Rethinking Passwords

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

Sep 11

Sep 11

- **“Daddy, come home.”**

Sep 11

- “Daddy, come home.”
- SFO to Parsippany in 47 hours, with two strangers (including a smoker)

Sep 11

- “Daddy, come home.”
- SFO to Parsippany in 47 hours, with two strangers (including a smoker)
- Bob Weaver, NYECTF

Sep 11

- "Daddy, come home."
- SFO to Parsippany in 47 hours, with two strangers (including a smoker)
- Bob Weaver, NYECTF
- John Jay, 138 agents, one case

Sep 11

- “Daddy, come home.”
- SFO to Parsippany in 47 hours, with two strangers (including a smoker)
- Bob Weaver, NYECTF
- John Jay, 138 agents, one case
- half a dozen folks from industry were there

Sep 11

- "Daddy, come home."
- SFO to Parsippany in 47 hours, with two strangers (including a smoker)
- Bob Weaver, NYECTF
- John Jay, 138 agents, one case
- half a dozen folks from industry were there
- piles of donated equipment (Dells, Blackberry's, etc.)

These meetings build relationships that are vital to flexible national response to new attacks

because the ounce of prevention doesn’t always work

at&t

Rethinking Passwords

Bill Cheswick

AT&T Labs - Research

ches@research.att.com

5 of about 102

AT&T Shannon Labs

- Not Bell Labs (alCatel Lucent)
- Lots of folks from the Labs
- Trying to help the phone company and invent the future
- Brand new talk on iPhone forensics
  - because I left mine in a movie theater
- You may or may not like the idea I came up with last week, but it will probably be in every firewall in five years

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

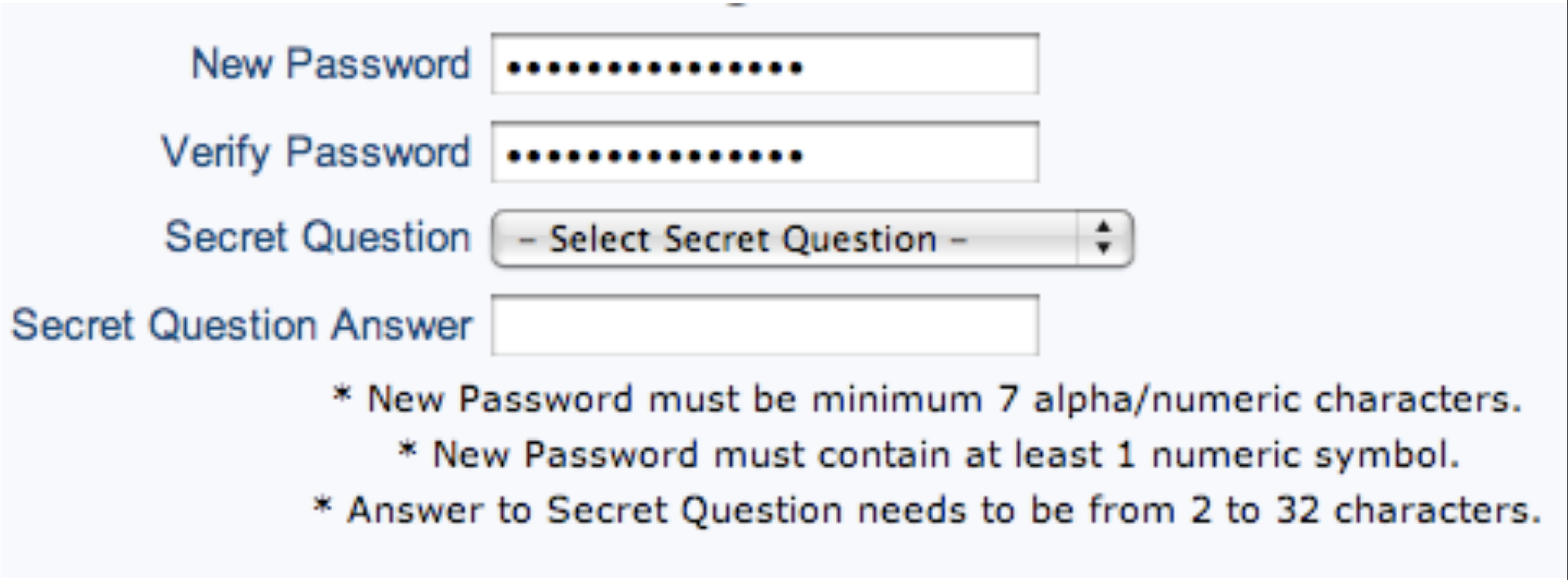
Passwords may be any combination of six (6) characters and are case insensitive.

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, !,$,#,%)

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

Use A Different Password on each Target System

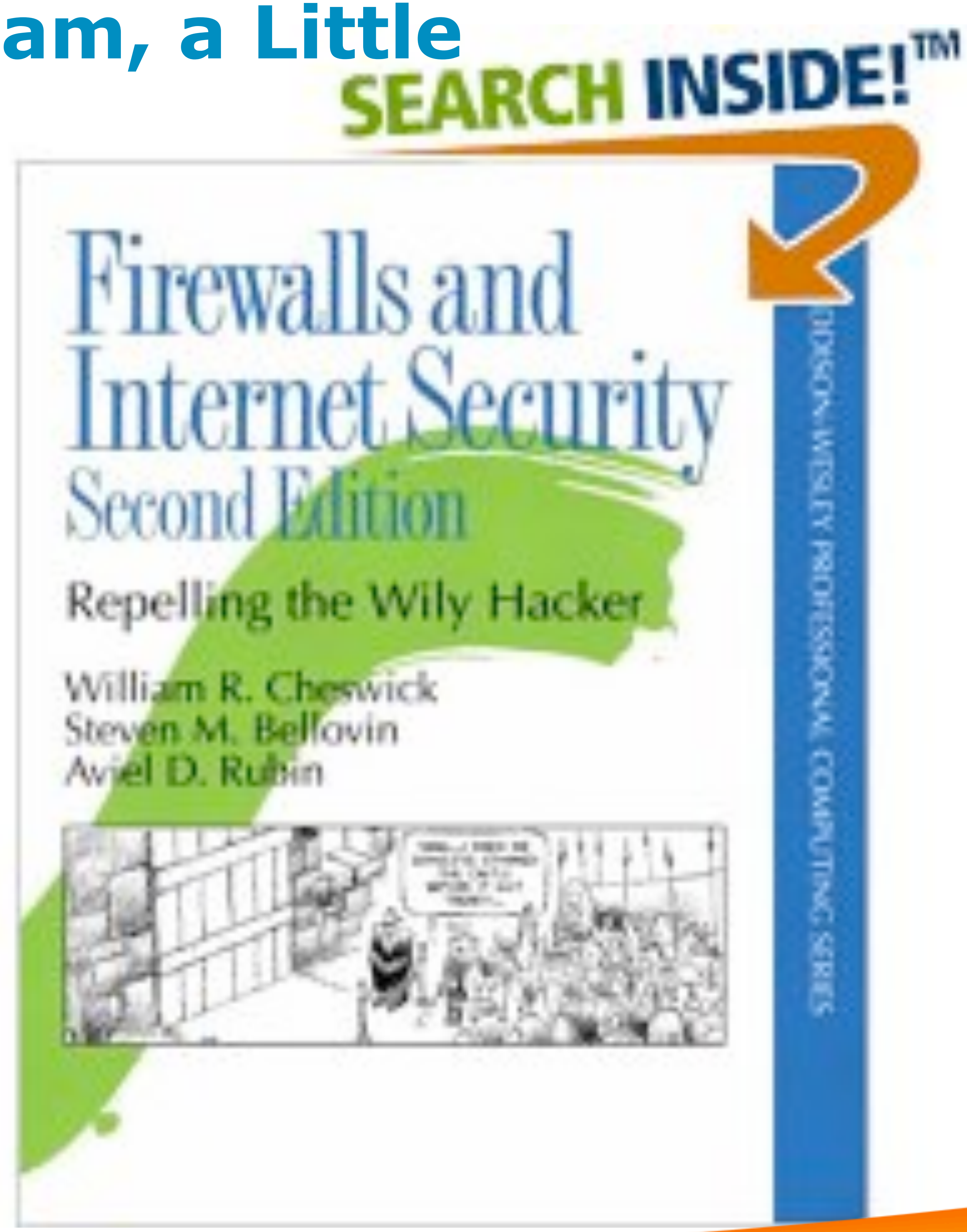
Change Your Password Frequently

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?

- 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?**

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

What are the most common current threats

- Keystroke loggers
- Phishing attacks
- Password database compromise

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

Summary solution

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

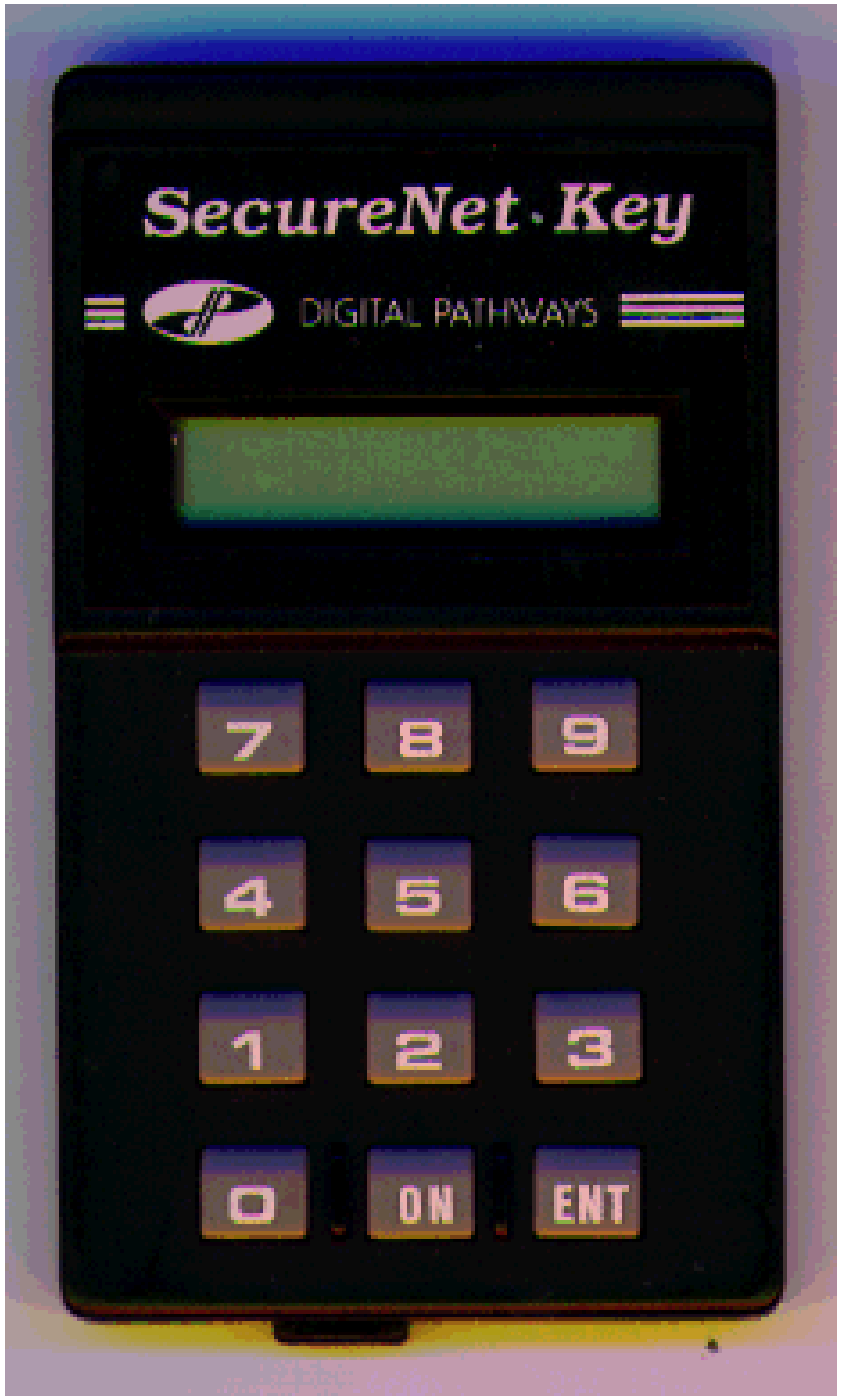
Less painful account locking

- 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

Better Solutions

Getting out of the game

SecureNet Key SNK-004

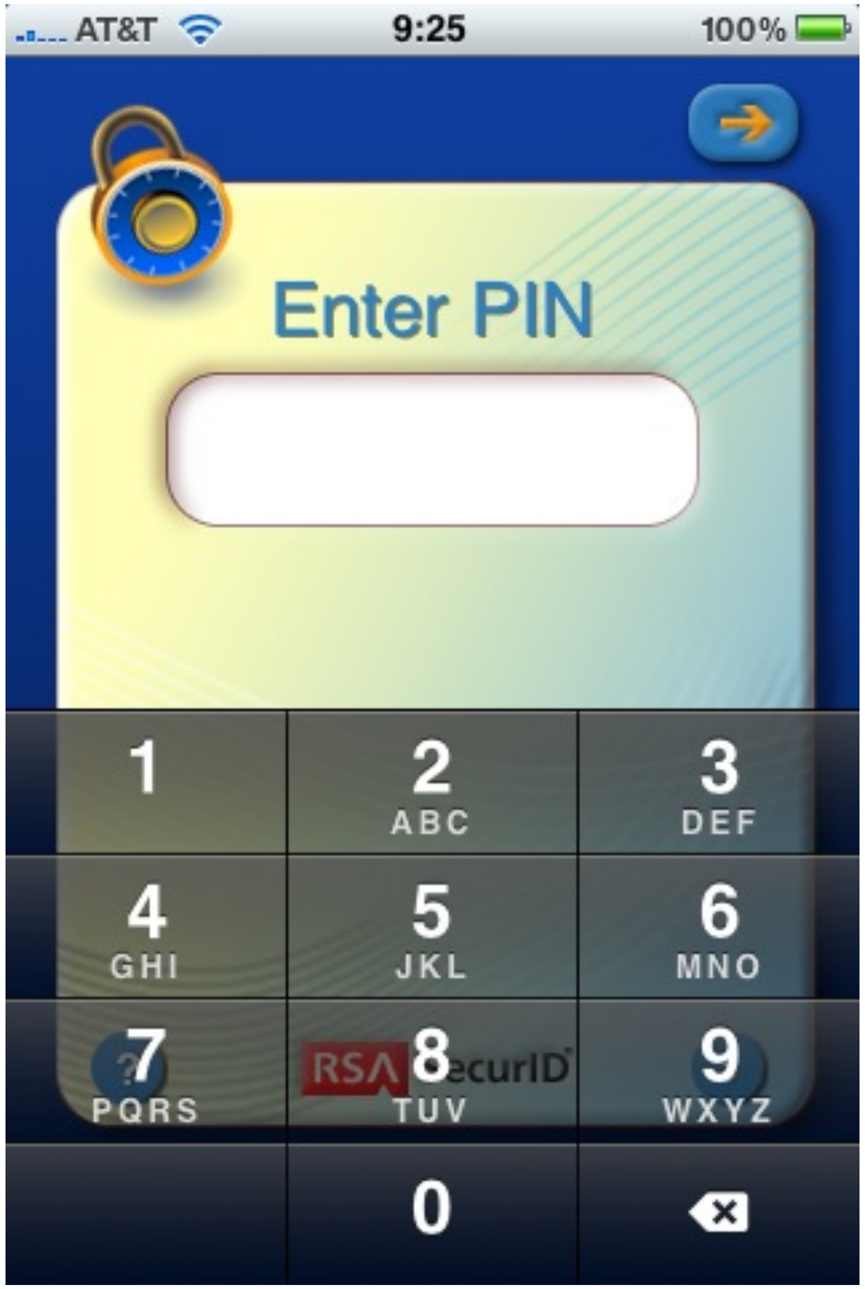


A login from my distant past

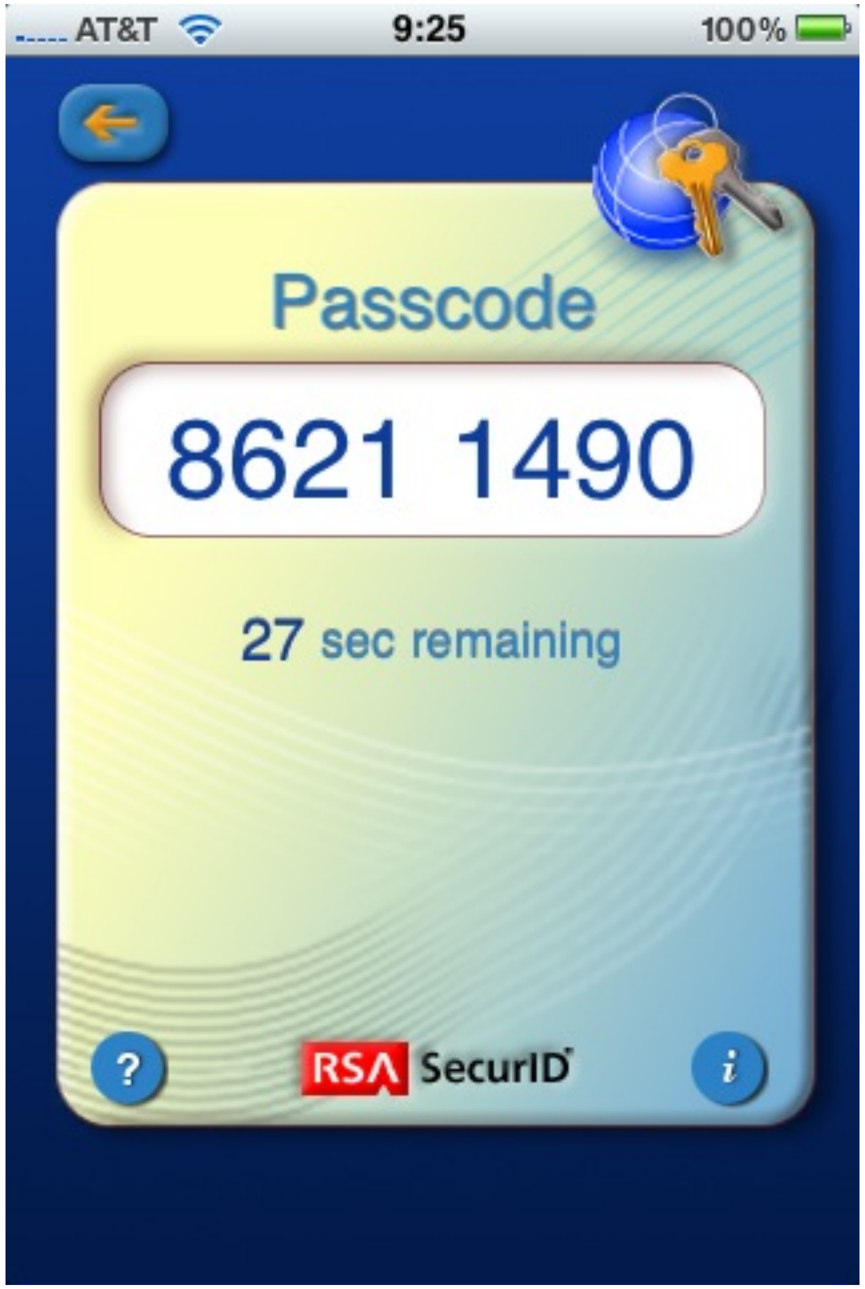
```
RISC/os (inet)

Authentication Server.

Id? ches
Enter response code for 70202: 04432234


Destination? cetus
$
```

SecureID

RSA Softkey



Enter PIN



Passcode

8621 1490

27 sec remaining

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

Password strength is measured in entropy, a number of bits

- 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

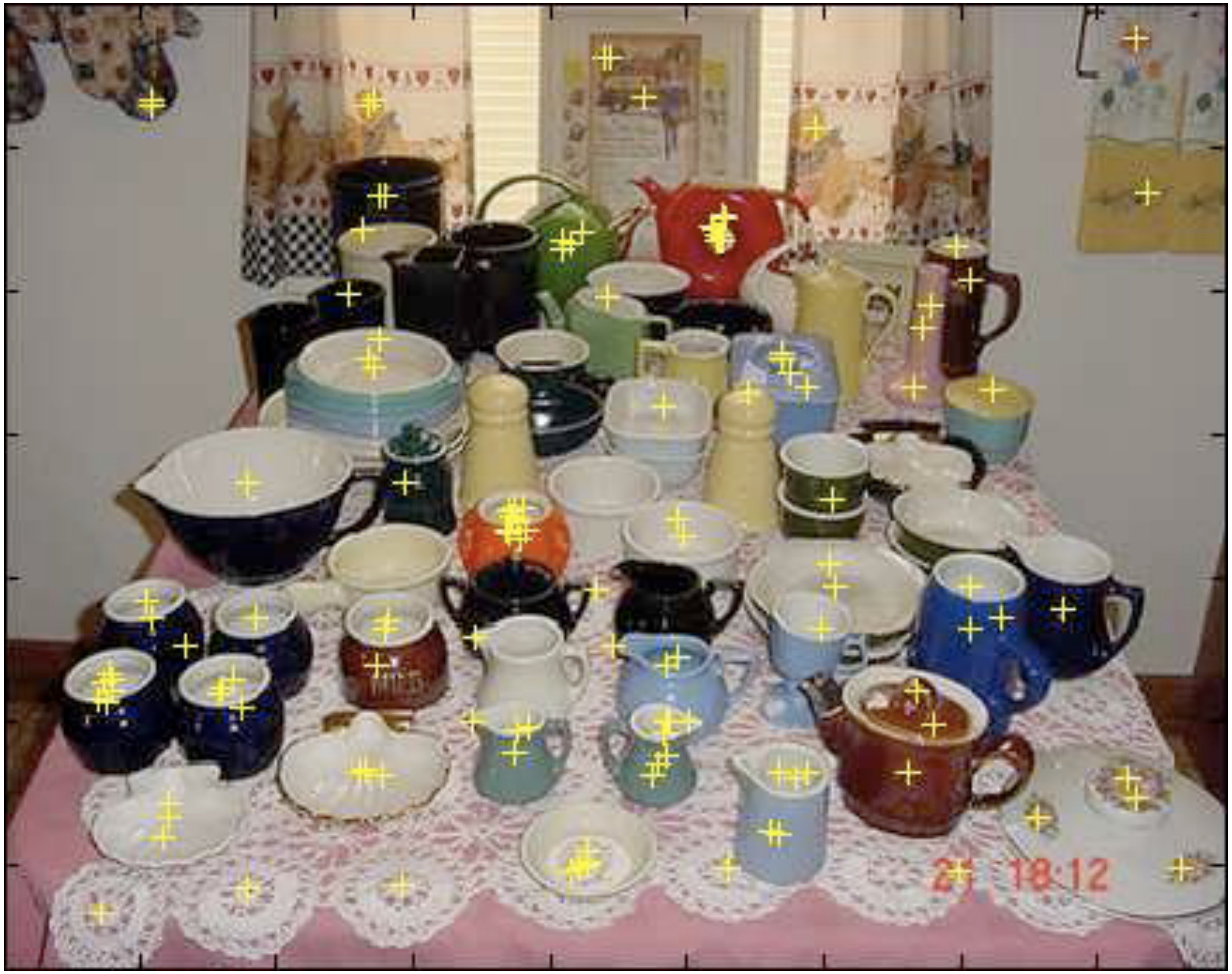
You hard-featured fistula of podagric macaque flux

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

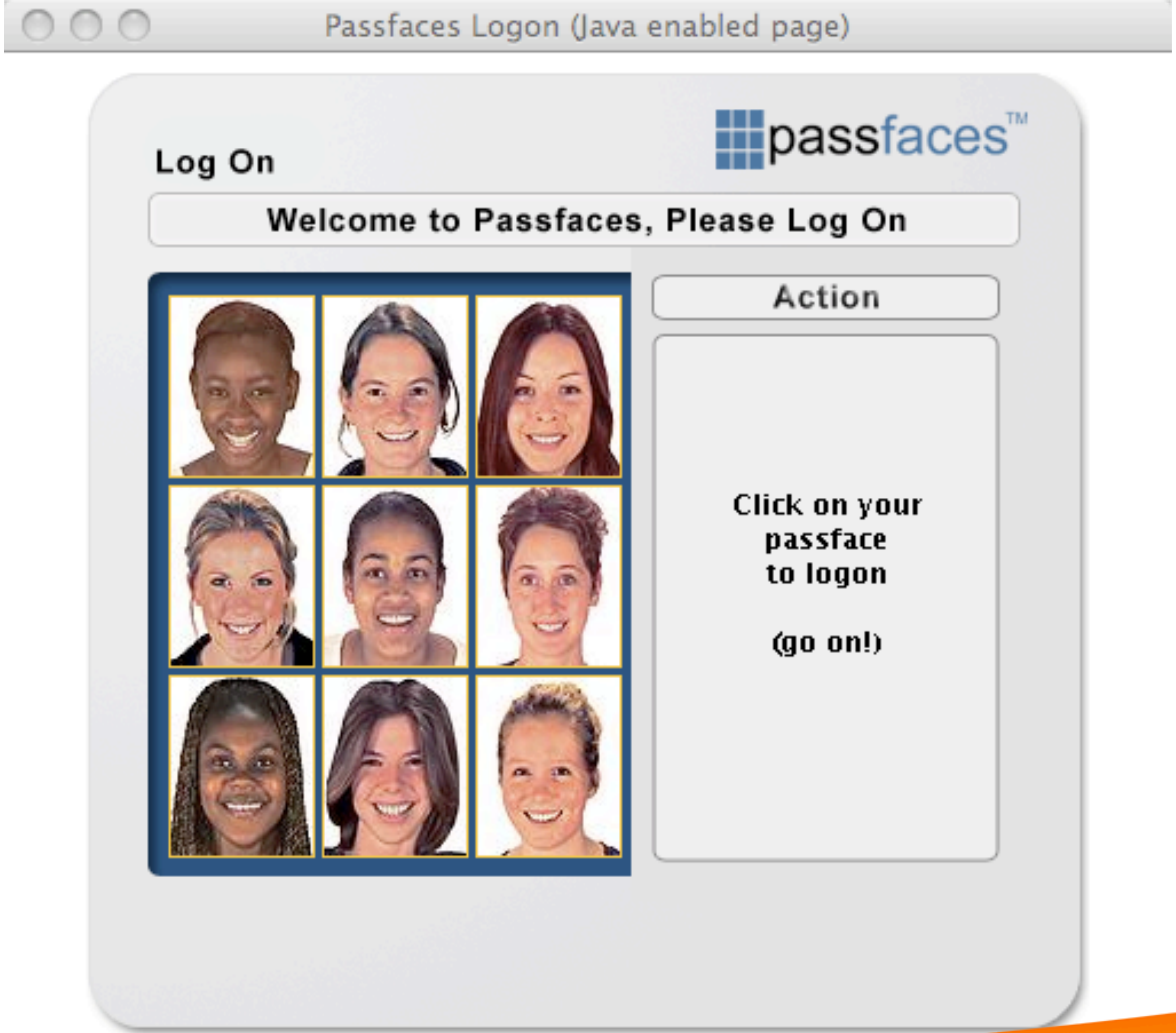
Some Password Ideas

From academia, and me



from *Dirik, Memon, Birget*; SOUPS 2007

Passfaces



Passfaces Logon (Java enabled page)

Log On

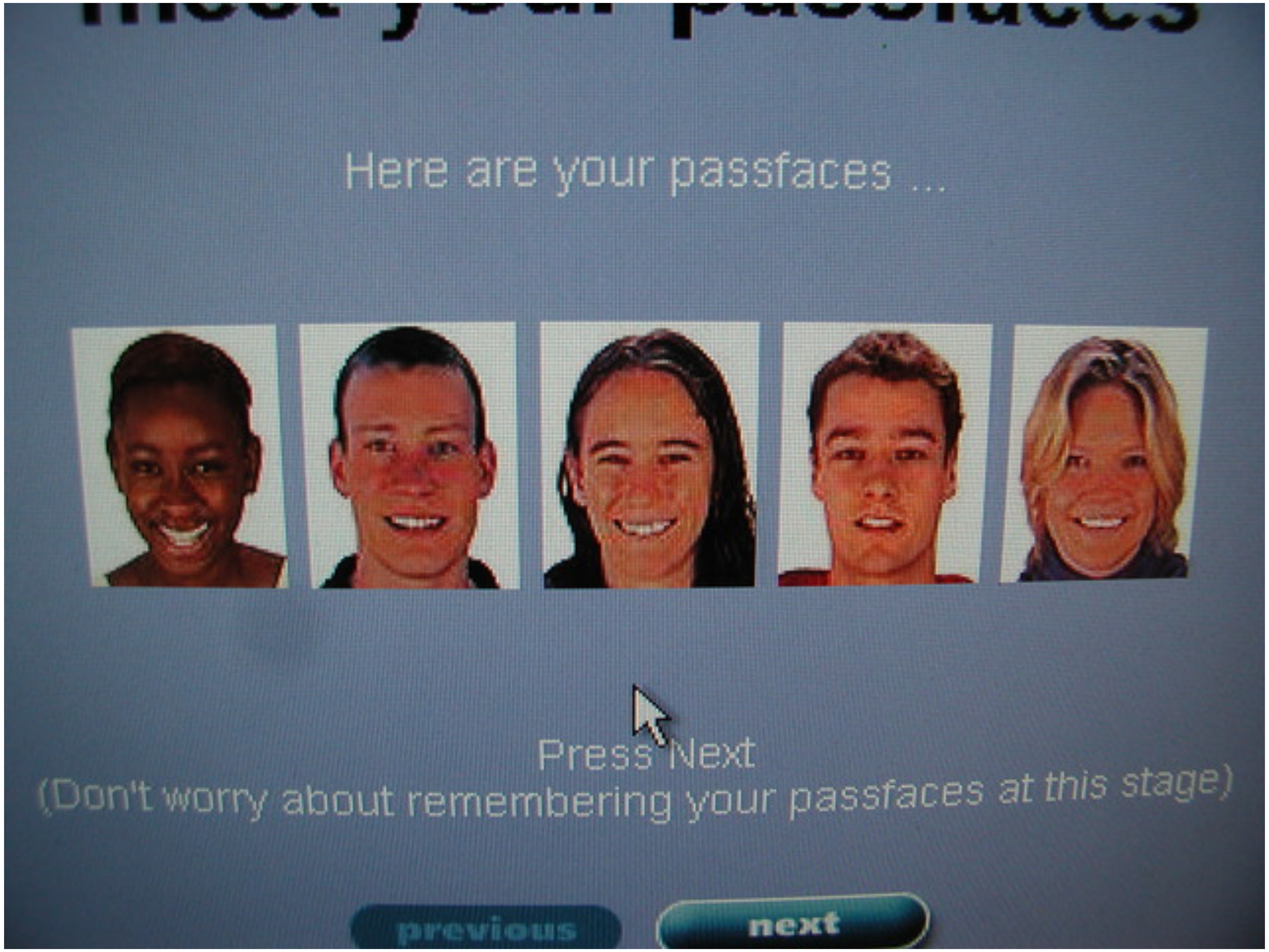
Welcome to Passfaces, Please Log On

Action

Click on your
passface
to logon

(go on!)

My passfaces

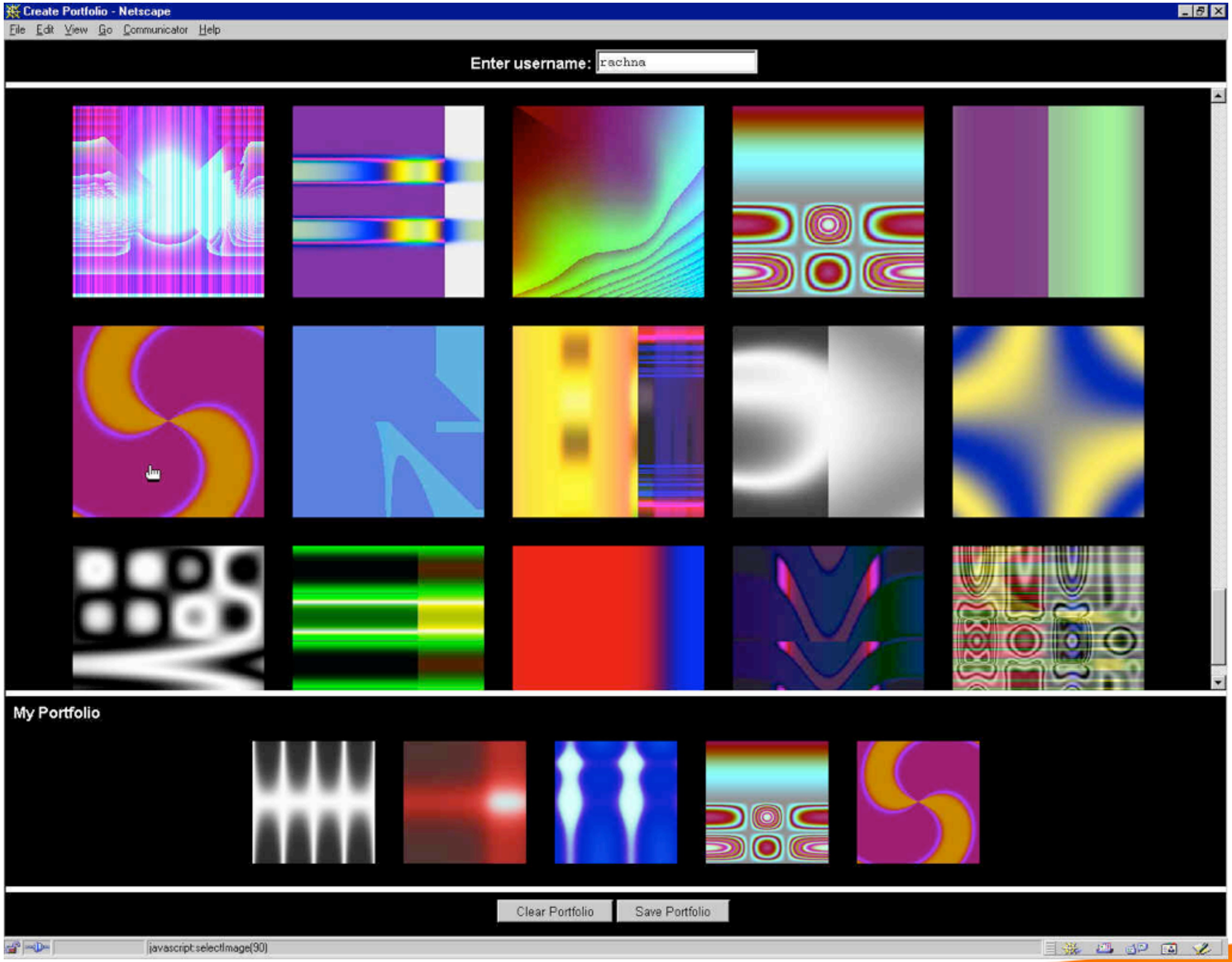


meet your passfaces

Here are your passfaces ...

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

Deja Vu (Recognition-based)

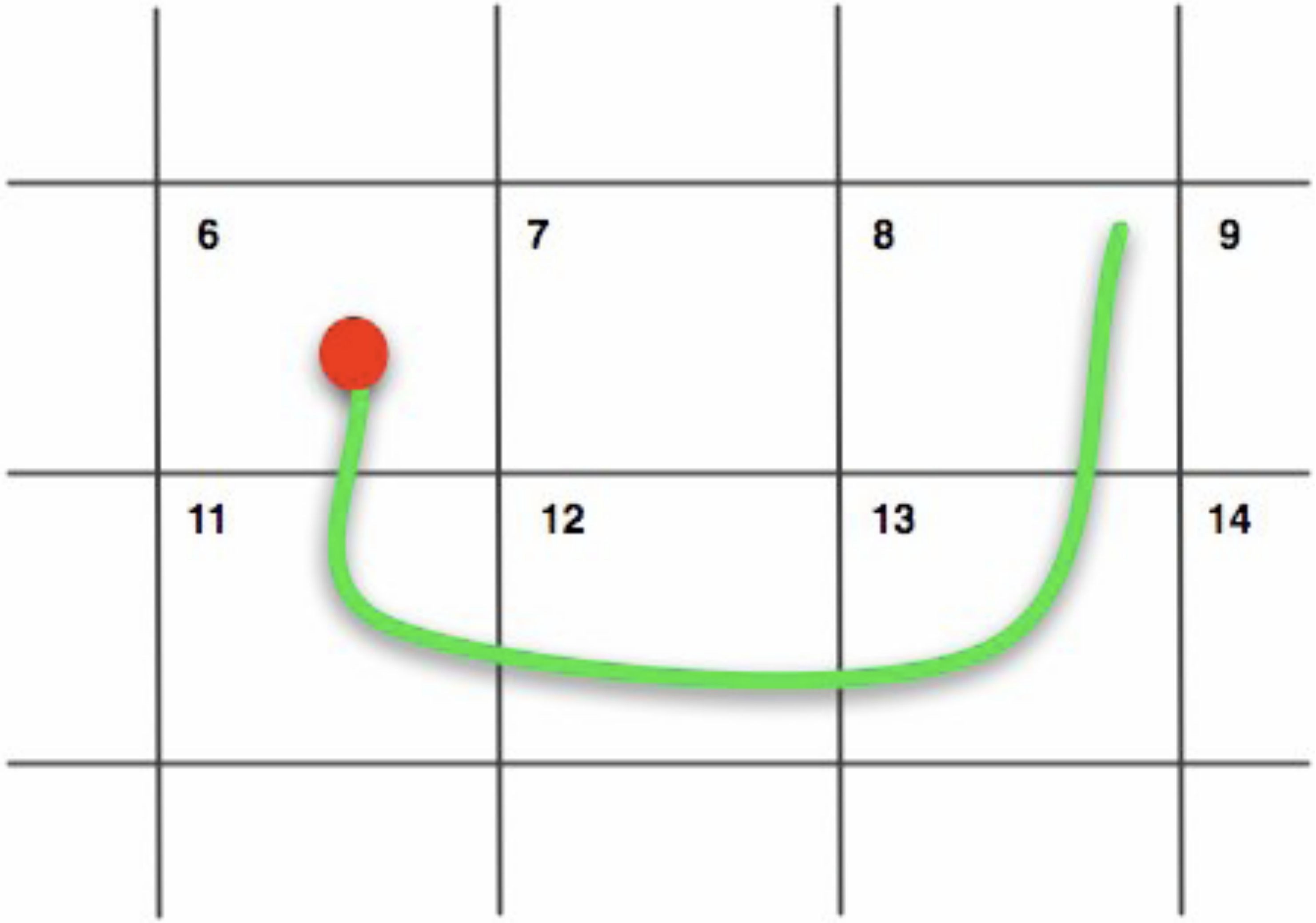


Create Portfolio - Netscape
File Edit View Go Communicator Help
My Portfolio
Clear Portfolio
Save Portfolio

Enter username: rachna

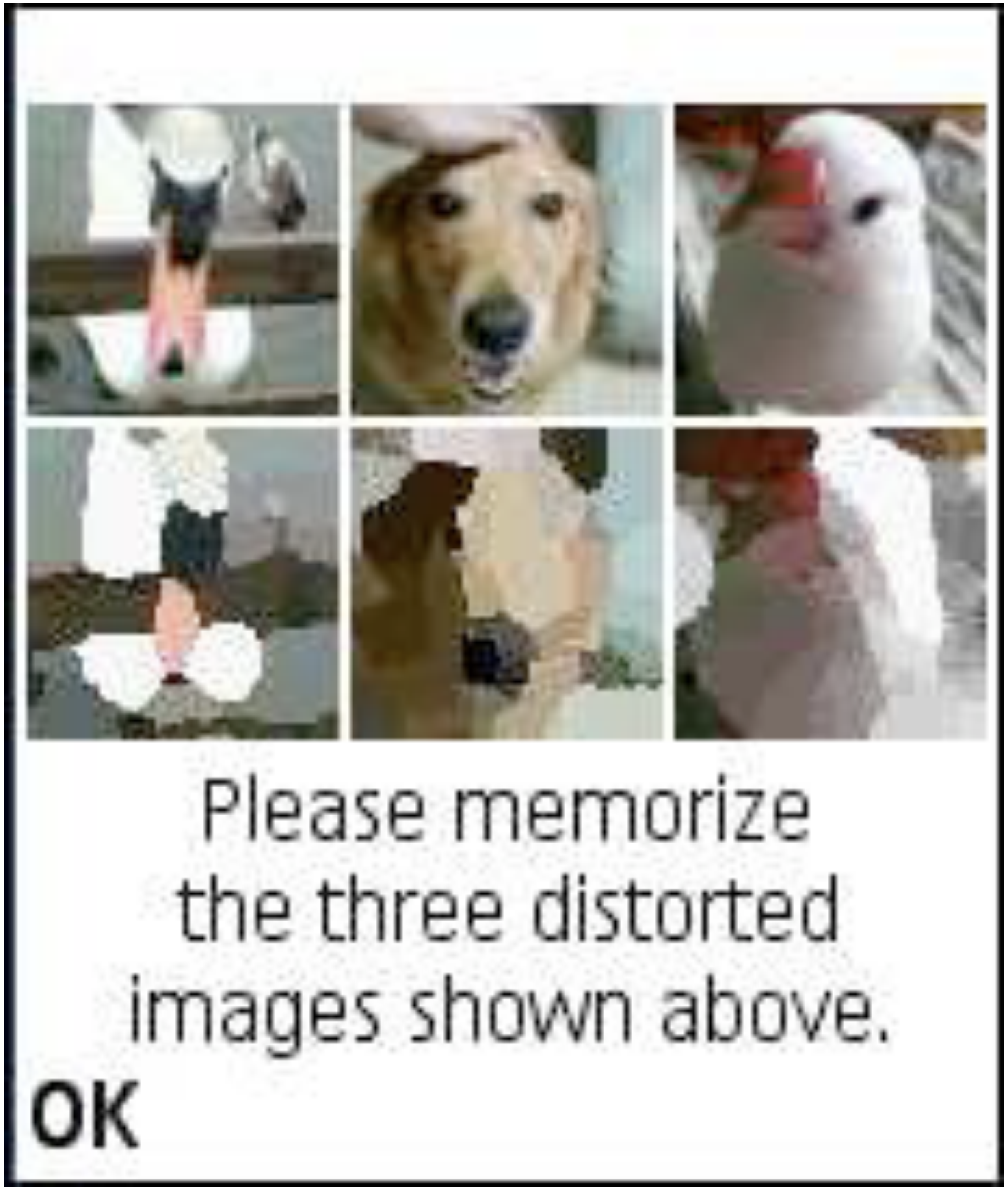
javascript:selectImage(90)

Draw a Secret



Lin, Dunphy, *et al.* SOUPS 2007

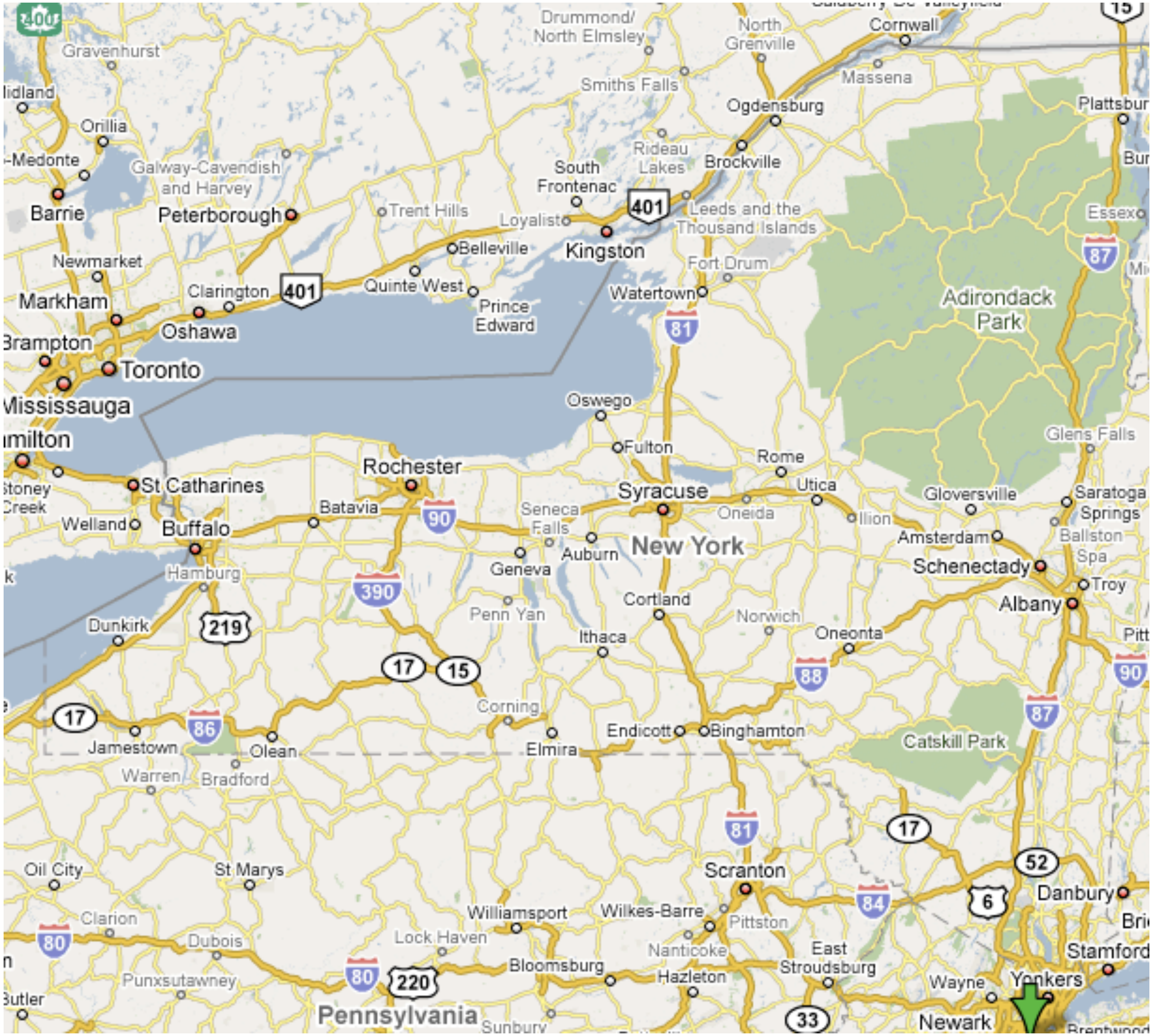
Use Your Illusion (SOUPS 2008)



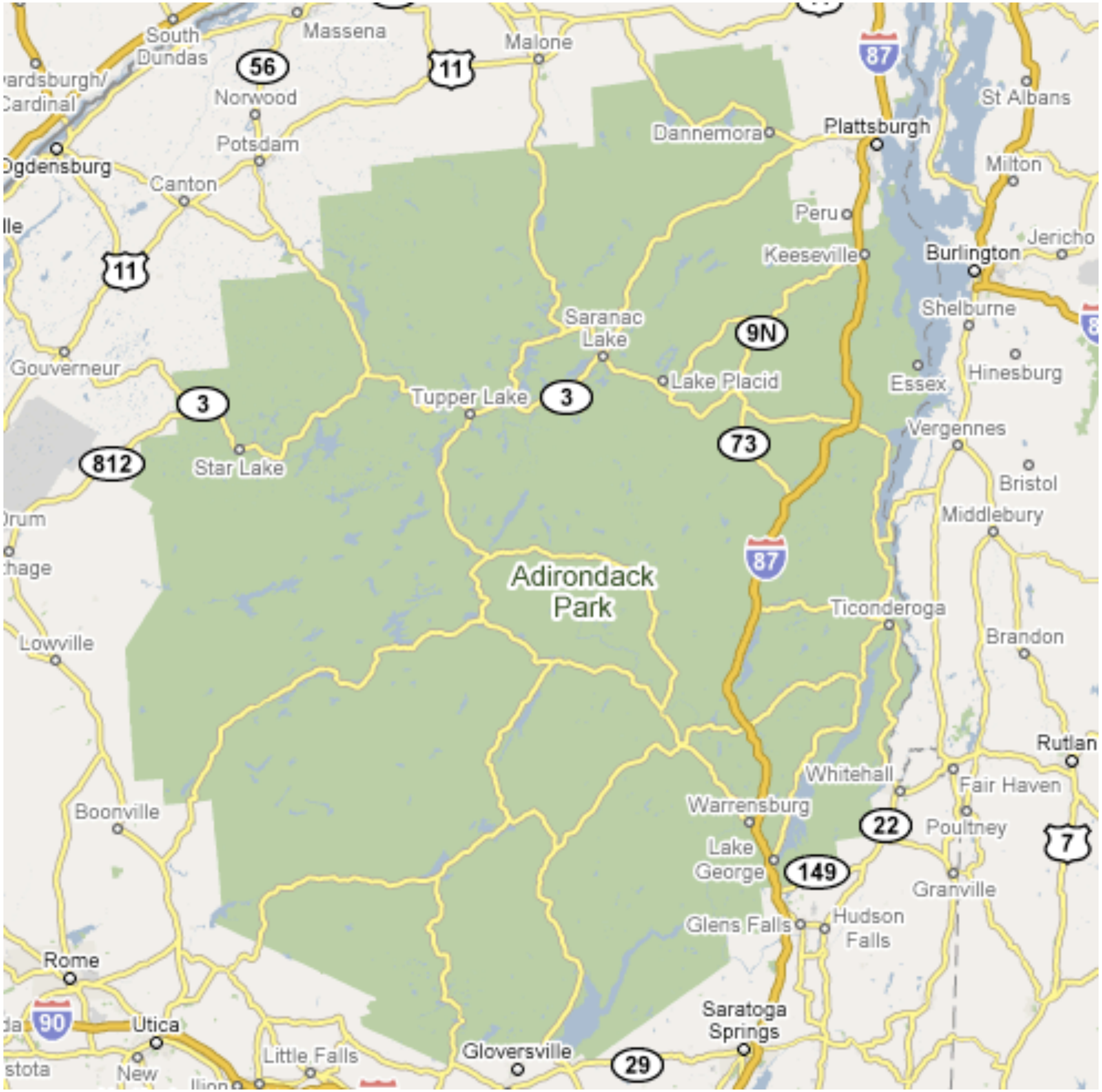
Please memorize the three distorted images shown above.

Some Whacko Ideas from ches

Passmaps

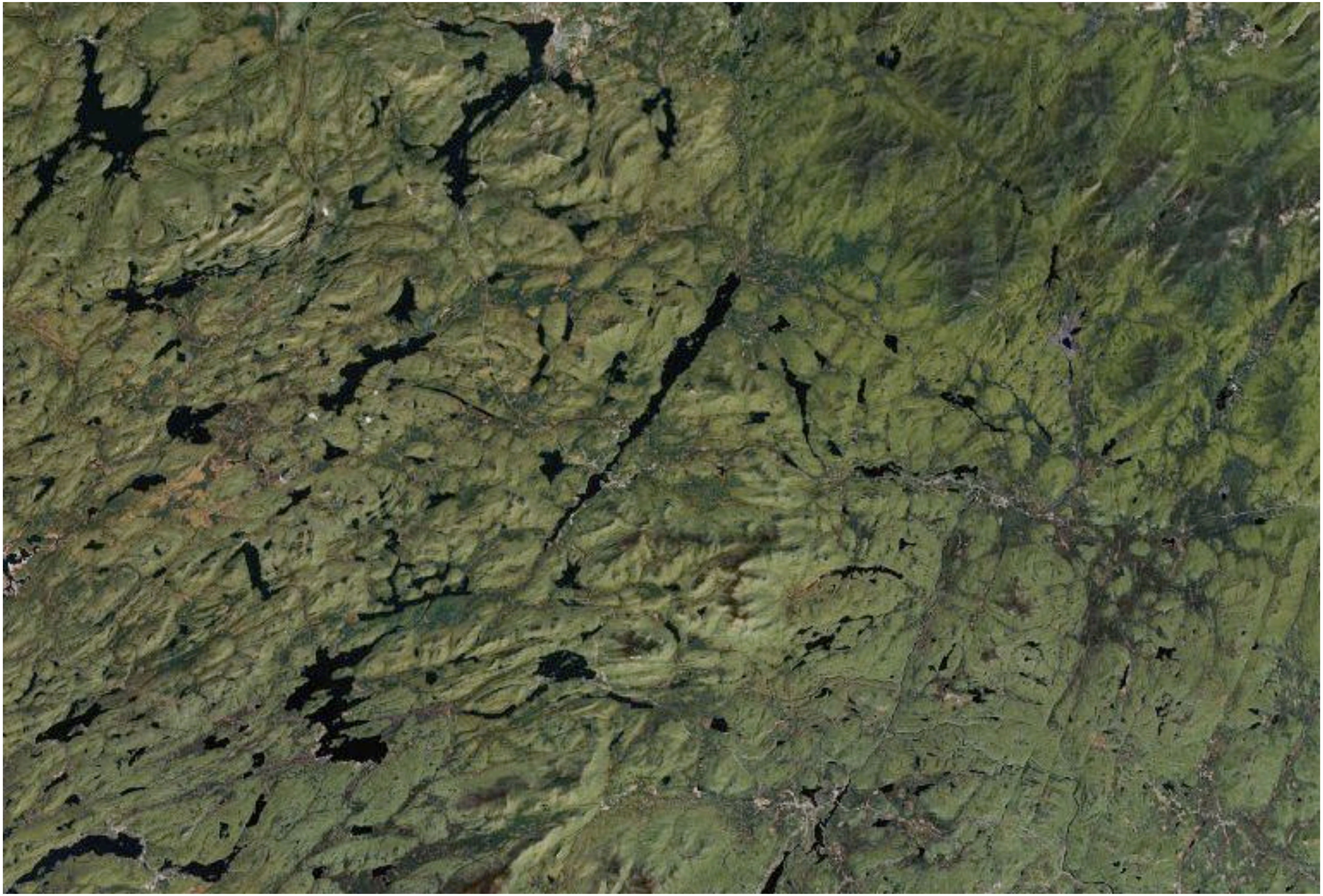


TODO: Find a point in New York State
Adirondacks are nice

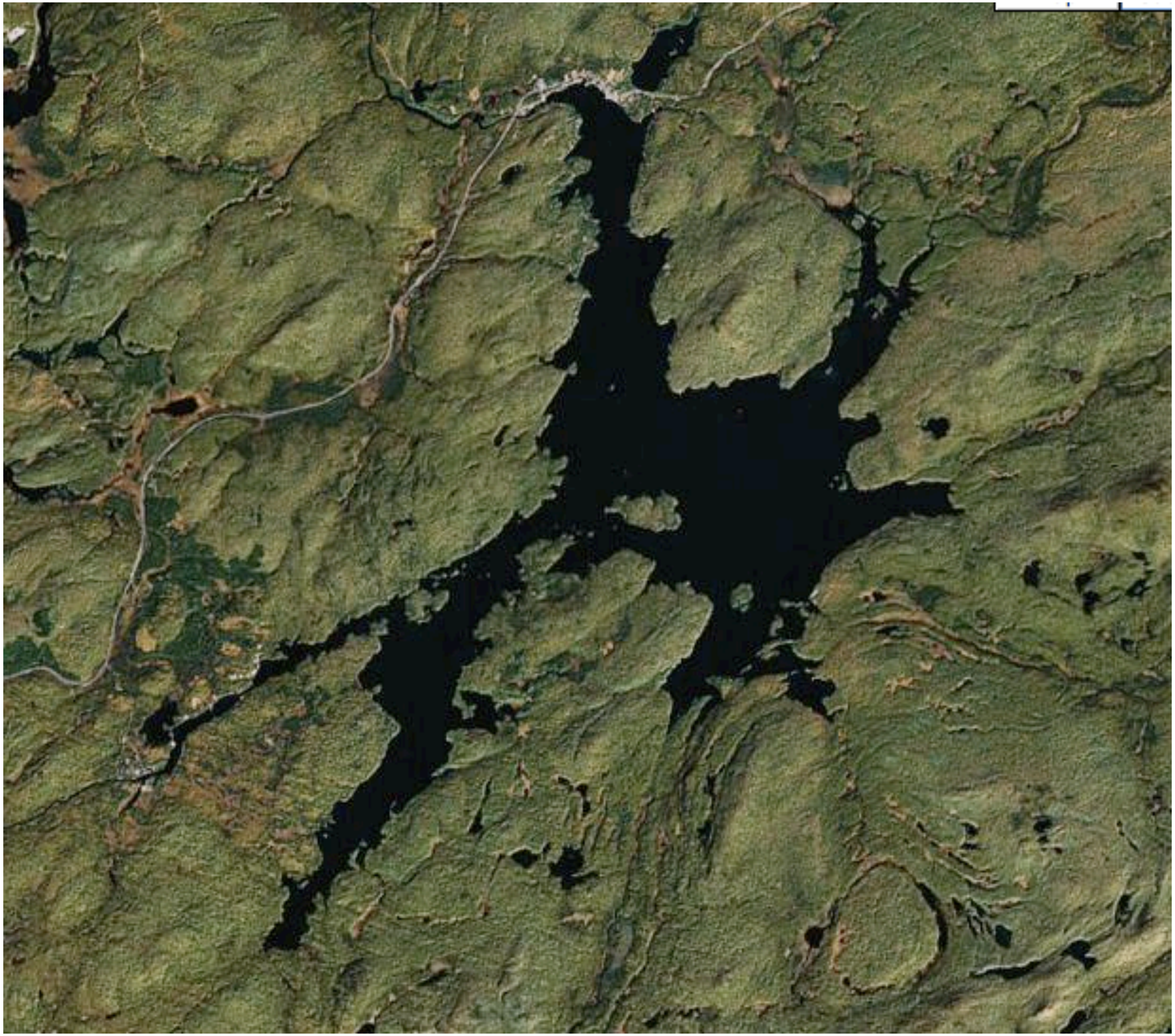


61 of about 102

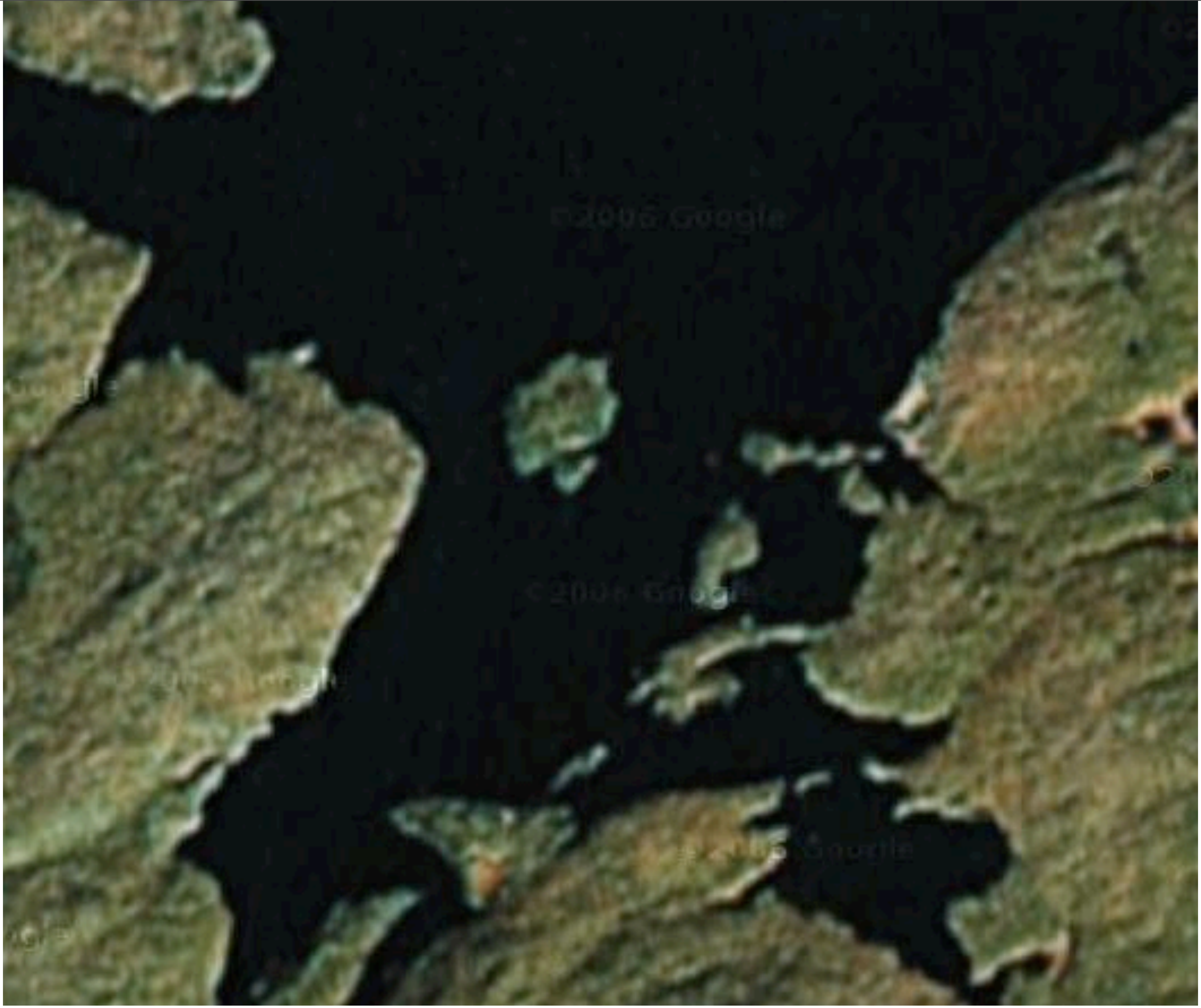
Lakes have interesting shapes,
let’s zoom in on the middle



Upside down dog in the upper left



Dogs bark, check out the voice box



PW is lat/long of the center island

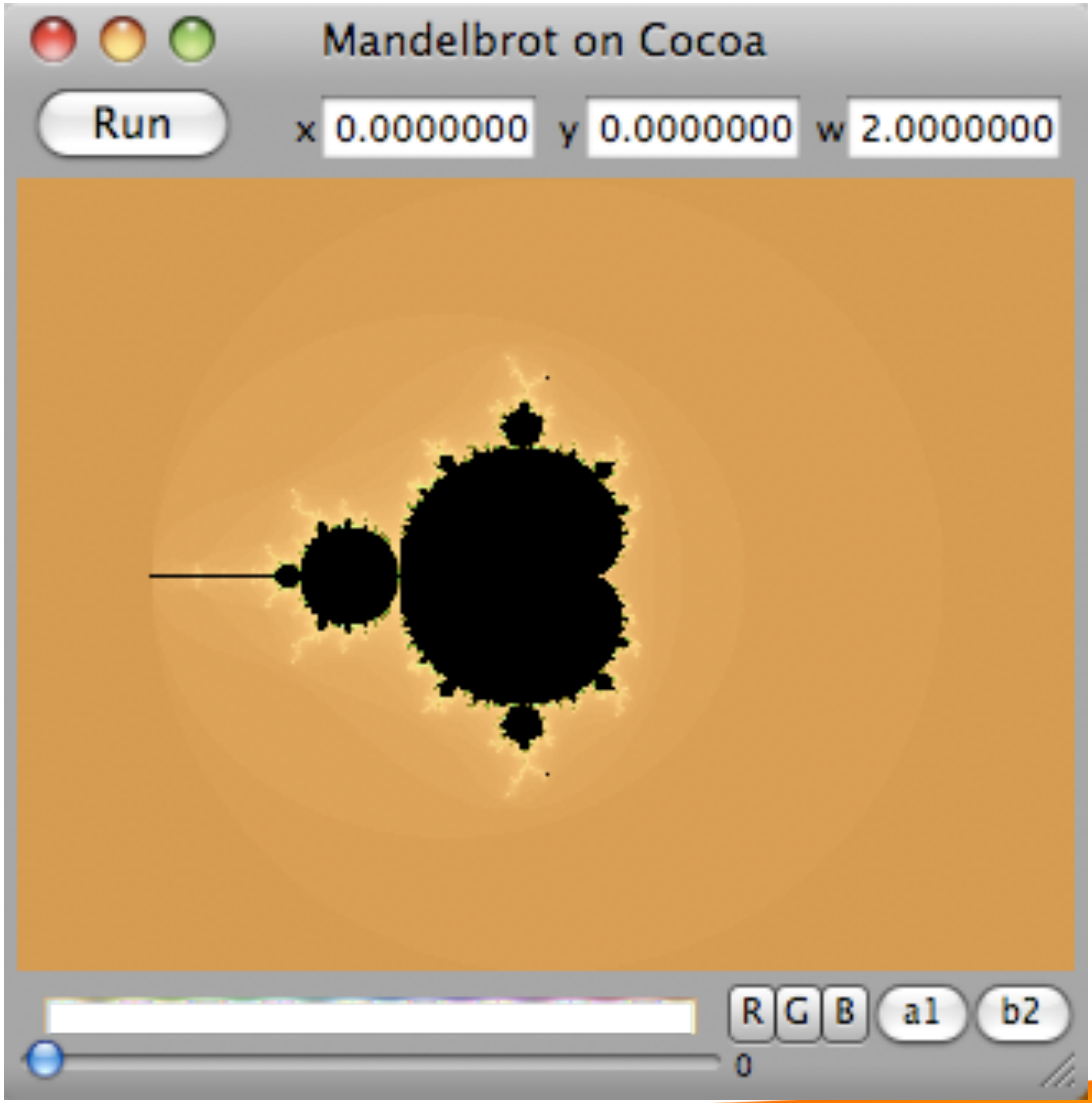
Passmaps?

- 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?

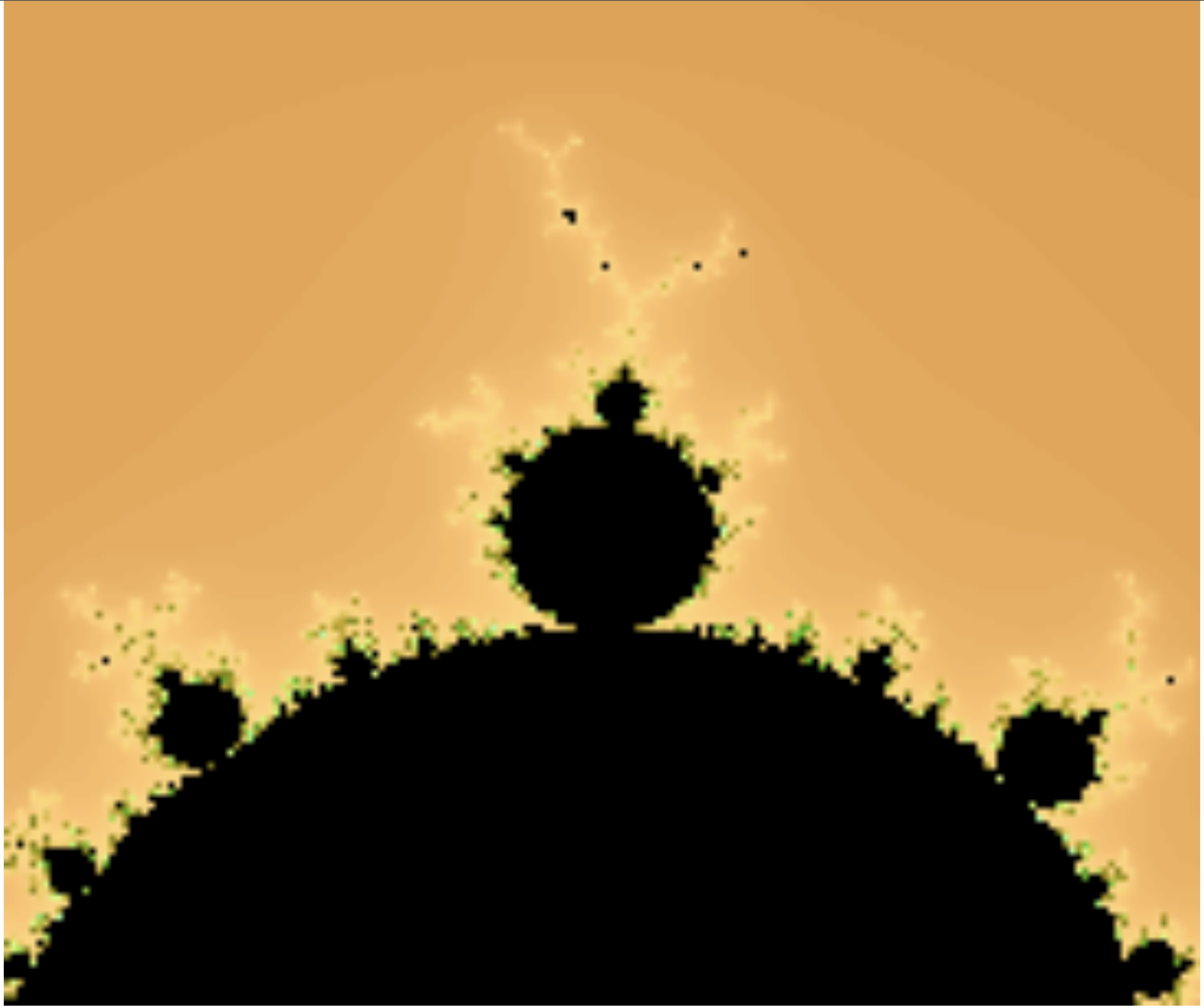
Some Whacko Ches Ideas

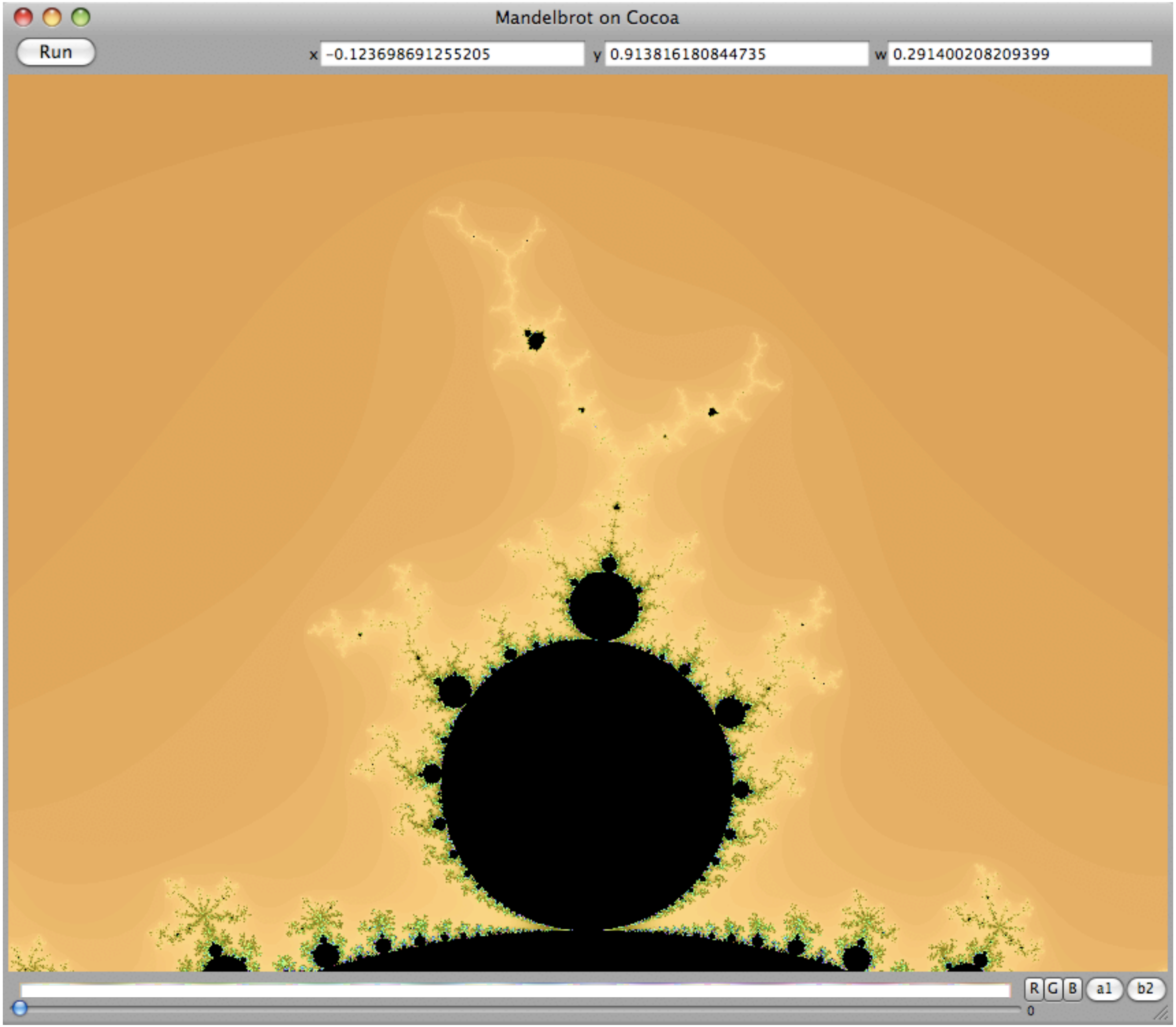
How about passgraphs? Get Google out of the loop

The Mandelbrot Set



x 0.0000000 y 0.0000000 w 2.0000000



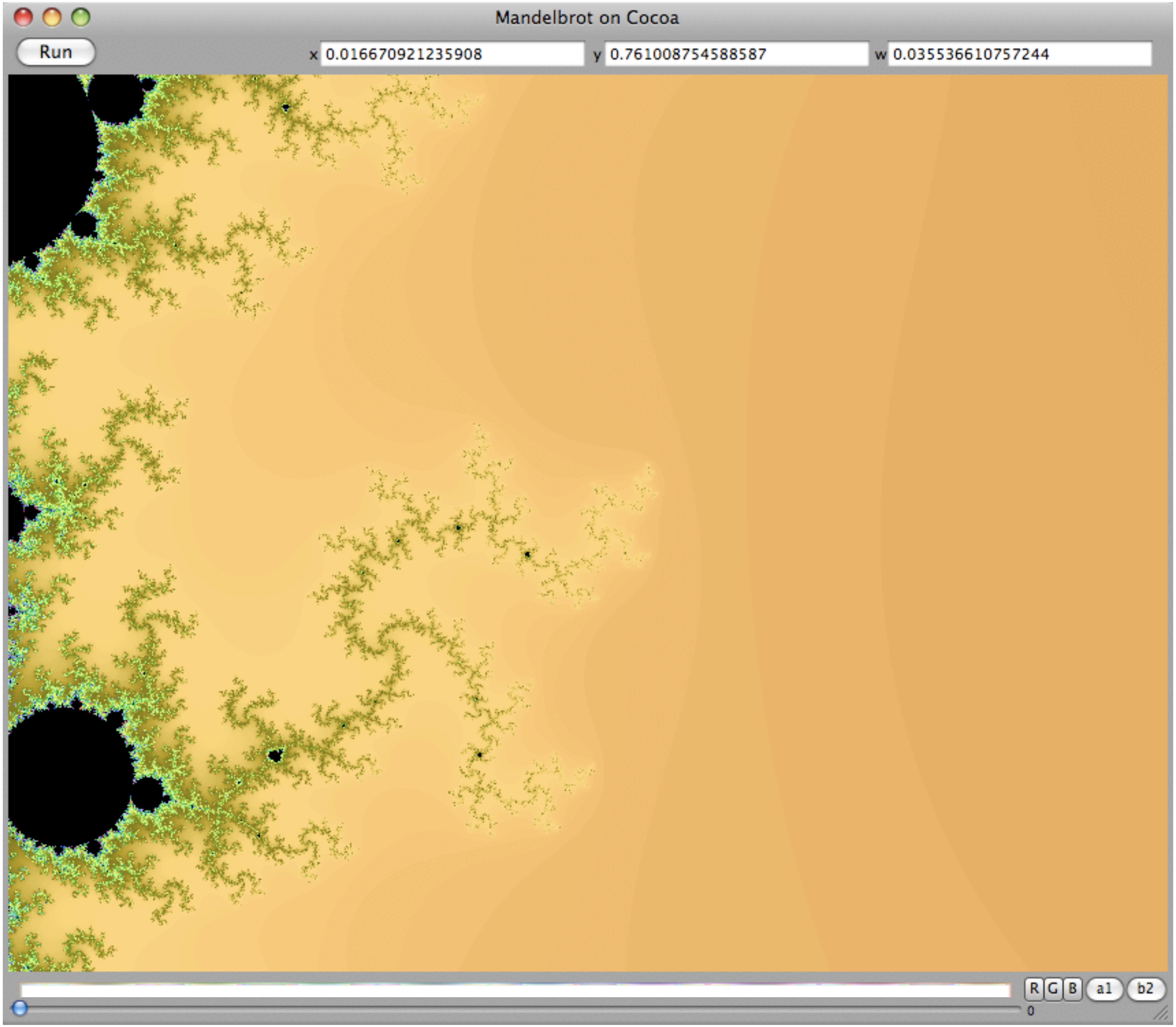


Mandelbrot on Cocoa

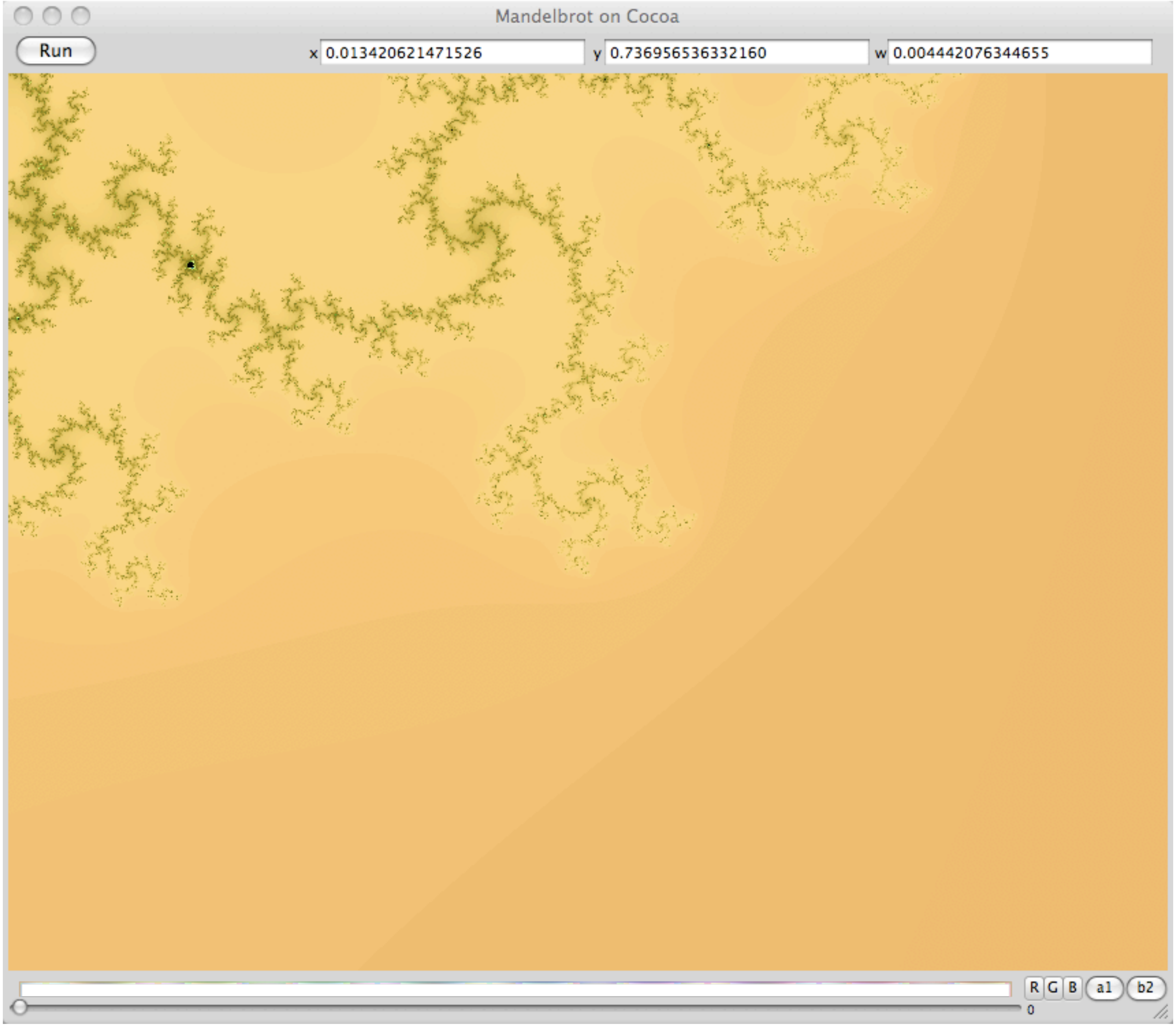
x -0.123698691255205

y 0.913816180844735

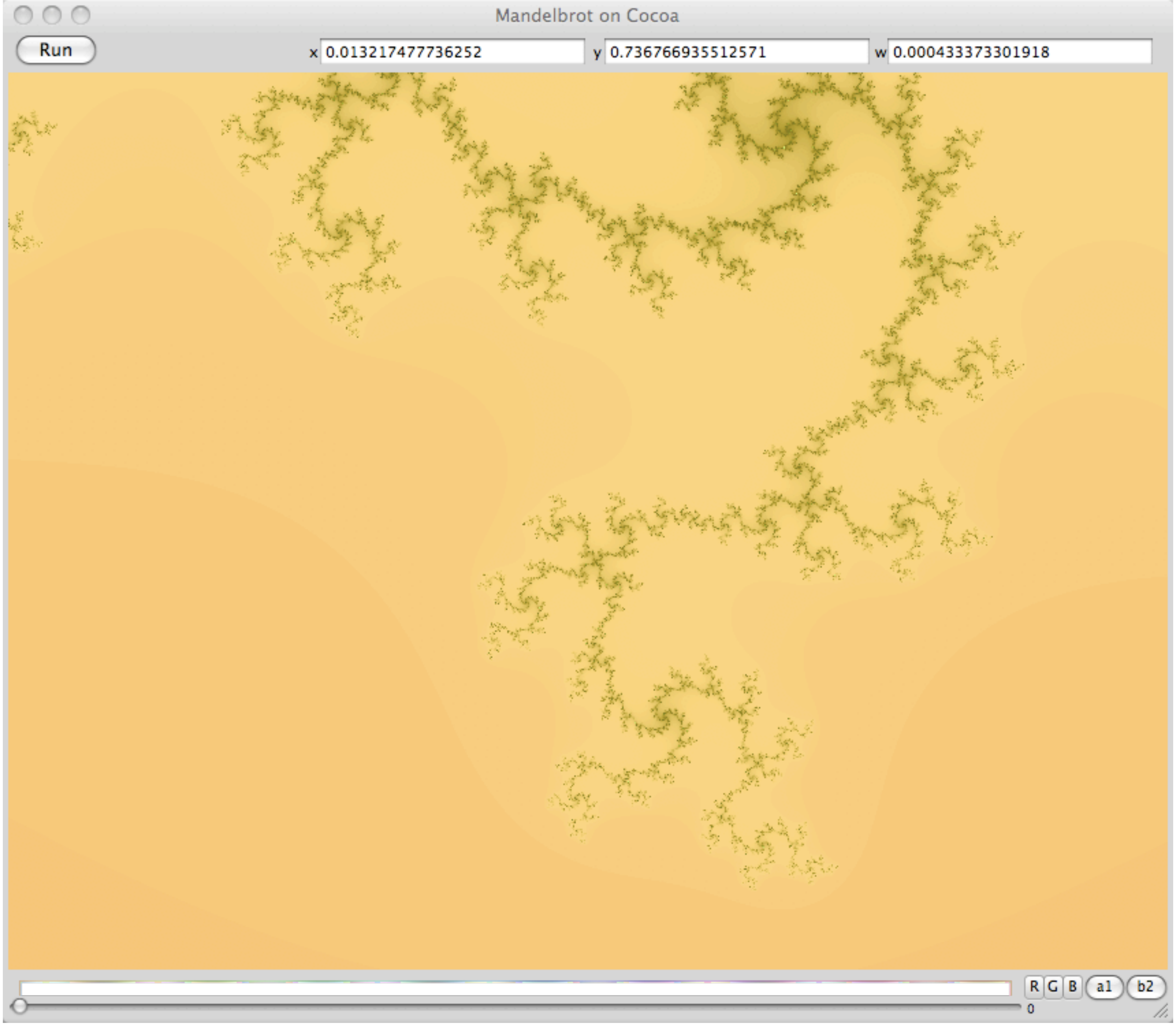
w 0.291400208209399



x 0.016670921235908 y 0.761008754588587 w 0.035536610757244



x 0.013420621471526 y 0.736956536332160 w 0.004442076344655

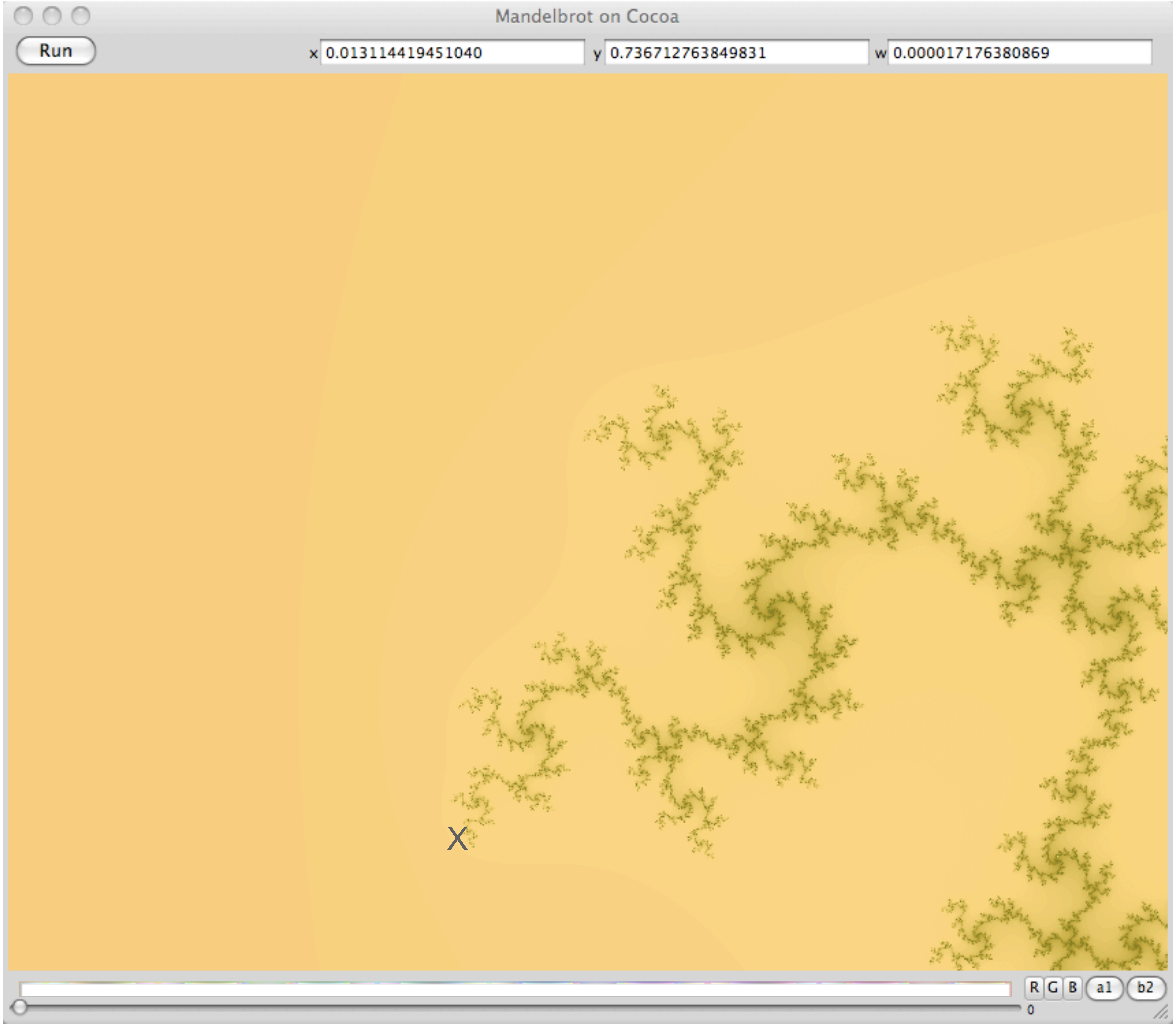


Mandelbrot on Cocoa

x 0.013217477736252

y 0.736766935512571

w 0.0004333373301918



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

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***

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

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