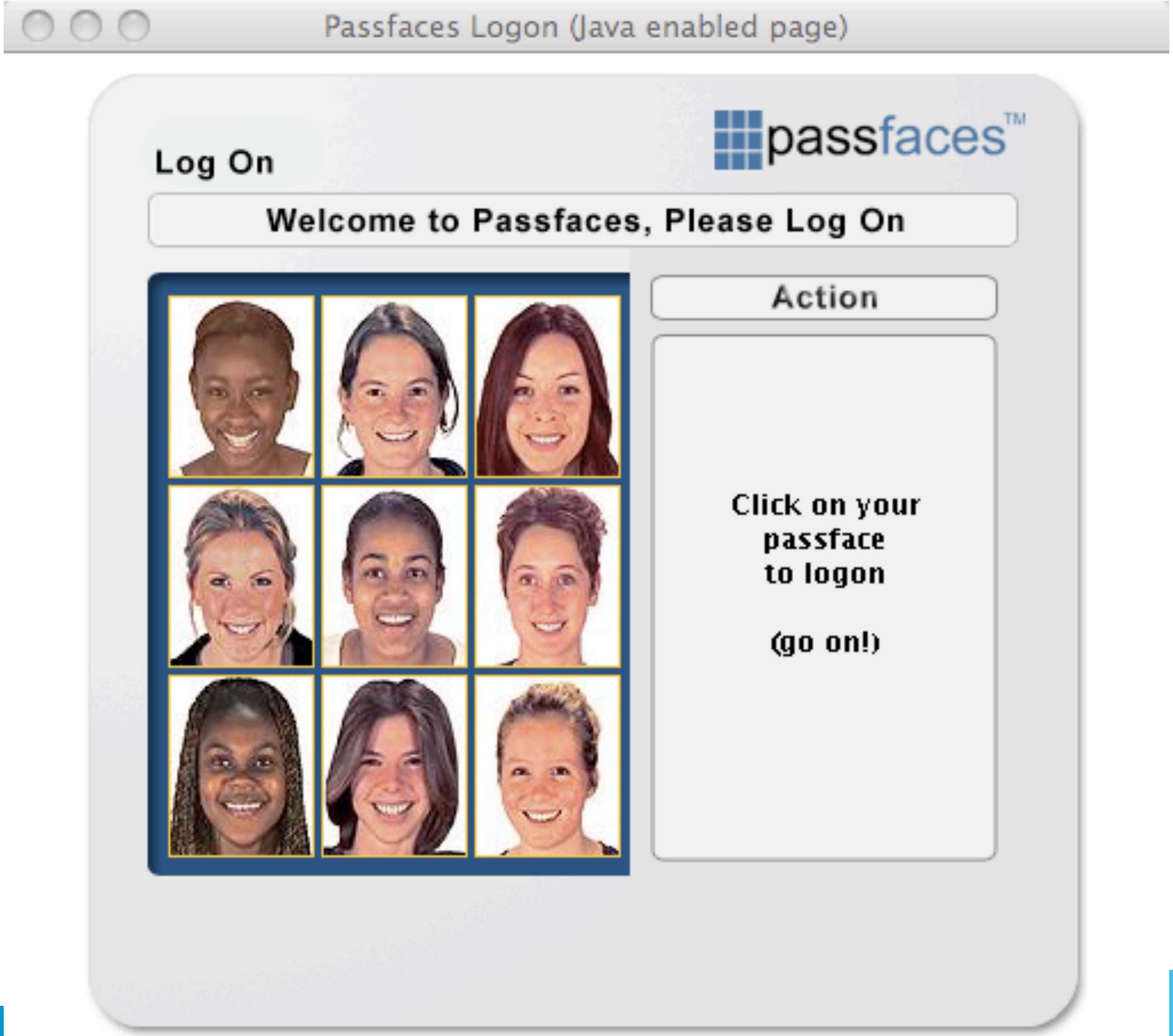
Some Graphical Solutions

Passpoints



from *Dirik, Memon, Birget*; SOUPS 2007

Passfaces



Passfaces Logon (Java enabled page)

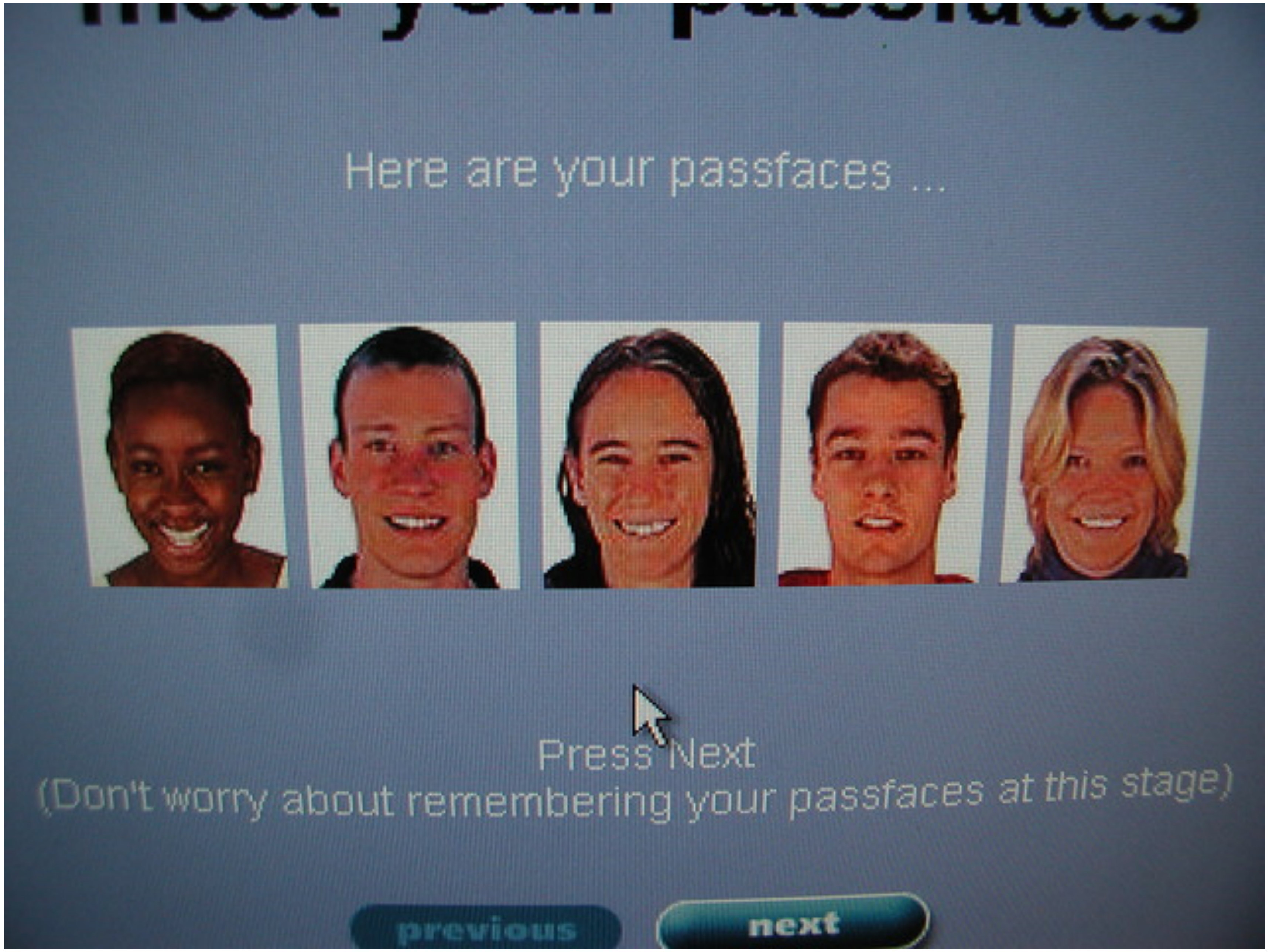
Log On

Welcome to Passfaces, Please Log On

Click on your
passface
to logon

(go on!)

Passfaces

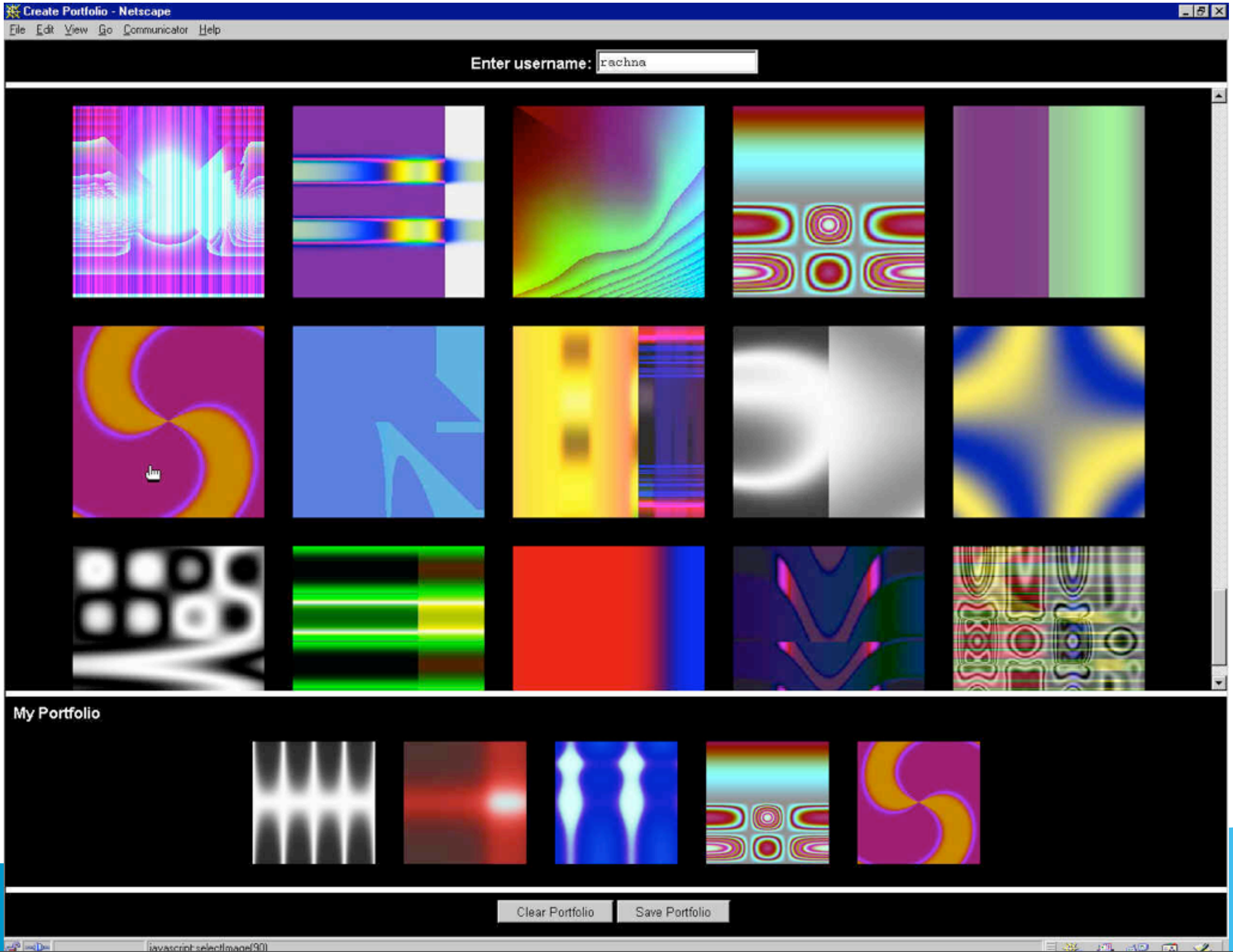


meet your passfaces

Here are your passfaces ...

Press Next
(Don't worry about remembering your passfaces at this stage)

Deja Vu (Recognition-based)



Create Portfolio - Netscape

Enter username: rachna

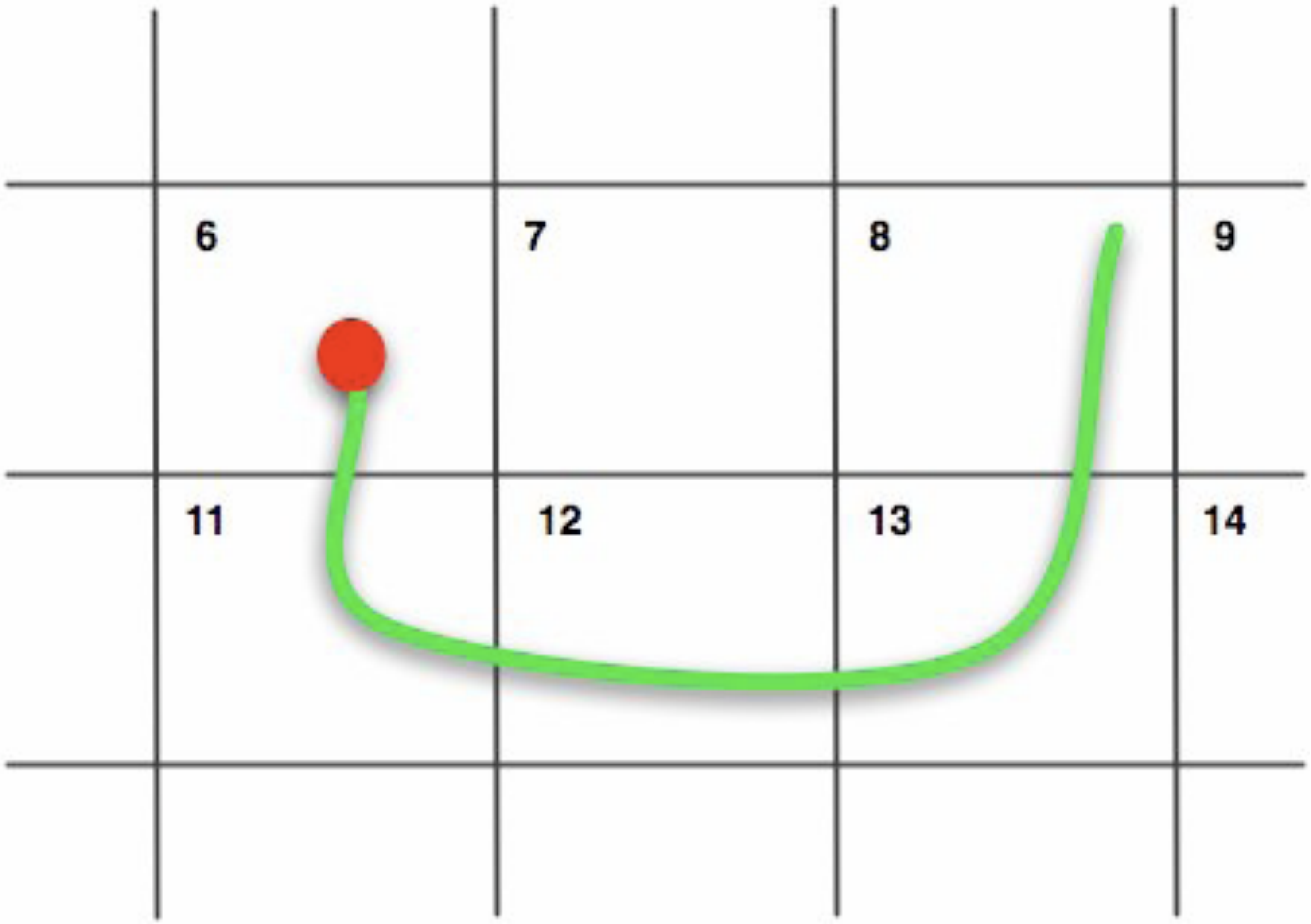
My Portfolio

javascript:selectImage(90)

Deja Vu

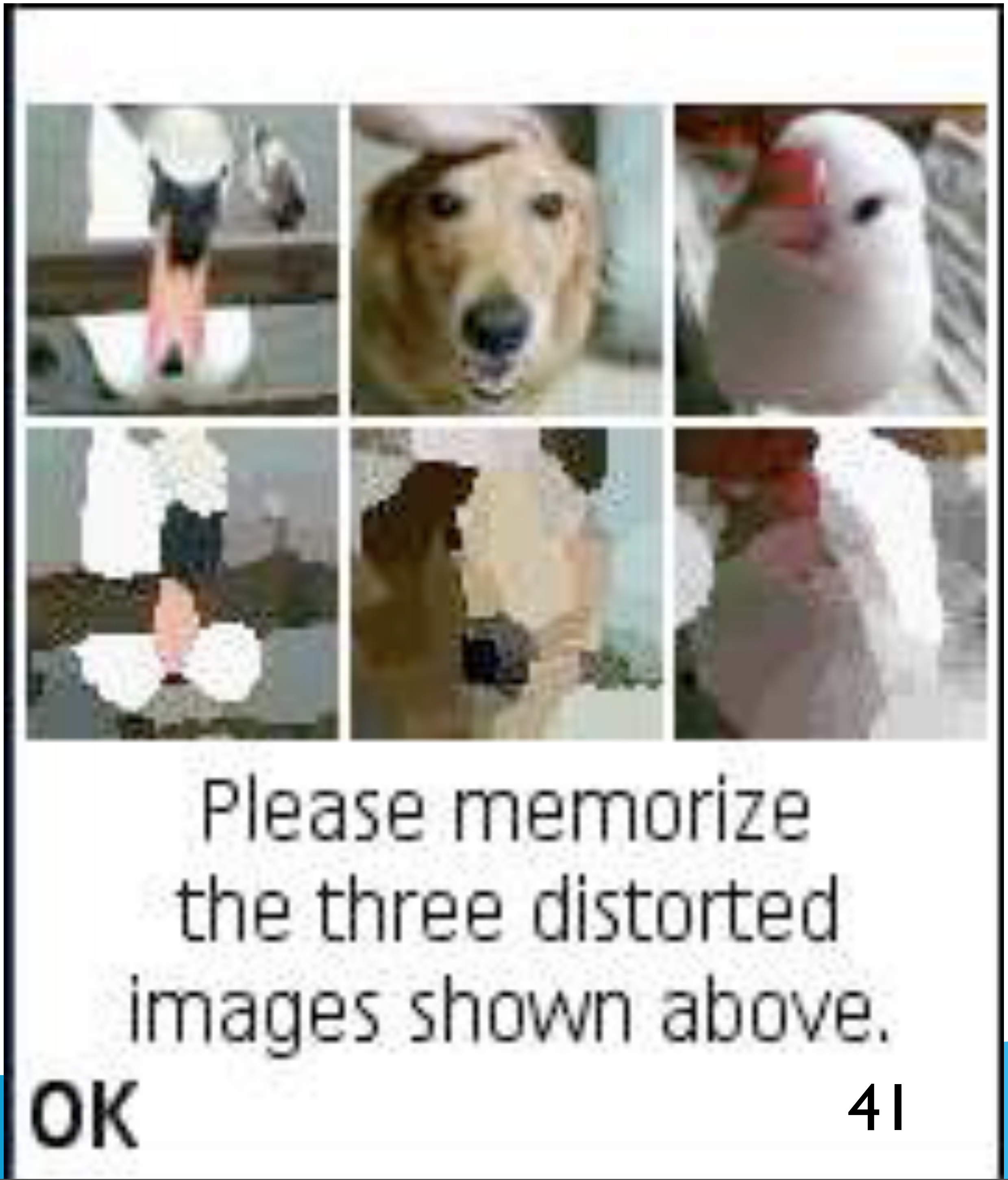
- Out of Berkeley, 1999-2000
- recognize previous images, rather than memorizing them.

Draw a Secret



Lin, Dunphy, *et al.* SOUPS 2007

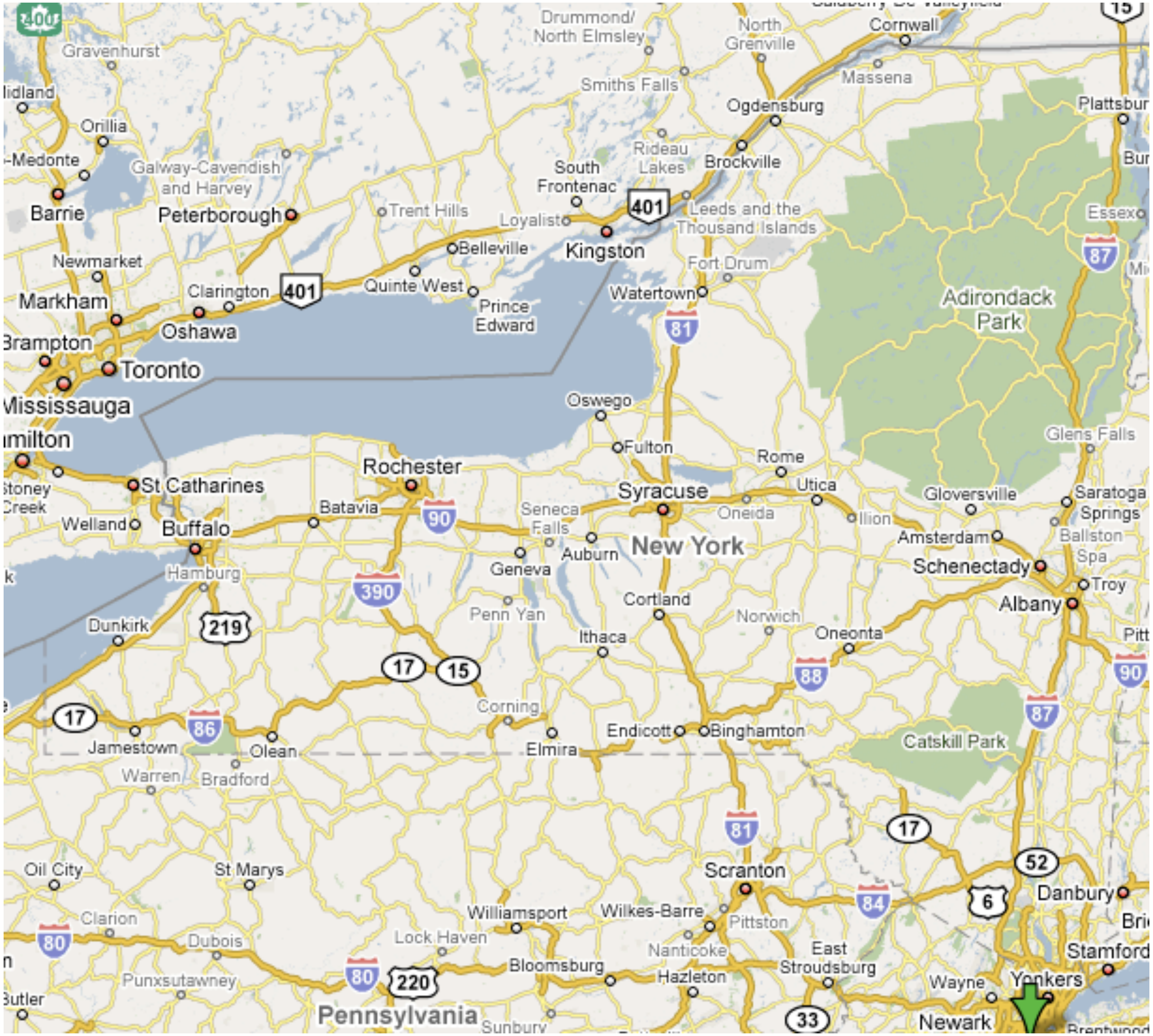
Use Your Illusion (SOUPS 2008)



Please memorize the three distorted images shown above.

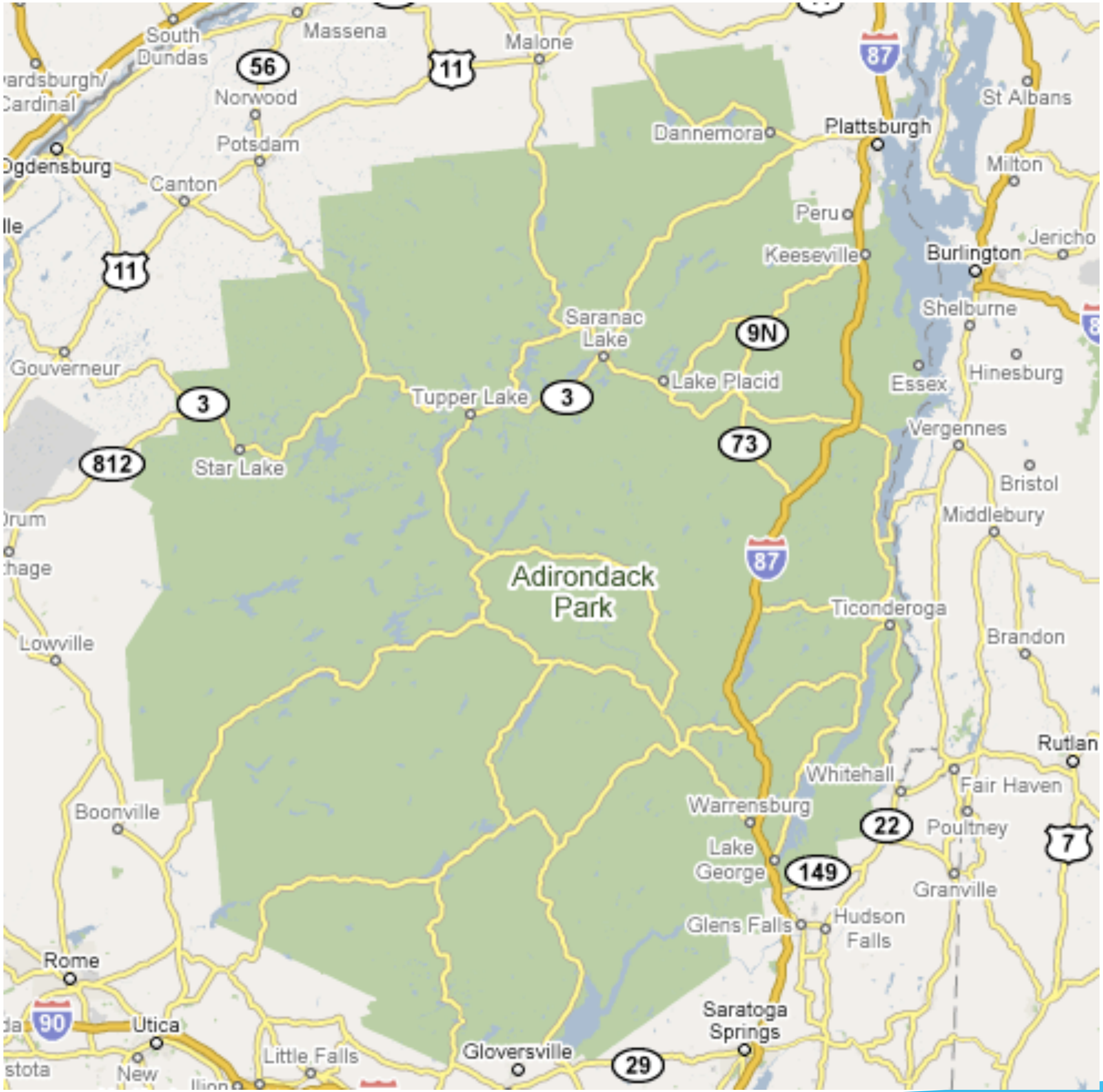
Some Whacko Ches Ideas

Passmaps

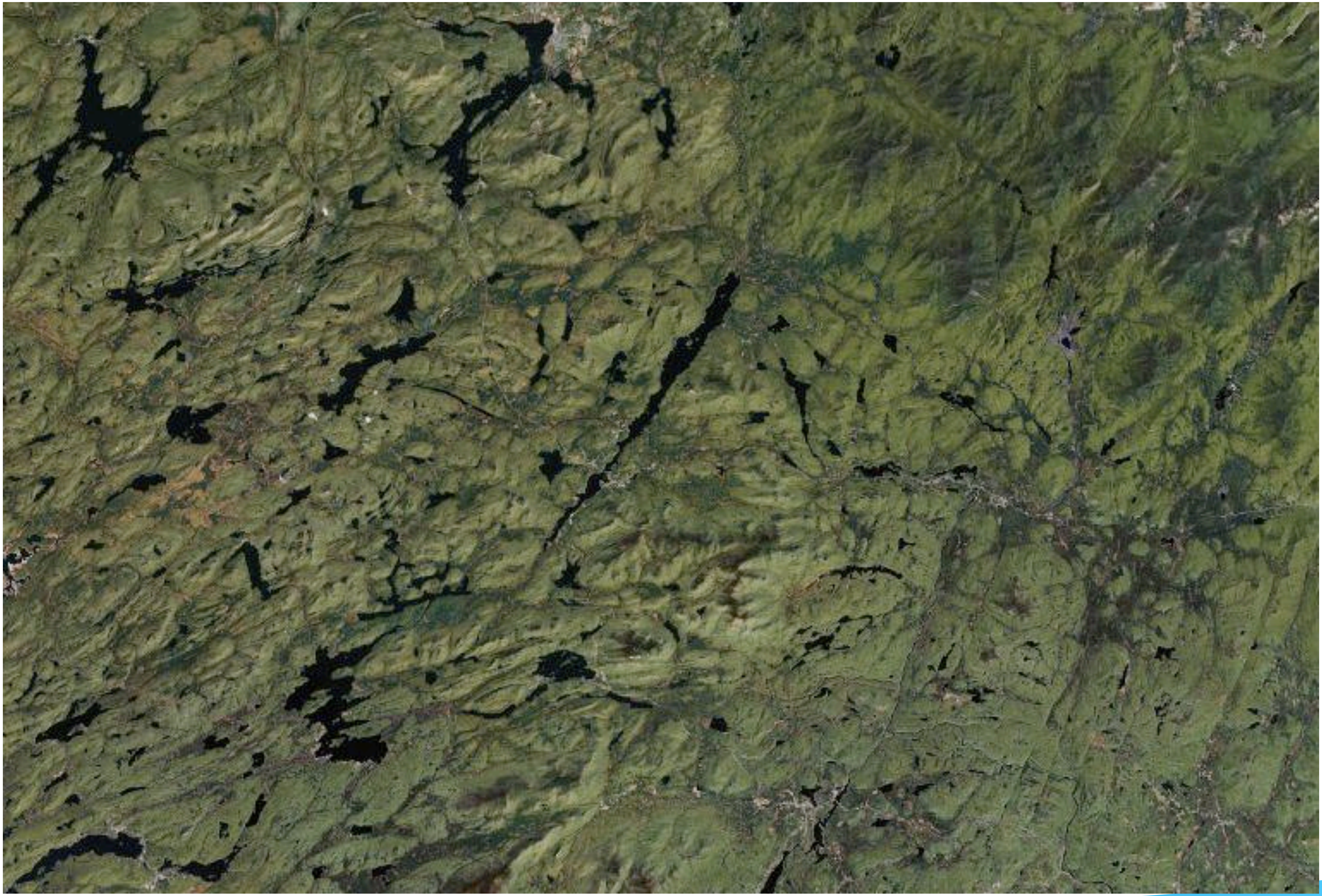


TODO: Find a point in New York State

Adirondacks are nice

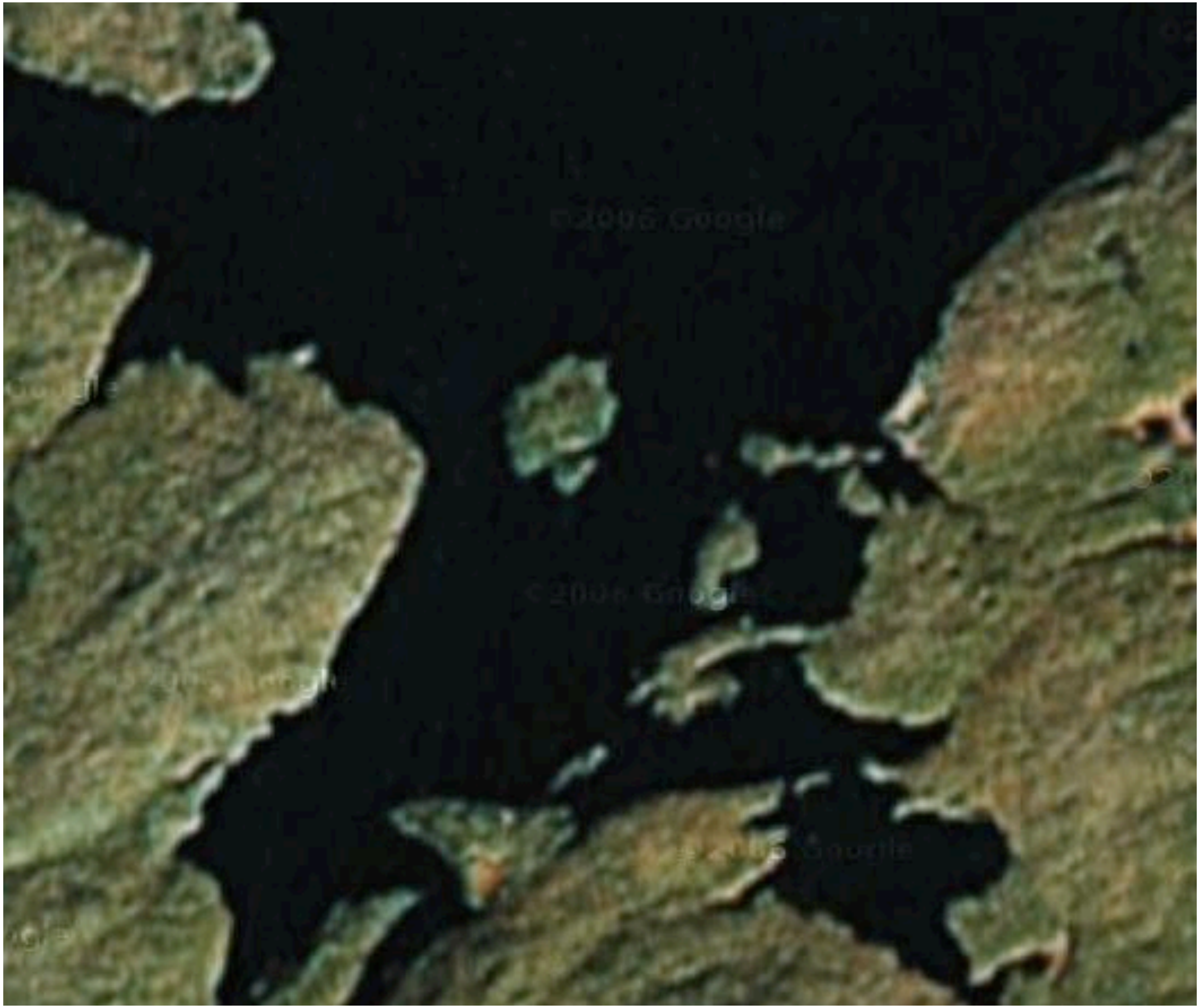

South Dundas
Massena
Malone
56
11
87
St Albans
ardsburgh/ Cardinal
Norwood
Dannemora
Plattsburgh
Potsdam
Milton
Ogdensburg
Canton
Peru
Jericho
lle
Keeseville
Burlington
11
Shelburne
Saranac Lake
9N
Gouverneur
Lake Placid
Essex
Hinesburg
3
Tupper Lake
3
Vergennes
73
812
Star Lake
Bristol
Drum
Middlebury
hage
87
Adirondack Park
Ticonderoga
Lowville
Brandon
Rutlan
Whitehall
Fair Haven
Boonville
Warrensburg
22
Poultney
7
Lake George
149
Granville
Glens Falls
Hudson Falls
Rome
Saratoga Springs
90
Utica
Little Falls
Gloversville
29
stota
New
Ilion

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



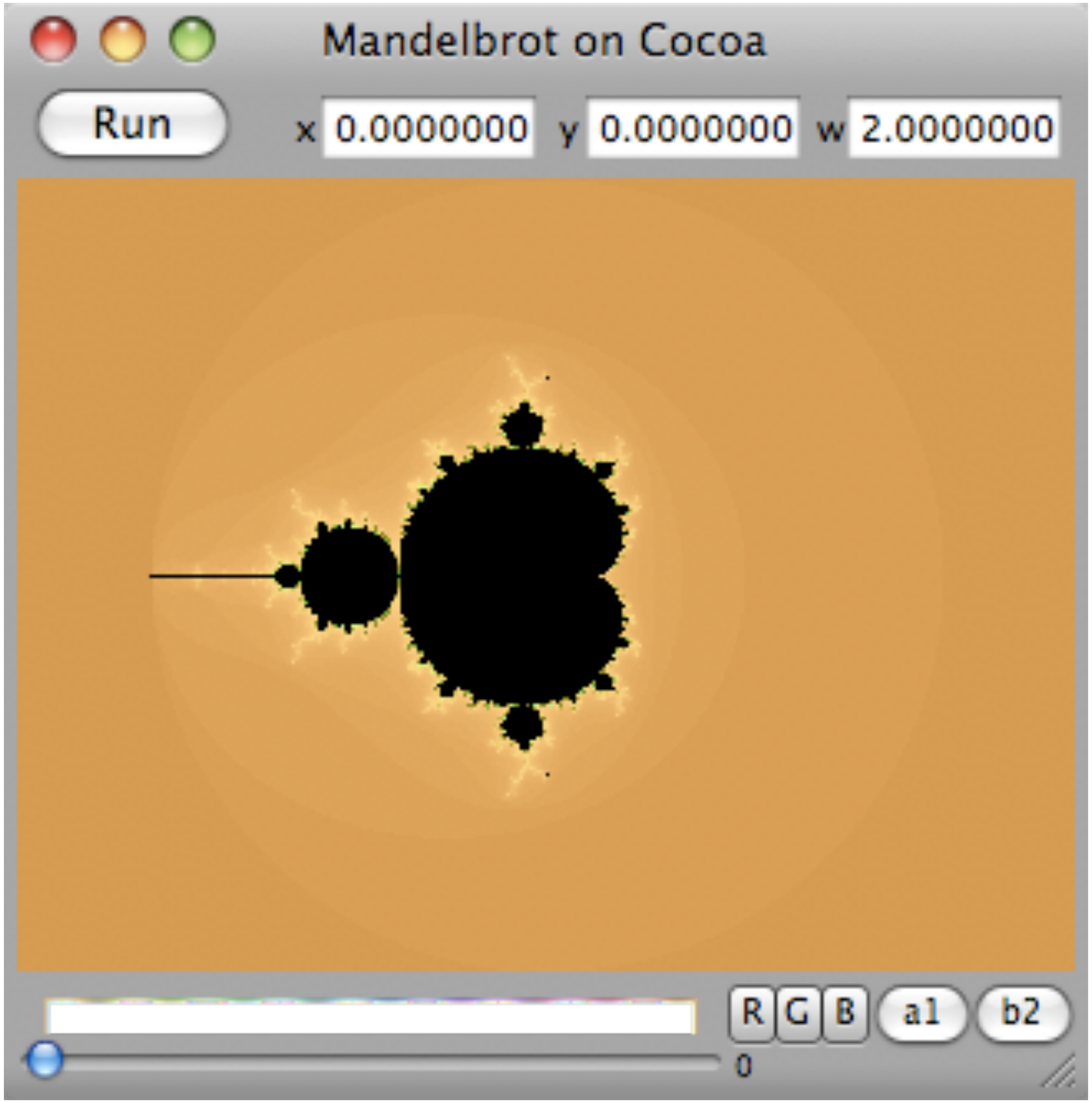
PW is lat/long of the center island

Passmaps?

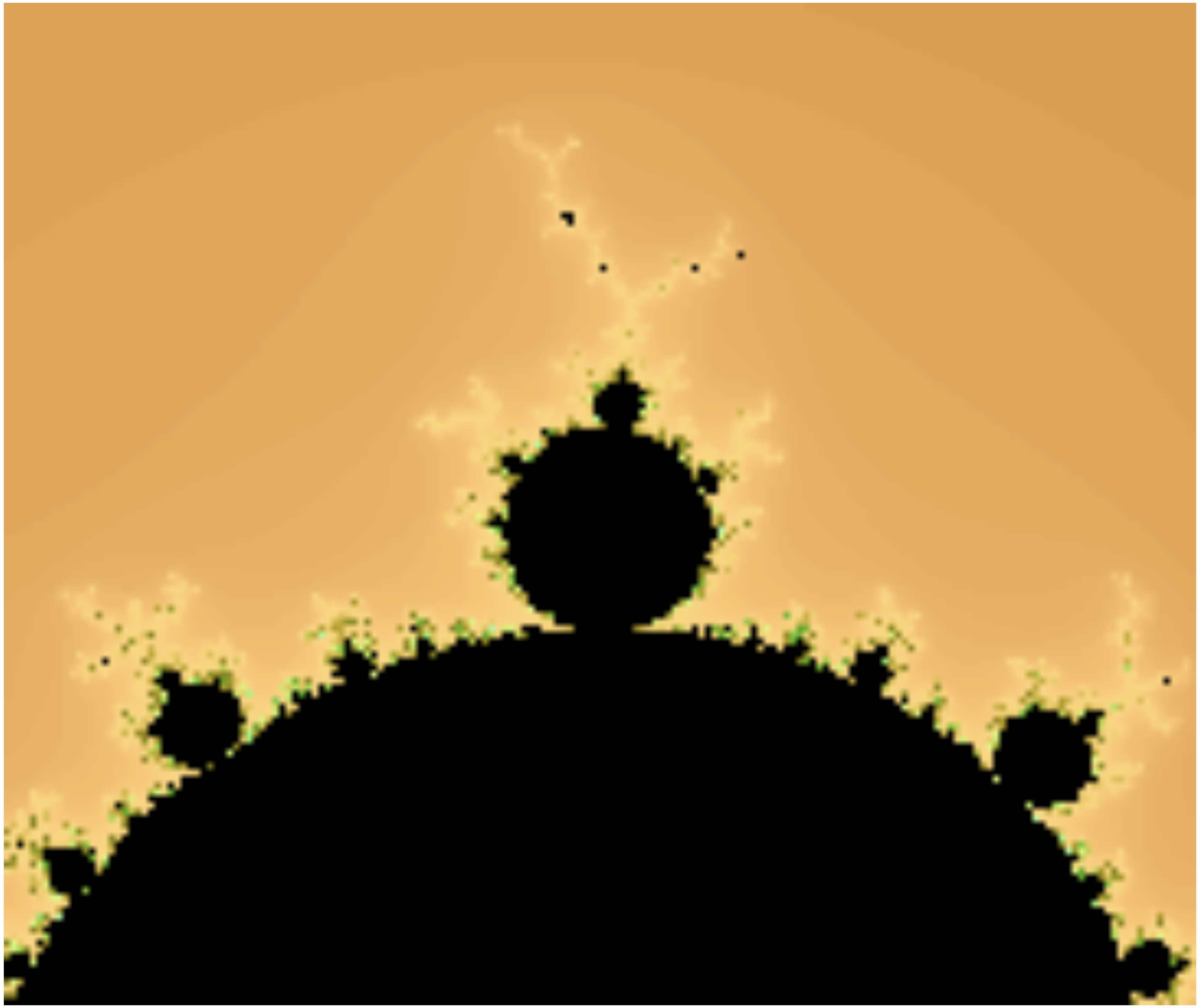
- Reproducibly zoom in on a remembered set of map features?
- Lots of bits
- Maybe hard to shoulder surf
- Not challenge/response
- memorable over a year?

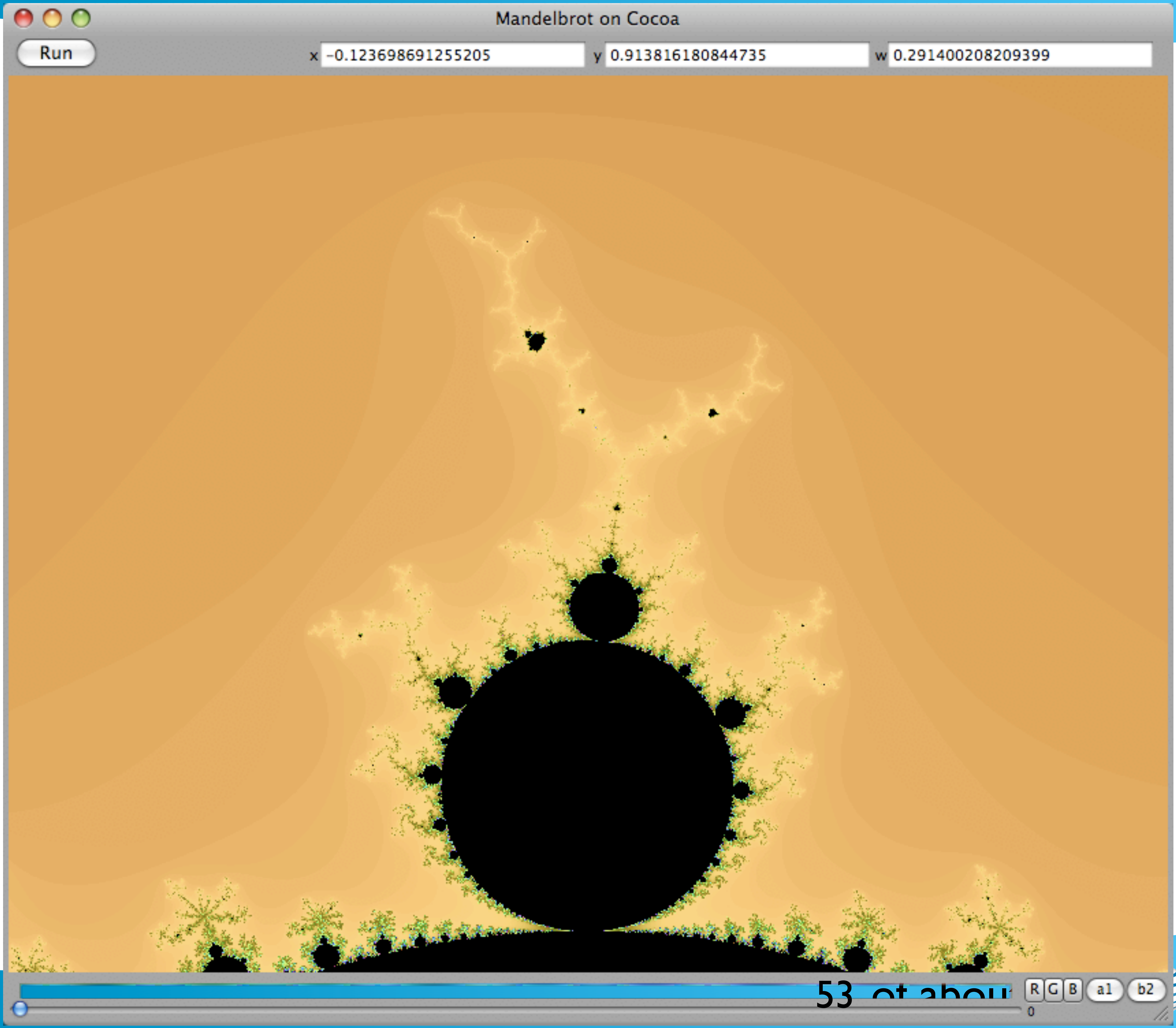
Some Whacko Ches Ideas

How about passgraphs? Get Google out of the loop



Mandelbrot on Cocoa
Run
x 0.0000000
y 0.0000000
w 2.0000000
R
G
B
a1
b2
0



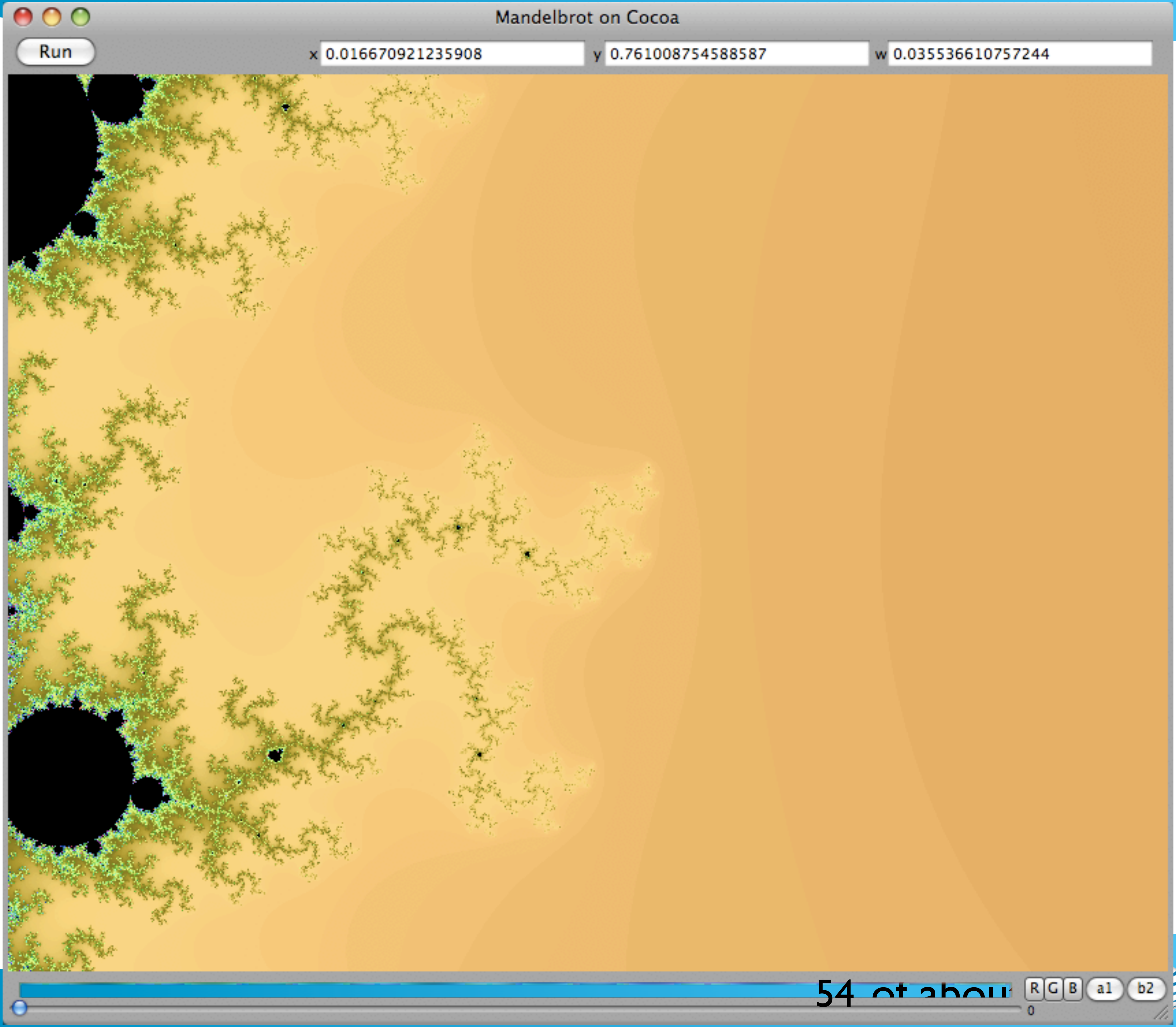


Mandelbrot on Cocoa

x −0.123698691255205

y 0.913816180844735

w 0.291400208209399

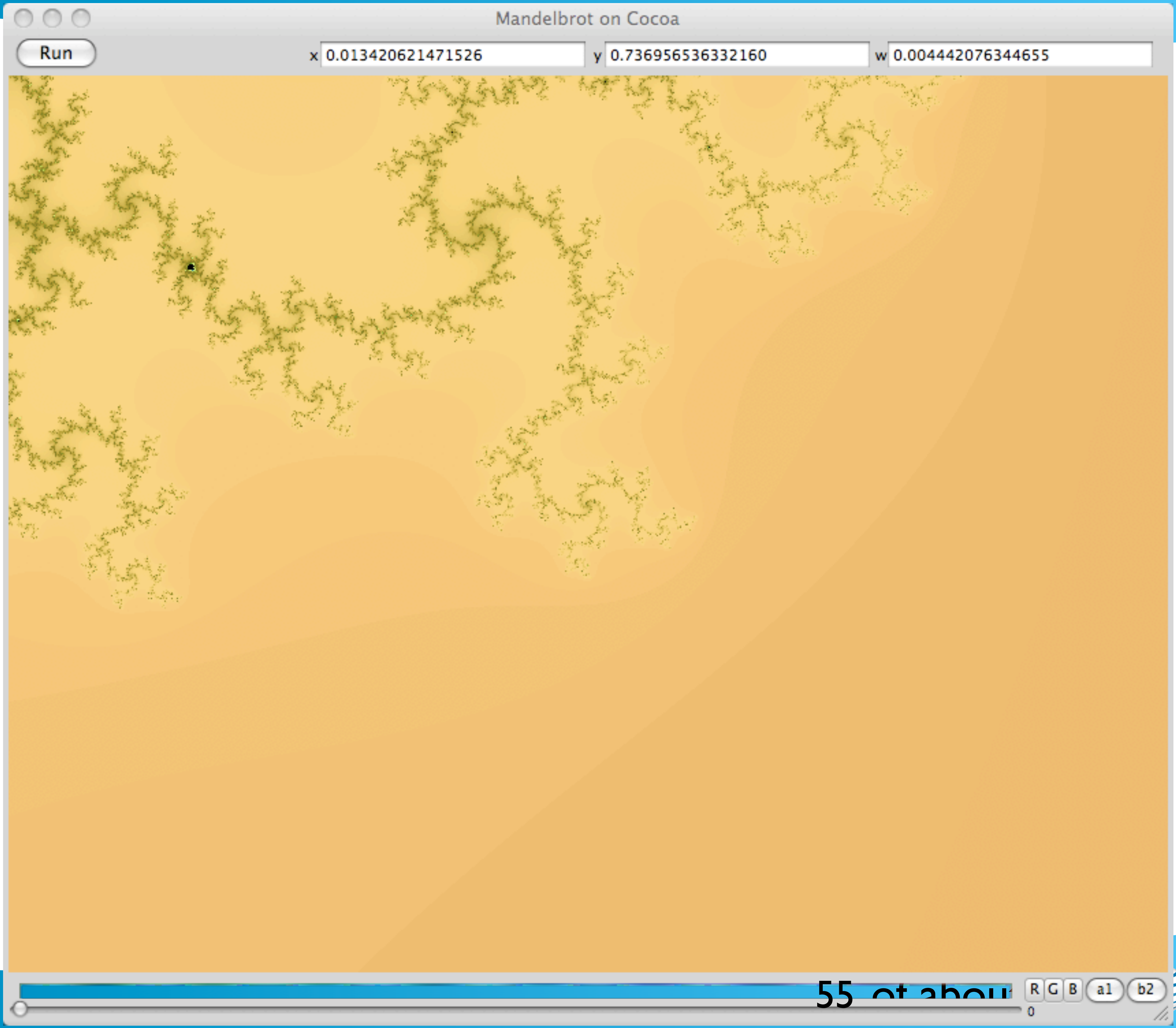


Mandelbrot on Cocoa

x 0.016670921235908

y 0.761008754588587

w 0.035536610757244

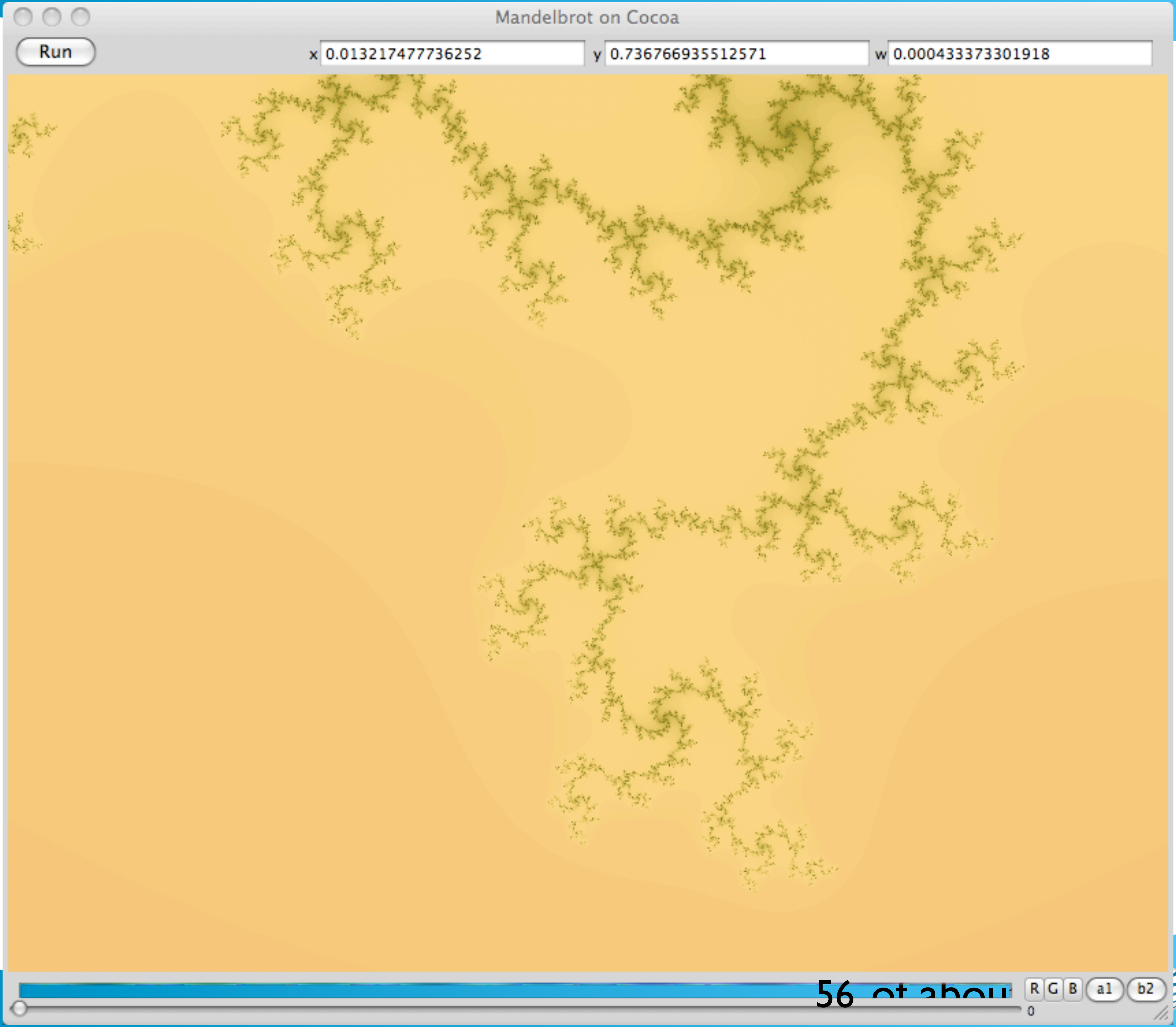


x 0.013420621471526

y 0.736956536332160

w 0.004442076344655

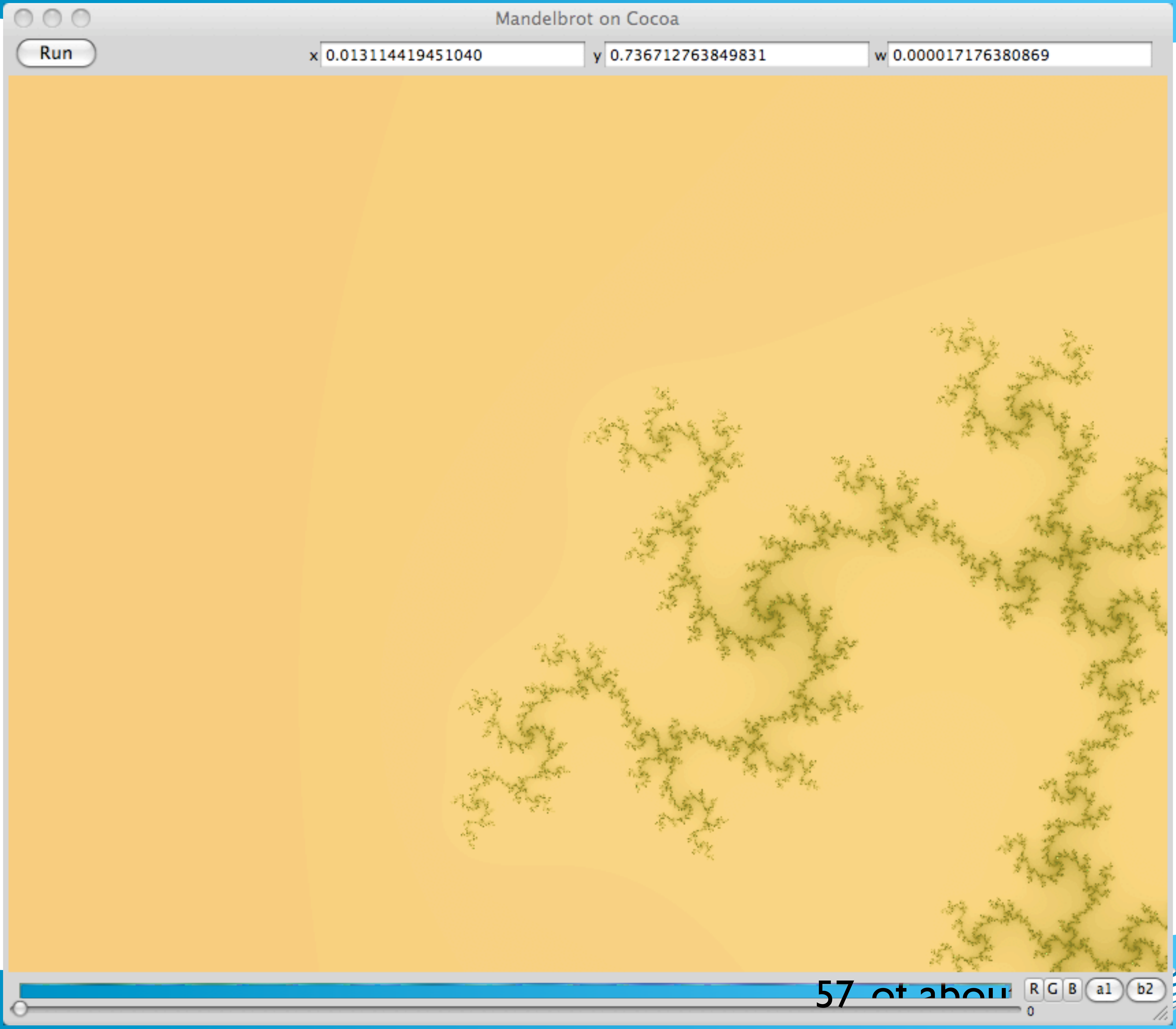
55 of abou



x 0.013217477736252

y 0.736766935512571

w 0.000433373301918



Mandelbrot on Cocoa

x 0.013114419451040 y 0.736712763849831 w 0.000017176380869

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

34

210
210
4
NIA INSURANC

210
NIA INSURA

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

Text-only, please

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

```
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

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

Disclaimer

- These are all guidelines, suggestions, thoughts for your own risk/benefits analysis
- Every security person I've discussed this with has a somewhat different take
- Rethink and reengineer these systems, when appropriate

Threats to casual targets

- Password capture by phishing
- Password capture by keystroke logging
- *Not* dictionary attacks
  - Most online systems limit password guessing
- Most attacks are wholesale, not targeted

Dictionary attacks still a concern

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

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

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

Use an authentication server

- Centralizes the security function
- Make it strong and robust
- Replication is dangerous, reliability is better
- Limit authentication attempts

If password is forgotten

- Use a user-supplied reminder of the primary password
- Do not 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

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

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

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

Accounts should still not be shared

- You want accountability, even (especially) on shared bank accounts.
- It doesn't matter on the lowest grade authentication

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

If you still think you need strong passwords

- What is your threat model?
  - crooks? foreign governments?

Use One-time passwords if you can

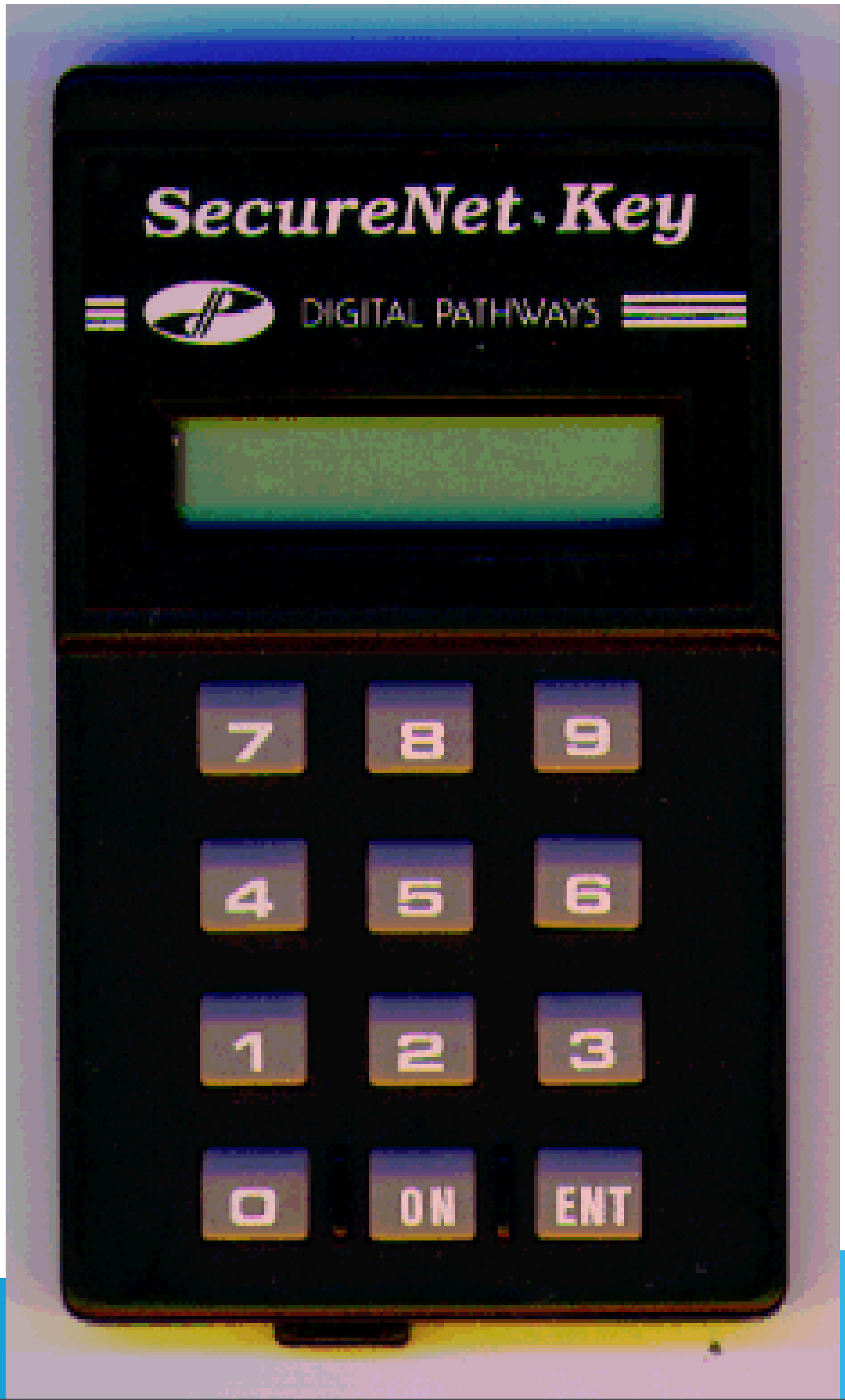
- No replay attacks
- Bad guy (or his software) must be present to win
- May not be sharable
- Usually requires device or printout

Challenge/Response passwords

- One time, one session password
- Closes up the S/Key race

SecureID

SecureNet Key SNK-004



A login from my distant past

```
RISC/os (inet)

Authentication Server.

Id? ches
Enter response code for 70202: 04432234


Destination? cetus
$
```

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

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, POP3S, IMAPS, 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

If you must, here are at least 60 random bits

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

If you must

- not user-chosen, but user can veto, waiting for a “good one”
- User-chosen phrases have *much* lower entropy
- they are going to write it down, for a while
- for daily use: who’s going to remember this over a year?

Words are better than eye-of-newt

- much easier to type
- spelling checking (iPhone) is your friend, not enemy

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.

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 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?

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
- Tell them I said it was probably a good idea
- Backup passwords are usually weaker
- Improve the users' experience
- Annoyed users are less cooperative

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.

Rethinking Passwords

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